Copyright and Citation Considerations for this Thesis/Dissertation

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

- **NonCommercial** — You may not use the material for commercial purposes.

- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

**How to cite this thesis**

Smart Grid Critical Information Infrastructure
Protection through multi-agency
by
Sheu Menete Alexandre Mavee
submitted in fulfilment
of the requirements for the degree
Magister Commercii
in Informatics
for the
Faculty of Science at the
University of Johannesburg
Supervisor: Prof. E.M. Ehlers
Co-supervisor: Dr. W.S. Leung
Critical Infrastructure is the term used to describe assets that are of utmost importance, or in other words, essential in the functioning of an environment. Societies depend on their critical infrastructure in order to maintain and continuously improve on their population's standard of living.

The creation of more self-sustainable methods of energy consumption and generation drives towards the creation of a better and more efficient evolution of the power grid critical infrastructure, named the smart grid. The introduction of the smart grid brought in a paradigm shift towards the practices used to manage the generation and distribution of electric power.

The introduction of highly capable information systems to intrinsically work with current power grid technologies provided the ability to enhance economic and environmental efficiency of power systems. Although providing a wide variety of benefits, such information systems also created new points of vulnerabilities, which if exploited, place the smart grid at risk of disruptions.

In order to address the security issues that occur at the application and data exchange level of smart grid information systems, the dissertation proposed the use of a security model to protect the smart grid. The Multi-Agent Smart Grid Security (MA-SGS) model is based on the use of multiple autonomous intelligent software agents which attempt to create operational stability and efficiency in the smart grid.

The MA-SGS model uses a multi-agent setup at each of the network nodes found in the smart grid. Agents deployed at a specific network node work together to ensure security and stability on their location, co-operating to generate new knowledge which can be used by the agents deployed at every other node of the smart grid network.

In order to test the evaluation of the model, a smart grid simulation environment (SmartGridSim) was developed. The SmarGridSim simulation environment exhibited the main characteristics of the smart grid in order to demonstrate the functioning of the MA-SGS model. In order to further test the MA-SGS model, a malicious disruption software
agent was introduced to the simulation in order to attempt to destabilise the smart grid. Results demonstrated that with the ability of learning, the MA-SGS agents helped maintain the operational stability of the SmartGridSim environment.

**Keywords:** critical infrastructure, smart grid, agent simulation, multi-agent systems, intelligent agent, information security, complex adaptive systems, artificial intelligence.
Dedication

To my parents, Armindo Alexandre & Salmina Alfeu Alexandre, who through their humble beings, their hard work, dedication and personal sacrifices in the search of providing all that is best for myself and my siblings, have truly shown me what to aim for in my personal life and have made me the person I am today. For all that you are to me and all that you have done I will forever love you!

I would like to thank my siblings and girlfriend who witnessed all my efforts and dedication into completing my research dissertation. Thank you for all your support, motivation and patience through this tough journey. All your understanding truly did not go unnoticed and I am grateful I had you all in my life throughout this time.

I would like to extend a word of thanks to all my friends and my colleagues (whom I also regard as friends) at the Academy of Computer Science and Software Engineering for all your continuous support and encouragement through this time.

To Doctor Wai Sze Leung, I would like to thank you for all your dedication in making sure the dissertation was of the best quality possible in all research aspects. I will forever be grateful to you for having been an inspirational figure in my academic life and also having believed in me since my first year at the Academy.

Last but not least, to Professor Elizabeth Ehlers, I would like to thank you for believing in me and having supported my studies since my fourth year at the Academy. Thank you for all your patience throughout this entire journey, which would have not had the immense level of success that was achieved if you were not present.

P.S.: All makers of energy drinks! I salute you!

“If you have God on your side, all becomes clear.”

Ayrton Senna
Agradecimentos

Para os meus pais, Armindo Alexandre & Salmina Alfeu Alexandre, que através de seus seres humildes, seu trabalho duro, dedicação e sacrifícios pessoais na busca de proporcionar tudo do bom e do melhor para mim e para os meus irmãos, verdadeiramente mostraram-me o que eu desejou alcançar na minha vida pessoal e fizeram-me a pessoa que sou hoje. Por tudo o que vocês são para mim e tudo o que vocês sempre fizeram eu sempre irei ama-los!

Gostaria de agradecer aos meus irmãos e minha namorada que testemunharam todos os meus esforços e dedicação para completar a minha dissertação. Obrigado por todo o vosso apoio, motivação e paciência nesta viagem difícil. Toda a vossa compreensão verdadeiramente não passou despercebida e eu sou grato por ter todos vocês na minha vida, durante este tempo cheio de desafios.

Gostaria de dirigir uma palavra de agradecimento a todos os meus amigos e os meus colegas (que eu também considero como amigos) na Academy of Computer Science and Software Engineering por todo o apoio neste tempo difícil.

Para Doutora Wai Sze Leung, eu gostaria de agradecer-lhe por toda a sua dedicação no sentido de assegurar que a dissertação foi da melhor qualidade possível em todos os aspetos. Serei eternamente grato pela doutora ter sido uma figura inspiradora na minha vida académica e também ter acreditado em mim desde o meu primeiro ano na universidade.

Por último, mas não menos importante, a Professora Elizabeth Ehlers, gostaria de lhe agradecer por ter acreditado em mim e ter apoiado os meus estudos desde o meu quarto ano na universidade. Eu lhe agradeço por toda paciência durante todo esse percurso, que não teria sido o imenso nível de sucesso que foi alcançado se você não estivesse presente.

P.S.: Todos os fabricantes de bebidas energéticas! Eu vos saludo!

“Se você tem Deus ao seu lado, tudo fica claro.”

Ayrton Senna
# Table of Contents

List of Figures ............................................................................................................................... xiv

List of Tables ................................................................................................................................. xvii

List of Acronyms ............................................................................................................................ xviii

Chapter 1: Introduction ................................................................................................................ 1

1.1 – Introduction ....................................................................................................................... 2

1.2 – Problem Statement ............................................................................................................ 3

1.3 – Research Objectives ......................................................................................................... 4

1.4 – Research Questions .......................................................................................................... 6

1.4.1 – Resulting Research Outputs ........................................................................................ 7

1.5 – Research Methodology .................................................................................................... 7

1.5.1 – Introduction ................................................................................................................. 8

1.5.2 – Background Study & Literature Review .................................................................... 8

1.5.3 – Model Construction & Overview .............................................................................. 10

1.5.4 – Model Implementation, Results & Conclusion ............................................................ 10

1.6 – Conclusion ....................................................................................................................... 10

Chapter 2: Critical Infrastructure ............................................................................................... 12

2.1 – Introduction ..................................................................................................................... 13

2.2 – Critical Infrastructure ..................................................................................................... 13

2.3 – Critical Infrastructure Interdependencies .................................................................... 16

2.4 – Management and Ownership of Critical Infrastructures ........................................... 18

2.5 – Critical Infrastructure Protection ................................................................................... 20

2.6 – Conclusion ...................................................................................................................... 21

Chapter 3: Critical Information Infrastructure Protection ......................................................... 23

3.1 – Introduction ...................................................................................................................... 24
## Chapter 5: The Smart Grid as a Critical Infrastructure

- **5.1 – Introduction** ................................................................. 59
- **5.2 – Power Layer** ................................................................. 60
  - **5.2.1 – Distributed Generation** .............................................. 62
  - **5.2.2 – Microgrids and Virtual Power Plants** ......................... 63
- **5.3 – Communications Layer** ................................................. 66
- **5.4 – Applications Layer** ....................................................... 69
- **5.5 – Vulnerabilities and the Smart Grid Critical Infrastructure** ......................................................................................... 72
- **5.6 – Conclusion** ..................................................................... 75

## Chapter 6: Software Agents

- **6.1 – Introduction** ................................................................. 78
- **6.2 – Agent Systems** ............................................................. 78
  - **6.2.1 – Types of Environments** .............................................. 82
  - **6.2.2 – Types of Agents** ........................................................ 83
- **6.3 – Multi-Agent Systems** .................................................... 87
- **6.4 – Conclusion** ..................................................................... 89

## Chapter 7: Intelligence Enabling Machine Learning Models

- **7.1 – Introduction** ................................................................. 91
- **7.2 – Intelligent Agents** .......................................................... 92
- **7.3 – Learning** ........................................................................ 94
- **7.4 – Machine Learning Models** ............................................. 96
  - **7.4.1 – Neural Networks** ....................................................... 97
    - **7.4.1.1 – Feed-Forward Neural Networks** ............................. 97
    - **7.4.1.2 – Self-Organised Maps Neural Networks** .................. 98
    - **7.4.1.3 – Limitations of Neural Networks** ............................ 98
7.4.2 – Artificial Immune System ........................................................................ 99
7.4.2.1 – Clonal Selection Theory ..................................................................... 99
7.4.2.2 – Immune Network Theory .................................................................. 100
7.5 – Conclusion ............................................................................................. 101

Chapter 8: Intelligent Agents and Complex Adaptive Systems ......................... 103
8.1 – Introduction ............................................................................................ 104
8.2 – Complex Adaptive Systems ..................................................................... 105
8.3 – Modelling Complex Adaptive Systems .................................................. 110
8.4 – Modelling Intelligent Agents for Complex Adaptive Systems ............... 112
8.5 – Conclusion ............................................................................................ 114

Chapter 9: Agent Technology and Critical Information Infrastructure Protection 116
9.1 – Introduction ............................................................................................ 117
9.2 – Application of Agent Technology in Critical Information Infrastructure Protection ............................................................................................................. 118
9.3 – Agent Frameworks for Critical Infrastructure ........................................ 119
    9.3.1 – Agent Development Frameworks ..................................................... 120
    9.3.2 – Critical Infrastructure Security Platforms ....................................... 122
9.4 – Conclusion ............................................................................................ 123

Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS) .................... 125
10.1 – Introduction ........................................................................................... 126
10.2 – Model Construction Rationale ............................................................... 128
10.3 – Model Overview .................................................................................... 129
    10.3.1 – Overall Model Simulation ............................................................... 131
    10.3.2 – Attack Agent ................................................................................ 133
10.4 – Network Node Structure ....................................................................... 133
10.4.1 – Process Monitoring Agent ................................................................. 135
10.4.2 – Security Response Agent ................................................................. 135
10.4.3 – Interoperability Agent ................................................................. 135
10.4.4 – Database Store Module ................................................................. 135
10.5 – Individual Agent Structure ................................................................. 136
10.5.1 – Sensor Component ........................................................................ 137
10.5.2 – Information Processing Component ................................................. 137
10.5.3 – Internal State Component ............................................................... 137
10.5.4 – Actuator Set Component ............................................................... 137
10.6 – Conclusion ....................................................................................... 138

Chapter 11: MA-SGS Node Agents ................................................................. 139
11.1 – Introduction ...................................................................................... 140
11.2 – Node Agent Types ........................................................................... 141
11.2.1 – Process Monitoring Agent ............................................................... 141
11.2.1.1 – Sensor Component ...................................................................... 141
11.2.1.2 – Information Processing Component ............................................. 141
11.2.1.3 – Internal State Component .......................................................... 142
11.2.1.4 – Actuator Set Component ........................................................... 142
11.2.2 – Security Response Agent ............................................................... 142
11.2.2.1 – Sensor Component ...................................................................... 143
11.2.2.2 – Information Processing Component ............................................. 143
11.2.2.3 – Internal State Component .......................................................... 143
11.2.2.4 – Actuator Set Component ........................................................... 144
11.2.3 – Interoperability Agent .................................................................... 144
11.2.3.1 – Sensor Component ...................................................................... 145
14.3 – Interoperability Agents’ Internal Environment ........................................... 166
14.3.1 – Sensor Component ................................................................................ 167
14.3.2 – Information Processing Component ....................................................... 168
14.3.3 – Internal State Component: ................................................................. 168
14.3.4 – Actuator Component .............................................................................. 169
14.4 – Conclusion .................................................................................................... 169

Chapter 15: MA-SGS: Attack Agent Structure ...................................................... 171

15.1 – Introduction ................................................................................................... 172
15.2 – MA-SGS: Attack Agent – The Proof of Concept Agent ................................ 172
15.3 – Agent Environment ....................................................................................... 174
15.4 – Conclusion .................................................................................................... 177

Chapter 16: MA-SGS: Smart Grid Simulation and Model Implementation ........... 178

16.1 – Introduction ................................................................................................... 179
16.2 – Prototype Implementation Layers and Tools ................................................ 179
16.3 – Smart Grid Simulation ................................................................................... 181
16.3.1 – Energy Agent .......................................................................................... 185
16.3.1.1 – Power Station Energy Agent............................................................. 185
16.3.1.2 – Transformer Energy Agent ............................................................... 186
16.3.1.3 – Microgrid Energy Agent .................................................................... 187
16.3.1.4 – Consumer Energy Agent .................................................................. 188
16.3.2 – Energy Agent and the MA-SGS Model ................................................... 189
16.3.3 – Agent Communication .......................................................................... 191
16.3.4 – Simulation Controller Agent .................................................................... 193
16.3.5 – Attack Agent on the Simulated Smart Grid ............................................. 195
16.3.5.1 – Scenario 1 Attack Agent Disruption: Single Node Disruption .......... 195
16.3.5.2 – Scenario 2 Attack Agent Disruption: Multiple Node Disruption ........ 198
16.4 – Simulation Environment and MA-SGS Model Data Integration .......... 201
16.4.1 – Simulation Environment Data Integration ........................................ 201
16.4.2 – MA-SGS Model Data Integration ................................................... 204
16.5 – Visualisation Layer ......................................................................... 207
16.5.1 – Initiate Simulation Environment ................................................... 207
16.5.2 – Initiate Node Agents ..................................................................... 210
16.5.3 – Initiate Attack Agent ..................................................................... 214
16.6 – Conclusion ....................................................................................... 217

Chapter 17: MA-SGS: Model Results ......................................................... 218
17.1 – Introduction ...................................................................................... 219
17.2 – MA-SGS Model Simulation Results .................................................. 219
17.2.1 – Agent Interaction ......................................................................... 220
17.2.2 – Agent Activity ............................................................................... 226
17.2.3 – Threat Detection .......................................................................... 228
17.2.4 – Defence Strategy Selection ......................................................... 229
17.2.5 – Smart Grid Simulation Operational Stability ................................. 232
17.2.6 – Smart Grid Simulation Restoration and Recovery ....................... 233
17.3 – Conclusion ....................................................................................... 234

Chapter 18: Conclusion ............................................................................ 235
18.1 – Introduction ...................................................................................... 236
18.2 – Model Evaluation ............................................................................ 236
18.2.1 – Resilience and Robustness .......................................................... 237
18.2.2 – Model Component Modularity ..................................................... 238
18.2.3 – Consistency and Integrity ............................................................. 239
List of Figures

Figure 1.1 – Dissertation Roadmap ................................................................................. 9
Figure 2.1 – Interpretive Structural Modelling .................................................................. 16
Figure 3.1 – The Cyber-To-Physical Bridge of Attacks in CII ........................................ 34
Figure 4.1 – Goals of Power Systems ............................................................................. 38
Figure 4.2 – Power Grid Network Composition ............................................................. 38
Figure 4.3 – Power System Control Centre Interactions ................................................. 45
Figure 4.4 – Basic Composition of the Smart Grid ....................................................... 46
Figure 4.5 – The Vision of The Smart Grid ................................................................... 49
Figure 4.6 – Benefits of Smart Grid Implementation .................................................... 50
Figure 4.7 – Conceptual Model of the Smart Grid ....................................................... 52
Figure 5.1 – Smart Grid Taxonomy in terms of the Power, Communications and
Applications Layers ........................................................................................................ 60
Figure 5.2 – The Topology of a Smart Grid microgrid .................................................. 64
Figure 5.3 – Virtual Power Plant in the Smart Grid ....................................................... 65
Figure 5.4 – Integrated Communication Network for the Smart Grid ....................... 67
Figure 5.5 – Classification of Security Threats towards Communication Networks in the
Smart Grid ....................................................................................................................... 68
Figure 6.1 – Agent Definition ......................................................................................... 79
Figure 6.2 – Agent Classification .................................................................................... 85
Figure 6.3 – Typical Multi-Agent System Setup ............................................................. 88
Figure 8.1 – Complex Adaptive System Architecture .................................................. 106
Figure 8.2 – Framework for Engineered Complex Adaptive Systems ....................... 111
Figure 10.1 – Configuration of the MA-SGS Model .................................................... 132
Figure 10.2 – Individual Node Agent Setup ................................................................... 134
Figure 10.3 – Internal Agent Structure .......................................................................... 136
Figure 11.1 – Internal Node Structure .......................................................................... 140
Figure 12.1 – Phase I Environment Setup ...................................................................... 150
Figure 12.2 – Process Monitoring Agent ...................................................................... 151
Figure 13.1 – Phase II Environment Setup .................................................................... 157
Figure 13.2 – Security Response Agent ................................................................. 158
Figure 13.3 – Security Response Agent High Level Static Class Specification ...... 159
Figure 14.1 – Phase III Environment Setup .......................................................... 165
Figure 14.2 – Interoperability Agent ................................................................. 166
Figure 15.1 – Example Simulated Network with an Attack Agent Node .......... 174
Figure 15.2 – Phase IV Environment Setup ...................................................... 175
Figure 16.1 – Prototype Implementation Layers .............................................. 180
Figure 16.2 – Smart Grid Simulation Area Node Types ................................. 182
Figure 16.3 – Energy Agent Generic Structural Components ......................... 189
Figure 16.5 – Internal Agent Communication ................................................... 191
Figure 16.6 – External Communication in the Simulated Smart Grid Environment .... 192
Figure 16.7 – External WCF Communication Medium .................................. 193
Figure 16.8 – Simulation Controller Agent Operating Environment ................ 194
Figure 16.9 – Attack Agent Scenario 1 Strategy Selection ................................. 196
Figure 16.10 – Attack Agent Scenario 2 Strategy Selection ............................... 199
Figure 16.11 – Data Sources for Attack-Resilient Control Systems .................. 204
Figure 16.12 – Overall Model Initialisation Steps ............................................. 207
Figure 16.13 – Simulation Layer Smart Grid Network Generation .................... 208
Figure 16.14 – Smart Grid Simulation Details Setup ........................................ 209
Figure 16.15 – Main User Interface Waiting for Simulation Start Command ........ 209
Figure 16.16 – Simulation Layer Network Node Agent Initialisation ................. 210
Figure 16.17 – Visualisation Layer Smart Grid Node User Interface Controls .... 211
Figure 16.18 – Visualisation Layer Simulation Network Network View ............. 211
Figure 16.19 – Simulation Smart Grid Network Node Detailed Views .............. 212
Figure 16.20 – Simulation Smart Grid Network Operational Status Gauge ....... 213
Figure 16.21 – Visualisation Layer User Interface ............................................ 214
Figure 16.22 – Visualisation Layer Attack Agent Initialisation ......................... 214
Figure 16.23 – Sample Attack Agent Disruption Attempt List ......................... 215
Figure 16.24 – Sample Attack Agent Event Log .............................................. 215
Figure 16.25 – Attack Agent Disruption Attempt User Control ....................... 216
Figure 16.26 – Attack Agent Operations Control User Interface ..................... 216
Figure 17.1 – Prototype Simulation Smart Grid Network and sample Live Results View
.............................................................................................................................................. 221
Figure 17.2 – Messages Processed (distributed by source)............................................. 223
Figure 17.3 – Messages Processed (distributed by sender Agent)................................. 223
Figure 17.4 – Messages Processed (by type)...................................................................... 224
Figure 17.5 – Messages Processed based on Completion ................................................. 224
Figure 17.6 – Number of Messages Processed over simulation time ............................. 225
Figure 17.7 – Agent Activity Results................................................................................ 227
Figure 17.8 – Process Monitoring Agent Detection............................................................ 228
Figure 17.9 – Security Response Agent Detection............................................................ 230
Figure 17.10 – Processed Attack Agent Disruption Attempts......................................... 231
Figure 17.11 – Smart Grid Operational Level Observed ............................................... 232
Figure 17.12 – Smart Grid Observed Operational States................................................ 233
List of Tables

Table 2.1 – Critical Infrastructure Examples .......................................................... 14
Table 3.1 – Countries and Critical Infrastructure Legislation ............................... 31
Table 4.1 – Electricity Distribution Network Components ................................. 41
Table 4.2 – Information Systems in the Power Grid ............................................. 43
Table 4.3 – Communication Standards in the Smart Grid ................................. 56
Table 5.1 – Applications and Challenges in the Smart Grid ................................ 74
Table 6.1 – Agent Concepts ................................................................................ 80
Table 9.1 – Tools and Frameworks for the Development of Federated Simulations . 121
Table 11.1 – Security Response Agent Possible Actions ..................................... 144
Table 16.1 – Classification Scheme of Operational States of a Power System ...... 183
Table 16.2 – Simulation Layer State Semantic ...................................................... 184
Table 16.3 – State Margins ................................................................................. 184
Table 16.4 – Disruption Scenario 1 Step Description .......................................... 197
Table 16.5 – Simulation Smart Grid Data Usage ............................................... 202
Table 17.1 – Simulation Network Details ............................................................ 219
Table 17.2 – Types of agents found in the prototype simulation .......................... 226
Table 18.1 – Research Objectives Addressed ...................................................... 242
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CII</td>
<td>Critical Information Infrastructure</td>
</tr>
<tr>
<td>CIIP</td>
<td>Critical Information Infrastructure Protection</td>
</tr>
<tr>
<td>MA-SGS</td>
<td>Multi-Agent Smart Grid Security</td>
</tr>
<tr>
<td>WPF</td>
<td>Windows Presentation Foundation</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>IA</td>
<td>Interoperability Agent</td>
</tr>
<tr>
<td>PMA</td>
<td>Process Monitoring Agent</td>
</tr>
<tr>
<td>SRA</td>
<td>Security Response Agent</td>
</tr>
<tr>
<td>WCF</td>
<td>Windows Communication Foundation</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>DMS</td>
<td>Distribution Management System</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy Management System</td>
</tr>
<tr>
<td>PCS</td>
<td>Process Control System</td>
</tr>
<tr>
<td>DG</td>
<td>Distributed Generation</td>
</tr>
</tbody>
</table>
Chapter 1
Introduction
1.1 – Introduction

The increased dependency of society on Critical Infrastructure has raised an important need for research on the methods used to protect them. Modern Critical Infrastructure relies heavily on cyber technology as it is mainly based on multiple computer systems and wide computer networks, which are used to control each component of Critical Infrastructure. One of the main challenges in this task is to enable the secure communications between the heterogeneous components found therein (Amin, 2012).

This reliance on cyber technology has brought forward all the security concerns inherent in the use of advanced network systems. Security breaches in these systems threaten the stability and integrity of Critical Infrastructure, which could cause detrimental effects in the services they provide to society. The resulting need for security measures that cover the technological spectrum of critical service provision has given rise to the field of Critical Information Infrastructure protection.

A Critical Information Infrastructure System, used to manage a Critical Infrastructure, comprises many different network components. The communication between these different components can occur through the use of many different media, of which the Internet is one. Vast quantities of information are transferred between the different components of a Critical Infrastructure system to ensure that accurate information is used when making configuration decisions that keep the infrastructure running in a stable manner.

The smart grid is an upgrade of the regular electric power grid Critical Infrastructure. It basically adds an information processing layer to the power grid. This is for electricity distribution, storage, generation, pricing etc— and is used to attain better power management in order to decrease costs and the carbon footprint of electricity usage. The Smart Grid is still composed of the basic instruments of the generic power grid (e.g. power stations, substations, power lines, generators, distribution stations etc.), but it adds on alternative electricity generation sources such as solar panels and electric
vehicles (Huang, Nguyen, Zheng & Han, 2013). Each of these components in the Smart Grid is closely monitored by computer systems, and all gathered information is sent to a central system for analysis.

1.2 – Problem Statement

Each of the components of the smart grid is equipped with information gathering sensors that are used to receive real time data for processing. These components within the smart grid are grouped into the nodes present in the network. The nodes in the network represent all generators and consumers of electric power that are connected to the grid (Knauss, Warren & Kearns, 2012).

The monitoring of the smart grid network nodes can become quite a complex task due to the amount of data that they gather. As the grid is based on a large network of systems that gather real time data, making sure that each node is protected against cyber-attacks can be a cumbersome task (Fadul, Hopkinson, Andel & Sheffield, 2014).

Security has to be maintained at both the node level and at the network level if the smart grid is to operate with no disruptions. The protection of consumer data, which is gathered by the smart meters used to measure electricity consumption of customers, is important as smart meters can be compromised, just as the networks to which they are connected can also be (Kim & Tong, 2013).

The security problems in the smart grid can be quite complex when initially tackled, and one of the best ways to solve some of these issues is to break them down into more concise problems where a framework for solving each issue can be used. In computer systems, one of the approaches used to solve complex problems by breaking them down into smaller sub-problems is through the implementation of intelligent multi-agent systems. These systems make use of multiple agents to solve each identified sub-problem, so that, together, through their communication and coordination, they can then collaborate to solve large complex problems.
When looking at the overall security issues involved in the communication of the different nodes in the smart grid, the following list provides some of the sub-problems that need to be addressed when attempting to improve communication security (Amin, 2012):

- Monitoring of information in the nodes of the smart grid network (e.g. smart meters, transmission stations, generators etc.);
- Ensuring integrity in the information transferred;
- Ensuring privacy in the information transferred;
- Detecting data tampering at the node and network levels;
- Mitigating attacks at the node and network levels.

The use of a multi-agent system is suitable for the problem domain as distributed autonomous agents provide a flexible, extendable and versatile approach to the monitoring of the different nodes in the Smart Grid network. Through communication and coordination of actions, each agent can help monitor the processes in its own node and those around its vicinity. This way, with a carefully examined agent distribution plan, the monitoring of the information transfer, as well as the capacity to provide protection against possible threats, can become more effective in order to protect the Smart Grid Critical Information Infrastructure.

When looking at the theoretical aspects of the problem domain, a multi-agent system can be a solution for enhancing security, but, in order to carry out an objective study of this suitability, a few goals need to be specified. The following section looks at the research objectives of the dissertation.

### 1.3 – Research Objectives

The main objective of this dissertation is the creation of a multi-agent system designed to monitor the information processing activities in the smart grid. The model aims at evaluating the communication between the nodes in order to enhance the security, robustness and resilience of the smart grid by protecting the confidentiality, integrity and availability properties of the information therein. The Multi-Agent Model for Smart Grid
Security (MA-SGS) will make use of a selection of intelligent agent techniques in order to protect the smart grid network and the nodes working within it.

Given the complexity of the problem domain and the research objectives of the dissertation, these objectives were broken down into more concise sub-objectives in order to create milestones that together achieve the bigger picture of the aimed result. Each chapter in the dissertation will cover one or more of the defined sub-objectives, and progressively contribute to accomplishing the main objectives. The following is a list of objectives that must be fulfilled in order to reach the main goal of the dissertation:

- Identification and analysis of aspects relevant to Critical Information Infrastructure protection;
- Description and understanding of the security requirements for a resilient and robust Critical Information Infrastructure;
- Identification and analysis of current developments in the smart grid and the security aspects discovered to date;
- Definition and discussion of concepts to do with intelligent agents and the use of multi-agent systems;
- Definition and discussion of common machine learning techniques;
- Design and implementation of a multi-agent system to monitor and enhance security in a simulated smart grid environment;
- Examination of results obtained from the simulated smart grid environment in order to evaluate the multi-agent approach to enhance security, resilience and robustness in the smart grid Critical Information Infrastructure.

In order to objectively achieve the combination of research objectives, a few questions need to be answered. The next section lists the research questions that the dissertation aims at answering.
1.4 – Research Questions

In essence, based on the research objectives listed in the previous section, this dissertation primarily attempts to answer the following question:

_Can Critical Information Infrastructure protection in a Smart Grid environment be achieved through the use of software agents using a multi-agent approach?_

To find an answer to the dissertation’s primary question, three questions are formulated to address each aspect of the problem statement that was defined. The three questions addressed in the dissertation are as follows:

- **Question 1**
  
  _Can intelligent agents in multi-agent systems be used in Critical Information Infrastructure protection?_

- **Question 2**
  
  _How can multi-agent system theory be applied to the Smart Grid?_

- **Question 3**
  
  _As a follow up for Question 2, how would the security, resilience and robustness properties of the Smart Grid’s Critical Information Infrastructure be improved with the use of a multi-agent system?_

The three questions above will be the main focus of the main body of the dissertation. The primary question is re-visited in the last chapter of the dissertation. The following section introduces the research methodology used to define the structure of the research content to be presented. The content presented addresses the dissertation’s research objectives and questions to be answered.

In order to evaluate the validity and current relevance of the research questions set in the dissertation, exploratory research works were carried out and published as peer-reviewed research outputs listed in the following sub-section.
1.4.1 – Resulting Research Outputs

The following is a list of the published and presented research papers undertaken to investigate the topic of the dissertation and to further define the reach of the proposed model:


Full abstracts of the peer-reviewed research papers listed above can be found in Appendix C of the dissertation. The published research papers are available on the dissertation’s accompanying DVD.

1.5 – Research Methodology

The dissertation achieves the objectives set in section 1.3 and answers the research questions posed in section 1.4 by:

- Carefully investigating the relevant concepts that exist within the problem domain;
- Creating a model that sets out to test the possibility of using a multi-agent system designed to work within the Critical Information Infrastructure of the smart grid;
- Testing the designed model through the use of a prototype system that uses the features of the designed model in order to evaluate the effectiveness of multi-agent systems in the enhancing of system security, resilience and robustness.
Olivier (2011) states that a model is used to ‘capture the essential aspects of a system or process, while ignoring the nonessential aspects’. As the main objective of the dissertation is the creation of a model that is to be used in Critical Information Infrastructure protection, the overall methodology used sets out to carefully discuss all essential aspects pertaining to Critical Information Infrastructure protection in the smart grid, and the concepts necessary in the creation of the model, its testing and evaluation.

The objectives of the dissertation (Section 1.3) were listed in a sequential order, in which each step guides the reader forward in the answering of all the research questions. The dissertation has therefore been divided into five sections where each section gradually addresses each of the defined research objectives. Each section is composed of chapters that can address one or more of the research objectives and the research questions posed to satisfy the former. Figure 1.1 illustrates each of the sections of the dissertation.

The dissertation’s research methodology follows the approach suggested by Olivier (2011), where the chapter under each section discusses and analyses relevant topics that address the objectives so that the overall picture is clear at the end. The following subsections briefly explain how each of the dissertation’s sections will follow the chosen research methodology.

1.5.1 – Introduction

The current section aims to introduce the reader to the problem domain of the dissertation, that is, the objectives it aims to achieve and the questions it endeavours to answer. It also gives a brief breakdown of how the dissertation is structured to provide a better understanding of the steps that are followed to satisfy the research objectives.

1.5.2 – Background Study & Literature Review

As the previous section gives a brief introduction of what the reader should expect, this section contains the relevant background information and the literature survey of the
problem domain and the main objectives on which the dissertation is based. The chapter covers the main topics, which will be useful in the understanding, analysing and criticising of the model constructed to solve the issues stated in the problem statement and to answer the research questions.

Figure 1.1 – Dissertation Roadmap
1.5.3 – Model Construction & Overview

After the relevant topics have been discussed, this section introduces the overview of the model built on the concepts discussed in the previous section of the dissertation. After an overview of the model is discussed, a careful examination of each component used to create the model is then carried out in greater detail to give a thorough explanation of how the model was constructed. After the model’s overview chapter, each following chapter provides the details of the underpinnings of the model’s components. The implementation of the model’s proof of concept prototype is also discussed in each of the chapters.

1.5.4 – Model Implementation, Results & Conclusion

As the previous section discusses the overall model and its implementation in detail, this section serves to provide the results achieved by the simulation prototype, analysing its performance in order to determine if, indeed, the model was able to objectively address the research questions posed in the beginning of the dissertation. An evaluation of the simulation run results will be carried out in order to determine if the use of the multi-agent approach in Critical Information Infrastructure protection is deemed viable or not.

To maintain the readability of the dissertation, all the necessary algorithm details and UML diagrams used to reflect each of the components of the model, as well as the details of the simulation components and environment, will be elaborated on in the final sub-sections. The reader interested in details of the model can refer to these sub-sections for a more in-depth explanation of the test conditions of the implemented model’s prototype.

1.6 – Conclusion

After an examination of the results obtained from the running of the MA-SGS model, an objective analysis will be used to determine the effectiveness and suitability of multi-
agent models. Any positive and negative aspects of the design decisions and infrastructure effects of the model will be evaluated in order to carefully evaluate how each original research question of the dissertation was answered.
Chapter 2
Critical Infrastructure

- Chapter 1: Introduction
- Chapter 2: Critical Infrastructure
- Chapter 3: Critical Information Infrastructure Protection
- Chapter 4: The Smart Grid
- Chapter 5: The Smart Grid as a Critical Infrastructure
- Chapter 6: Software Agents
- Chapter 7: Intelligence Enabling Machine Learning Models
- Chapter 8: Intelligent Agents and Complex Adaptive Systems
- Chapter 9: Agent Technology and Critical Information Infrastructure Protection
- Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS)
- Chapter 11: MA-SGS: Node Agents
- Chapter 12: MA-SGS: Process Monitoring Agent
- Chapter 13: MA-SGS: Security Response Agent Structure
- Chapter 14: MA-SGS: Interoperability Agent Structure
- Chapter 15: MA-SGS: Attack Agent Structure
- Chapter 16: MA-SGS: Smart Grid Simulation & Model Implementation
- Chapter 17: MA-SGS: Model Results
- Chapter 18: Conclusion
2.1 – Introduction

In many ways, modern society is dependent on the provision of services that satisfy the basic needs of a country’s population. In addition to providing water and electricity, the provision of such facilities ensures the continued progress of a country’s social and economic development. Infrastructures – defined as the base or foundation of a system, network or organisation – are set up by the governing bodies of nations to provide critical services. The definition below is found in the Australian National Guidelines for Protecting Critical Infrastructure from Terrorism document, where Critical Infrastructures are defined as follows:

“Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia’s ability to conduct national defence and ensure national security” (2011).

In order to elaborate on Critical Infrastructures, the current chapter will describe what these are, and some of the characteristics that define them. The chapter goes on to explain how different Critical Infrastructures depend on each other, and finally looks briefly at Critical Infrastructure protection.

2.2 – Critical Infrastructure

Several examples of such infrastructures have been listed in Table 2.1 (Yusufovna, Alisherovich, Choi, Cho, Abdurashidovich & Kim, 2009). As can be summarised from the nature of each example, such infrastructures are of the utmost importance to the efficient and effective functioning of a country, thus earning them the title of ‘Critical Infrastructures’.
Table 2.1 – Critical Infrastructure Examples (Yusufovna et al., 2009)

<table>
<thead>
<tr>
<th>Infrastructure</th>
<th>Example(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy resources</td>
<td>Electric power generation stations, distributions networks and smart grids</td>
</tr>
<tr>
<td>Finance</td>
<td>Banking systems, foreign exchange systems, payment systems</td>
</tr>
<tr>
<td>Food</td>
<td>Food distribution systems</td>
</tr>
<tr>
<td>Health</td>
<td>Medical systems</td>
</tr>
<tr>
<td>Government services</td>
<td>Water and electricity provision systems</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Production control systems</td>
</tr>
<tr>
<td>Transportation</td>
<td>Air, rail, and road traffic systems</td>
</tr>
<tr>
<td>People and education</td>
<td>Education systems</td>
</tr>
</tbody>
</table>

Although most definitions of Critical Infrastructure revolve around the running of an entire country, and keeping the stability of its economy and social well-being, Critical Infrastructure can also be defined in the context of its use. Large companies or businesses are often dependent on an array of assets that can range from software systems to heavy manufacturing machinery. These assets are hugely invested in by the company as the assets are directly linked to the revenue generation strategy.

Any damage to these assets could render the company unable to perform some or even the majority of its most basic business processes, thus causing massive losses in revenue. The loss in revenue could lead the company to close down if nothing is done to bring the usage of the assets back. Therefore, in the context of the business world, companies can consider those assets that directly contribute to their running to be part of their Critical Infrastructure.

Due to any Critical Infrastructure’s influence in many areas crucial to the development of the country, Yusta et al. (2011) affirmed that a country’s economic and social development cannot move forward or prosper if their operation is vulnerable to distortion. This way, the network of Critical Infrastructure in a country can be seen as a socio-economic component that keeps the livelihood of a country in constant motion.
Any failure in this network could bring about great change in both the economical standing of the country and the well-being of its resident population.

According to Yusta et al. (2011), a country’s national economic policy strategy should include a set of concise and defining policies that aim to promote the creation of a reliable and integrated Critical Infrastructure network. The set of policies stated in these strategies should cover all spectrums from which the infrastructure should be evaluated, including thorough elaboration in aspects that would range from infrastructure input-output integration to systems’ security needing to be analysed.

As Critical Infrastructure spans across areas that directly affect the well-being of a country’s populations, Popescu and Simions (2011) stated that the identification of which infrastructures should be deemed critical is of great concern due to the possible loss of life that could result from the damage to these. Therefore, an analysis of all the different infrastructures should be carried out using a set criterion that can help identify which of these are actually critical or crucial in the context or nature of their use.

Regardless of their physical or virtual nature, some of the areas which could be heavily and significantly impacted by the destruction and/or disruption of Critical Infrastructure are the following (Popescu & Simions, 2011):

- Social functions;
- Health;
- Safety;
- Security;
- Economy;
- Social well-being.

The abovementioned areas may not necessarily be affected individually, but the disruption or destruction of Critical Infrastructure can negatively impact a combination of these. For that reason, it is evident that before a Critical Infrastructure strategy can be put into effect, the interconnections and dependencies present between the different
infrastructures need to be studied and understood on an appropriate level. The next section briefly looks into the dependencies found between Critical Infrastructures in different areas of use.

2.3 – Critical Infrastructure Interdependencies

Interpretive Structural Modelling (ISM) is a methodology used to analyse complex interactions and dependencies of different components in a complex system. Figure 2.1 shows the relationships between different Critical Infrastructures identified by Han, Liu and Rong (2009) through the use of the ISM methodology.

Figure 2.1 – Interpretive Structural Modelling (Han et al., 2009)

Figure 2.1 places each of the Critical Infrastructure components in a hierarchy. Electric power infrastructure is placed at the bottom of the hierarchy as a support Critical Infrastructure that interacts with others on the same level of the hierarchy. The interdependencies between the different infrastructures show that a breakdown in at least one of them could throw the others out of balance.

Although the electric power infrastructure is, at a minimum, connected to the: information and communication; water supply system; and bank and finance Critical Infrastructures; this dissertation will only focus on its protection using the multi-agent model. It will focus on the power infrastructure effectiveness by monitoring the
information transfers between each of the nodes of the electric power network in an effort to enhance its security.

The connections shown in Figure 2.1, although crucial in illustrating the main concept of Critical Infrastructure dependency, are, to a certain point, simplistic. This is because if all possible Critical Infrastructures, their relationships and interdependencies were to be shown; the diagram could grow into a rather large network diagram. One needs to remember that the interdependencies between these systems can be logical, physical, geographic or cybernetic (Rinaldi, Peerenboom & Kelly, 2001). Therefore the connection between two infrastructures could be more complex than expected if interdependencies are further investigated.

The high level of interconnectivity evident in a network of Critical Infrastructures shows that possible failures in one component of the network could cause several other components to fail. According to Kalam, Deswarte, Baïna and Kaâniche (2009); the interdependencies between the infrastructures in a country increase the possibility of cascading and escalating failures if one component of the network ceases to function for any possible reason. Kalam et al. (2009) define cascading and escalating failures as follows:

- **Cascading Failure:**
  This occurs when a failure in one infrastructure causes the failure of one or more components in a second infrastructure.

- **Escalating Failure:**
  This is a failure in one infrastructure that is exacerbated by an independent failure in another infrastructure, generally in the form of increased severity, recovery time or restoration time coinciding with the first failure.

Critical Infrastructures face not only security issues that may hamper their ability to function efficiently to serve society, but also have to contend with other issues that could come from the inefficient management of the resources used. It is often found that Critical Infrastructure working to the benefit of a country’s society may not be completely
owned and managed by the country’s governmental institutions (Eckert, 2005). The following section briefly discusses this point.

2.4 – Management and Ownership of Critical Infrastructures

Critical Infrastructures, such as hydroelectric dams, are often used by developed and developing countries as a source of income. An example of this is Mozambique’s Cahora Bassa hydroelectric dam, where the electricity generated is not only used by Mozambique itself, but also sold to neighbouring countries, namely South Africa and Zimbabwe (Sebitose & Graça, 2009).

Apart from providing services that enhance the standards of living of the countries in which they are located, these infrastructures are also important because of the possible economic gain they can provide for the countries or states that own them. The public and private sectors have, on many occasions, cooperated in the provision of critical functions or services that benefit the nation.

The cooperation between the public and private sectors is mainly driven by the need for assets that can only be found in the private sector (Eckert, 2005). It is therefore seen as a much more cost-effective option to create partnerships with the private sector to get access to these assets in order to provide services. According to Hellstrom (2007), the public sector entity, or the government, is present in the partnership to protect the public and ensure that an appropriate level of service delivery is provided by the private companies who are entrusted to provide the necessary technologies and or operations to them.

Eichler, Auxila and Pollock (2001) define public-private partnerships as: “A contractual arrangement between a public sector institution and a private party in which the private party performs an institutional function or uses state assets and assumes substantial financial, technical and operational risks in the design, financing, building and/or operation of the project, in return for a benefit”. The contractual arrangement set up by
the public sector entity serves as a service level agreement where all aspects of the provided service are explicitly stated and rules are set as to how the assets (from either the private or the public entity) will be used.

The contract agreed upon in public-private partnerships also aims to set the performance targets that will improve service delivery. Shuping and Kabane (2008) listed the following as some of the objectives public-private partnerships attempt to achieve:

- The public sector is able to leverage private finance to strengthen the public sector;
- The sharing of scarce resources between the sectors maximises benefits for the broader population;
- There is an improvement in the quality of services rendered;
- This partnership promotes an equitable allocation of resources.

The services provided by Critical Infrastructure tend to be very costly to realise. The provision of these services consume a lot of resources (both labour and natural) that have to either be sourced within the boundaries of the country, or be outsourced from other nations that possess them in abundance. All these complexities place a great burden on a country’s government to provide these services efficiently in a cost-effective manner. For this reason, the control of many Critical Infrastructures, in both developed and developing countries, has been shifted to the private sector (Auerswald, Branscomb, La Porte & Michel-Kerjan, 2005).

The move to privatisation of Critical Infrastructures has been a bid to improve service provision and to increase investment in infrastructure development. Increased investment and management of this infrastructure can improve the well-being and social standing of the country. The private sector can be seen as a catalyst for economic development with its access to investment capital and its profit-driven motivation.

Full privatisation, though, is not what is currently implemented, as some control still needs to be under the control of a fair governing body in order to protect society from
monopolistic behaviour and exploitation. Thus, public-private partnerships have become essential to the running of Critical Infrastructures.

2.5 – Critical Infrastructure Protection

Disturbances in the economic and social stability of a nation that have resulted from the vulnerabilities in the country’s infrastructure have opened discussions regarding new ways of protecting a country’s key resources. The efforts exerted in the creation of security enhancing methods and policies resulted in the research field named ‘Critical Infrastructure Protection’ (CIP). According to Murray and Grusbesic (2011), security efforts in Critical Infrastructure require a large amount of investment from the responsible entity, with some of these investments often geared towards:

- Upgrading structural facilities of the infrastructure;
- Hiring human resources to protect the infrastructure;
- Developing software components to detect and prevent attacks against the infrastructure.

According to Hellstrom (2007), the US National Strategy for the Physical Protection of Critical Infrastructures and Key Assets of 2003 named three types of effects that could indicate the vulnerability of a Critical Infrastructure system. These are:

- Direct infrastructure effects;
- Indirect infrastructure effects;
- Exploitation of infrastructure.

One of the characteristics of developing countries is the construction of many new infrastructures that aid in the improvement of the country’s economy. Over time, and after significant consecutive monetary investments, these infrastructures evolve to provide an increasing number of services. This way, the evolution of these infrastructures – in terms of service provision, complexity and interconnectivity with other infrastructures – could turn them into a critical component in the infrastructure network of a country. It then, however, becomes difficult to assess the vulnerabilities
these developing infrastructures face as one cannot tell in advance what problems the evolution will bring.

Chunlei, Lan and Yiqi (2011) reported that, because of Critical Infrastructure interdependencies and the high chance of occurrence for cascading and escalating failures; nations have begun to stipulate national strategies to mitigate against the risks of failures in the Critical Infrastructure networks. Many research projects have been funded by entities, such as the government of the United States of America, to uncover the security risks inherent in their Critical Infrastructure systems (Hu, Pota & Guo, 2014).

2.6 – Conclusion

Due to their contribution towards national stability, Critical Infrastructure is a field of research where content constantly needs to be updated with the aim of finding out how best to improve the services they provide and how to maintain their operation in a safe and reliable manner. Critical Infrastructures play a major role in the standard of living of populations around the world.

Thus their performance reflects how well the country is doing in terms of human and economic development. For this reason, developing and developed countries have put in a lot of effort in improving their Critical Infrastructures.

As Critical Infrastructures are, for the most part, inextricably linked, and the downfall in one sector can spread to others, causing a wide array of the country’s critical services to shut down; their protection becomes vitally important.

This dissertation aims at investigating and enhancing the protection of the systems used in Critical Infrastructure. Therefore, the next chapter is devoted to the field of Critical Information Infrastructure protection, and shall discuss the existing risks Critical
Infrastructures endure, and the methods that have been established to attempt to mitigate such risks.
Chapter 3
Critical Information Infrastructure Protection

Chapter 1: Introduction
Chapter 2: Critical Infrastructure
Chapter 4: The Smart Grid
Chapter 5: The Smart Grid as a Critical Infrastructure
Chapter 6: Software Agents
Chapter 7: Intelligence Enabling Machine Learning Models
Chapter 8: Intelligent Agents and Complex Adaptive Systems
Chapter 9: Agent Technology and Critical Information Infrastructure Protection
Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS)
Chapter 11: MA-SGS: Node Agents
Chapter 12: MA-SGS: Process Monitoring Agent
Chapter 13: MA-SGS: Security Response Agent Structure
Chapter 14: MA-SGS: Interoperability Agent Structure
Chapter 15: MA-SGS: Attack Agent Structure
Chapter 16: MA-SGS: Smart Grid Simulation & Model Implementation
Chapter 17: MA-SGS: Model Results
Chapter 18: Conclusion
3.1 – Introduction

As with most other modern day systems, technology has been a major driver in the efficient provisioning of crucial services in Critical Infrastructure. In energy resources infrastructure, for example, information systems are used to monitor the demand for electricity, rerouting electrical power to areas where demand is the highest and cutting electricity provision when generators reach maximum capacity.

As briefly mentioned earlier, such information systems used to manage Critical Infrastructures are known as “Critical Information Infrastructure Systems” and their failure to function can bring about grave disruptions to critical services provisioning that lead to destabilising a country’s society and economy (Ten, Manimaran & Liu, 2010). The protection of such highly networked systems is therefore seen as being of the utmost importance for a country.

The development of security mechanisms and methodologies designed for the protection of Critical Information Systems has been the topic of numerous research projects and heated debates, mainly due to the weight of importance behind safeguarding a country’s most important resources and services. According to Ten et al., Critical Infrastructures are based on both technology and the Internet, and are physically complex (2010).

The current chapter is devoted to discussing the concepts that have to be taken into account when considering the protection of Critical Infrastructure. The chapter begins by discussing Critical Information Infrastructure and looking at what threats such systems are vulnerable to and how efforts have been made to protect them and the physical systems that such computer systems manage.
3.2 – Critical Information Infrastructure

Technology has mostly been present as a support system to tasks being carried out in most areas where it is applied. As an example, before the massive utilisation of technology, information processing activities in organisations such as banks had to be done manually. The approval of loan applications required the use of many analysts to go through all available financial records in order to accept or reject candidates (Norris, 2000). The manual processing of data is quite costly in terms of time and financial resources. Thus, technology has been widely used to create systems that automate these functions, greatly reducing most costs in areas where human resources are needed.

The use of real time information is key in the provision of services in Critical Infrastructure. Therefore, Critical Information Infrastructures provide the layer which allows the effective and efficient control of Critical Infrastructure. These computer aided systems collect information using a wide array of sensors from all spectrums involved in the provision of an infrastructure’s services.

Such Critical Infrastructure Information Systems also monitor the values they collect in real time in order to carry out analysis processes that help decision configuration control systems keep the Critical Infrastructure stable. The following is a list of the most commonly used Critical Information Infrastructure Systems (Coutinho, Lambert-Torres, da Silva, Martins, Lazarek & Neto, 2009):

- Supervisory Control and Data Acquisition Systems (SCADA);
- Energy Management Systems (EMS);
- Process Control Systems (PCS);
- Distribution Management Systems (DMS).

Critical Information Infrastructures around the world have been the victim of several cyber-criminals. Their complex mechanisms have been threatened by criminals in an attempt to disrupt their functions. With the advancement of technology, current cyber-
attacks have become much more sophisticated and pervasive (Choo, 2010), with both attack frequency and the severity thereof on the increase.

The use of technology and the social status of a country, in terms of its economy and human development index (HDI), seem to have a positive relationship, because developed countries tend to depend on the reliability of technology in the running of some of their most important systems. Developed countries, such as Australia and the United States, place computers and network-based systems either directly in the management of their Critical Infrastructures, or as the key components that allow their Critical Infrastructures to function (NIAC, 2004).

The increased dependency on network-based systems and other information and communication technologies has been due to their ability to improve productivity and efficiency. According to Choo (2010), the use of technology has not only brought about ‘faster communication capabilities and immeasurable convenience’ in the running of Critical Infrastructures, but also opened doors for the possible criminal exploitation of these systems.

Critical Information Infrastructures (CII) are the systems used to run and manage the infrastructures that contribute to the social well-being and economic stability of a country. These systems are composed of complex networks used for the communication and coordination of activities between the different physical components that make up the entire infrastructure. The interdependency of Critical Infrastructures often arises from the sharing of critical information, therefore creating the possibility of cascading failures.

Apart from their own purposeful computer networks, CII systems also make use of the Internet as a communication or information gathering medium. This poses a certain degree of vulnerability to the stability of the systems as the threat posed by criminals on the Internet also increases. Hacktivist and terrorist groups could use the inherent
security issues on the Internet as a gateway to infiltrate and compromise Critical Information Infrastructure Systems.

Sommerville (2008) defined safety-critical systems as those where “it is essential that system operation is always safe; that is, the system should never damage people or the system’s environment even if the system fails”. Systems that help in the running of hospitals can be deemed ‘safety-critical’ as their failure could cause the loss of lives. The systems running on a hospital’s premises can be classified as part of its Critical Information Infrastructure.

Safety-critical systems cannot be limited to those used in healthcare facilities alone, as infrastructures such as power utility stations and gas stations also make use of systems whose failure could eventually lead to life-threatening situations. From this observation, Critical Information Infrastructures can be classified as safety-critical systems that need to be protected at all costs.

There have therefore been extensive efforts to enhance the protection of systems running within Critical Infrastructures. These have, in turn, given rise to immense research conducted in the field, which has been labelled ‘Critical Information Infrastructure Protection’ (CIIP). The following section is devoted to CIIP and some of the main concepts pertaining to it when securing Critical Infrastructure.

### 3.3 – Critical Information Infrastructure Protection

In our modern era, the number of security issues over the use of Internet technologies has sky-rocketed from what they used to be in the past when most people only concentrated on the Internet’s benefits rather than dangers. Furnell & Warren (1999) state that while technology provides several benefits, it also exposes vulnerabilities, which are often exploited by hackers. The growing awareness of all potential uses of the Internet is what has caused threats to be taken into consideration.
Convenience appears to be one of the biggest drivers of the development of new technologies. According to Prothero (2001), using technology for increasing convenience has created a general tendency for the embracing of very powerful tools without proper consideration of any of the possible safety concerns.

The use of newly developed technology, even without proper understanding and control, shadows the possibility of such technology also possibly being a tool for creating disruptions. Only after the technology is better understood and controlled, are security measures developed for its use. Prothero (2001) named the delay time between the embracing of technologies and the development of security measures as the ‘convenience overshoot’.

A threat can be defined as a source of danger or as a sign of something dangerous or unpleasant which may be about to happen (Ciampa, 2014). By being on the Internet, individuals and organisations expose themselves to numerous possible threats. In Sophos’ 2011 report, it was uncovered that 95 000 new malware pieces, on regular computer devices, were analysed, on a daily basis, by their laboratories in 2010 (SophosLabs, 2010). Four years later, Sophos’ 2014 Threat Report observed, over the previous year alone, 350 000 new malware pieces on mobile platforms (SophosLabs, 2013). Over the years, information security threats driven by cybercrime have drastically increased in sophistication.

Before the adoption of networking technologies and the Internet in business, organisations’ security policies focused more on the direct unauthorised access to their computer systems. Theoharidou, Kokolakis, Karyda and Kiountouzis (2005) refer to this type of threat as the ‘insider threat’, where people with access rights violate the security policies of their organisations. Now hackers can remotely break into computer systems or can deploy viruses that autonomously collect critical information about individuals and organisations on the Internet (Benjamin & Chen, 2012).
As a method of adding security to their systems, organisations often use the ‘security through obscurity’ method where the different components of their systems are obfuscated (Edwards, 2014). Obfuscation is performed on the code embedded in components in order to produce one that is much more challenging to understand and replicate (Collberg & Thomborson, 2002). In this method, security is essentially implemented by hiding how systems are designed, as well as the algorithms and methods they use for the functions they possess. Here, security is dependent on the confidentiality of the software solution itself (Yu & Brune, 2011).

Using an authentication scenario as an example, security through obscurity could be implemented by masking the exact algorithms used for hashing passwords, and not making the name of such algorithms public knowledge as a bid to increase security. However, to some, such a method of ensuring security amounts to having no security at all and these parties advocate that such practices should not be used at all (Stuttard, 2005). Although Stuttard (2005) goes on to mention that instead of using ‘security by obscurity’ as a main measure of security, it should rather be used as an additional layer of security. This is where a software solution is, by its own design, able to be resilient, reliable and secure. By extension, by adding confidentiality to how components were designed and developed, the degree of its security is enhanced.

Section 85 of the South African Electronic Communications and Transactions (ECT) Act defines cybercrimes as “the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorized to access that data and still continues to access that data” (Gereda, 2003).

To summarise, the ECT Act’s definition of cybercrime can be described as the carrying out of criminal activities that threaten the stability and integrity of computer systems used by organisations. These activities, usually initiated by those termed ‘black hat hackers’ and by malicious groups, target vital systems with goals that range from stealing important information to causing a shutdown of the system.
The following section briefly discusses some of the considerations taken into account when defining standards and policies for information security in Critical Information Infrastructure.

### 3.3.1 – Security standards and policies

In all aspects pertaining to information security in any computer system, three important terms that explain the importance of security measures need to be discussed. These three crucial aspects are confidentiality, integrity and availability (CIA) of data in information systems, which must always be maintained if the system is to continue working in a reliable manner, or if it is to continue fulfilling the purpose for which it was made (Zhang, Zhao & Chen, 2010).

Therefore every information security strategy must always include policies and mechanisms that will protect information systems against threats and risks that may damage the confidentiality, integrity and availability of information assets. Choo, explained the three terms as follows (2010):

- **Data Confidentiality:**
  
  The disclosure of data is only to be given to authorised users or systems.

- **Data Integrity:**
  
  The modification of data is only to be allowed by authorised users or systems and the traceability of these changes is to be evident.

- **Data Availability:**
  
  The accessibility property of data is only afforded to authorised users or systems, when the need for the data arises.

Although there are counter-measures to improving information security measures, there are still many threats to the integrity, confidentiality and availability of organisational data (Workman, Bommer & Straub, 2008). Motivated by the possible financial benefits, hackers continuously devise new methods of gathering critical private information on the Internet. This information may be email addresses, passwords, credit card numbers etc.
Others create malicious software that aims at destabilising systems in a company in order to either stop their services or to steal important data.

Developed countries have realised the importance of Critical Information Infrastructure protection as a field that constantly requires updated policies and regulations (Auerswald, Branscomb, La Porte & Michel-Kerjan, 2005). Therefore, in order to boost research in the field, they have established formal commissions, departments and long-term programmes with the goal of formulating new policies that will help increase the security of the country’s Critical Infrastructure. Table 3.1 lists some of the established commissions and the regions for which they are responsible.

**Table 3.1 – Countries and Critical Infrastructure Legislation (Brömmelhörster, Fabry & Wirtz, 2004)**

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Commission(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Africa</td>
<td>State Information Technology Agency</td>
</tr>
<tr>
<td>European Union</td>
<td>European Programme for Critical Infrastructure Protection</td>
</tr>
<tr>
<td>United States</td>
<td>Presidential Commission on Critical Infrastructure Protection; Department of Homeland Security; Department of Defense; National Infrastructure Protection Centre</td>
</tr>
<tr>
<td>Australia</td>
<td>Critical Infrastructure Protection Group; National Guidelines for Protecting Critical Infrastructure from Terrorism</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>National Infrastructure Security Coordination Centre; Information Assurance Council</td>
</tr>
<tr>
<td>Switzerland</td>
<td>The Swiss Department for Defence, Civil Defense and Sport</td>
</tr>
<tr>
<td>Sweden</td>
<td>Swedish Emergency Management Agency</td>
</tr>
</tbody>
</table>

All commissions and programmes mentioned in Table 3.1 are necessary to help a country build capacity in the implementation of security measures for their Critical Infrastructure. When looking at the security requirements of any information system, elements that work with confidentiality, integrity and availability should also be studied. Such elements are quintessential to the five pillars of information security and are the topic of discussion of the following subsection.
3.3.2 – The five pillars of information security

In all aspects pertaining to the security of information and processes available in computer systems, five basic concepts or principles were set in order to ensure and evaluate the information security efforts put in place by organisations. These principles also hold in the field of Critical Information Infrastructure protection by providing the pillars under which all system security efforts are evaluated. The five pillars that are critical to information security efforts are listed below (Wilson, 2013):

- **Identification and authentication:**
  This involves the ability of a system to properly identify each of its users, and authenticate each by using a challenge to which only a genuine user will be able to respond.

- **Confidentiality:**
  As mentioned previously, the system should be able to protect against unauthorised disclosure of information kept or produced by the system.

- **Integrity:**
  The system should also be able to protect against the tampering of data kept or produced by the system.

- **Non-repudiation:**
  This involves the ability of the system to always provide a proof of origin for every transaction it processes. This enables one to trace down the initiators of actions performed on a system in a manner that cannot be denied.

- **Availability:**
  The system needs to be able to provide the necessary functionality and data to those who rightfully use it when such operations are requested. Therefore the system must be resilient to actions that threaten to bring it down.

Such pillars for information security are not only applied to the information managed by the Critical Infrastructure Information Systems. Since such systems also manage the hardware used in the Critical Infrastructure, these should also be looked at in order to
determine how threats can affect the Critical Infrastructure hardware. The following section discusses the cyber-to-physical link of cyber-attacks in Critical Infrastructure.

### 3.4 – Cyber-To-Physical (C2P) Link of Cyber-Attacks

Rajkumar, Lee, Sha & Stankovic (2010) define cyber-physical systems as “physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core”. Such information systems use networking technologies to control and monitor the operation of machinery to achieve a specific goal. Most of the modern Critical Infrastructure Information Systems (i.e. the cyber component) use a wide array of electronic sensors (i.e. the physical component) to constantly collect information (Hawrylak, Haney, Papa & Hale, 2012).

The inherent nature of most Critical Infrastructures involves the interaction of networked computer systems with the hardware necessary to work at the Critical Infrastructure installation. Reliability and availability in Critical Infrastructures is enabled by the use of intelligent software executing algorithms for the monitoring of the distributed components (Lin, Sedigh & Hurson, 2011). Through the rules and intelligence built into the Critical Information Infrastructure, the physical infrastructure and all its components can be controlled in a more consistent manner.

Critical Information Infrastructure Systems therefore create a cyber-to-physical link in Critical Infrastructure. The security of such systems has been highlighted as a primary concern as successful attacks against them can cause a sequence of events that can prove to be disastrous (Xie, Lu, Guo, Liu, Peng & Gao, 2013).

The cyber-to-physical link in Critical Infrastructure gives rise to a pathway for attacks referred to as a cyber-to-physical bridge which exposes some of the vulnerabilities created by the combination of cyber and physical systems (Stamp, McIntire & Ricardson, 2009). As the systems in the different Critical Infrastructures are also connected, any breach in these systems could allow perpetrators to remotely control the
physical components of the infrastructure in order to cause harm or simply disrupt services. Figure 3.1 illustrates the cyber-to-physical bridge in an electrical power grid environment.

![Figure 3.1 – The Cyber-To-Physical Bridge of Attacks in CII (Stamp et al., 2009)](image)

The attack vector in Figure 3.1 represents all combinations of cyber-attacks that a Critical Infrastructure such as the power grid could face. Such attacks could cause some form of noticeable outcome that directly leads to the physical result of disruptions. According to Stamp et al. (2009), these disruptions could lead to a grid-wide effect that strains the power grid’s functioning (e.g. reduction in grid capacity, equipment damage, loss of electricity, safety threats etc.). In order to effectively protect Critical Infrastructure, one also needs to understand the possible effects that cyber-attacks may have on the physical components of the infrastructure.

### 3.5 – Conclusion

If a nation is to prosper, it needs to have a properly functioning set of Critical Infrastructures. Thus, if a country’s Critical Infrastructure is to continue working efficiently, it needs to be properly managed by its interested parties, and properly secured against threats it faces.

Due to the vulnerabilities existing in the information systems running in Critical Infrastructure, research and development in the field of Critical Information Infrastructure protection is deemed very important. Such attacks may go beyond violating the confidentiality of information to creating much more life-threatening situations due to the cyber-to-physical link existent between all the information systems.
Attacks on Critical Information Infrastructures are carried out on a daily basis, therefore the development of new methods to enhance security while maintaining all security standards is of the utmost importance when dealing with these systems.

In closing, the current chapter was included in the dissertation to briefly discuss the security considerations examined in Critical Information Infrastructures. The dissertation will mainly focus on the smart grid as a Critical Infrastructure that needs to be secured. The next chapter is devoted to introducing the smart grid.
4.1 – Introduction

When considering all the contributions that have advanced the development of society in the modern era, one could argue that the harnessing of electric power is the most important. Without electricity, most of the discoveries made today would have not been possible. Its ability to power most tools used to facilitate everyday life has made electrical power one of society’s most basic needs. From this point of view, electricity, in its purest essence, can be seen to be an invaluable commodity to humans.

As is the case after their discovery and application in any specific field, all commodities are deemed to be of value and are therefore traded as primary materials used to meet a specific end (Radetzki, 2010). The trading of electricity as a commodity occurs between electric utility companies and the clients in the regions these companies serve. Electric utility companies (either private or government owned) are responsible for the generation, transmission and distribution of the electricity that they provide.

Electric power utility companies set up the infrastructure used for the transfer of electrical energy from power plants, which can also be either private or government owned, down to electrical substations, which, in turn, direct the electricity to the consumers in the electricity market. Consumers can range from private households to large business premises in any given region. This infrastructure is usually referred to as a ‘power grid’.

Wherever the power grid serves, the entities receiving the most focus are the consumers. As seen in Figure 4.1, the goal of a power system is to deliver energy to consumers in an affordable, reliable and sustainable manner (Slootweg, Cordova, Portela & Morren, 2011). Therefore all developments in the power grid aim to satisfy these three goals. Every development must improve the affordability of producing and consuming power. Affordability needs to be coupled with reliability for the consumer to be able to trust the provision of electric power. Electric power should still be provided
using sustainable technologies that are environmentally friendly, and long lasting. The following section describes the power grid and all its components.

**4.2 – The Power Grid**

Yan, Zhou, Deng and Huang (2011) defined the power grid as ‘a complex wide area network system that contains complex electric components’. The main components that form the power grid are shown in Figure 4.2. The components are discussed in subsection 4.2.1.
4.2.1 – Power Grid Essentials

An entire power grid could be managed by one or more companies operating in a specific region’s electricity market (Blumsack, 2007). The same power grid could also be extended to concurrently serve multiple electricity markets. Regardless of the regions to which the power grid must provide a stable power supply, it is a prerequisite that they have all the elements illustrated in Figure 4.2. The following subsections explain some of the essential aspects of each of the components necessary to form a power grid.

4.2.1.1 – Generation

The generation of electricity is located at the highest level of the grid, and can be viewed to have a basic tree structure, even though the production of electricity does not necessarily occur at a single point in the entire grid. The flow of electricity, from its generation to eventual consumption, starts off from the power plants producing large volumes of electricity. This is then sent over to high voltage (HV) power grids to be fed to the necessary end-consumers (Bialek, 1996).

A power grid can be powered by a variety of sources and/or different power plants that generate electricity using a variety of methods. The power stations illustrated in Figure 4.2 essentially take their role in the grid as power generators, and could be generating power using different methods.

Most power plants produce electricity from the combustion of fossil fuels such as natural gas and coal (Sieminski, 2013). Some power plants make use of other more readily available natural resources such as wind power, solar energy and hydro power. These non-combustible and renewable sources of electricity have a far less damaging effect on the environment. For this reason, research has currently been focused on finding more efficient ways to generate power (Blaabjerg, Teodorescu, Liserre & Timbus, 2006).
Given this drive to generate power in more efficient and environmentally friendly ways, the power grid has been going through constant changes in order to correctly integrate all new methods (Suryanarayanan, Ribeiro & Simoes, 2010). With all new technology, comes the need to correctly control and monitor its usage in order to evaluate its potential for long-term use. Information systems are developed to help monitor the progress of the new developments for power generation in order to check if they are achieving their set goals, while maintaining, if not improving, the power grid as a whole. Research on information systems goes hand-in-hand with the new developments that are made to the power grid.

4.2.1.2 – Transmission

Electric power transmission from the power plants is achieved through a combination of electric power substations, transformers and transmission lines (Brown & Sedano, 2004). The transmission process takes place on high voltage grids, which, in turn, transfer the electricity through to medium and low voltage grids. This generally takes place across long distances as these grids are often located away from demand centres but much closer to the power plants from which they receive all the electricity. A demand centre is the component of the power grid which uses the generated electricity from power plants. Demand centres are composed of the electric power consumers in the power grid.

A single transmission grid could be responsible for feeding one or more demand centre’s electricity distribution grid. The main task of the transmission network is to lower the voltage of the electricity it receives directly from power stations in order to make it compatible with the power consumption devices used by consumers. If power was not converted from high to lower voltage, it would put pressure on the existing infrastructure existent in the demand centres (Brown & Sedano, 2004).
4.2.1.3 – Distribution

The electricity distribution network is the last layer through which electricity flows before it reaches its end-consumer or demand centre. These networks are usually of low voltage, using transformers to increase the volume of electricity depending on the needs of the demand centre they serve. Table 4.1 lists the components found in the electricity distribution network.

Table 4.1 – Electricity Distribution Network Components (Liu et al., 2009)

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformers</td>
<td>Devices used to either reduce or increase the voltage of an alternating current.</td>
</tr>
<tr>
<td>Power lines</td>
<td>Cables used to transport electrical power from one point to another.</td>
</tr>
<tr>
<td>Substations</td>
<td>Stations used to reduce the voltage of the electrical power that is received from power transmission stations in order to make it usable by consumers.</td>
</tr>
<tr>
<td>Meters</td>
<td>Devices used to measure the amount of electricity consumed by customers at demand centres.</td>
</tr>
</tbody>
</table>

Distribution networks may be fed electricity from one or more transmission networks, depending on demand centre needs. Alternatively, economic or environmental concerns may determine a particular distribution network’s source.

4.2.1.4 – Customers

Customers in the electricity market range from individual households to large companies and all their business offices and warehouses. Each customer entity has different consumption patterns based on its specific needs. For example, family households would naturally consume less electricity than a company that specialises in the cold storage of products.
The consumption of electricity is what determines how much electricity is produced during any specific time. As storing electricity is not a very efficient and cost-effective process, utilities try to match the supply of electricity at the same level of demand (Guo & Fang, 2013). For example, in residential areas, more electricity is used during the afternoon as most people are home from work and use electric appliances, thus increasing the demand. In order to respond to this demand, power plants generate more electricity, whereas industrial and some commercial areas are shown to have increased electricity consumption loads during weekdays (Jardini, Tahan, Gouvea, Ahn & Figueiredo, 2000).

In order to continuously monitor all the different components of the power grid to ensure that the grid works in both an efficient and secure manner, multiple information processing systems are used to monitor its operational health. These power grid information systems are briefly discussed in section 4.2.2.

4.2.2 – Power Grid Control Information Systems

As with every Critical Infrastructure, control is of the utmost importance if it is to keep its functions and services available for the benefit of society. The power grid is treated no differently as a myriad of information systems are put in place to: control the generation of power, the demand for electricity, the load of electricity at any point across the entire grid, and the functioning of substations and transformers (Slootweg et al., 2011).

Since a considerable amount of information is generated and processed in the entire power grid, networked information systems are deployed across the grid in order to keep control of any events occurring at any point in time.

A detection of increased electricity consumption from a demand centre would lead to a chain of information transfer events reaching the supplying power stations in order to increase the production of electricity. This information transfer process would need to be executed at high speed in order to keep the supply of power constant and to avoid the
difference between demand and supply of power (Barnes, Johnson & Nickelson, 2004). Table 4.2 lists a few examples of systems found in the electric power grid.

Table 4.2 – Information Systems in the Power Grid (Barnes et al., 2004)

<table>
<thead>
<tr>
<th>Information System</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisory Control and Data Acquisition (SCADA)</td>
<td>An industrial control system used to monitor remote units that gather performance data in a network.</td>
</tr>
<tr>
<td>Energy Management System (EMS)</td>
<td>Information systems used by electrical power utility companies in order to monitor and control the flow of electricity.</td>
</tr>
<tr>
<td>Distribution Management System (DMS)</td>
<td>Information systems used in electric energy distribution networks to make sure electric power is delivered in an efficient, safe and reliable manner.</td>
</tr>
<tr>
<td>Process Control Systems (PCS)</td>
<td>A set of information systems used to monitor and control industrial grade management systems.</td>
</tr>
</tbody>
</table>

The information systems described in Table 4.2 form an important part of the power grid’s setup. When describing the power grid, the set of technologies and information systems used to better monitor and control the power grid only form one part or one layer of the entire network.

Coutinho, Lambert-Torres, da Silva, Martins, Lazarek & Neto (2009) separated the power grid into three different, yet highly connected and inextricably linked layers as shown in Figure 4.3. The identified layers can be described as follows:

- **Physical Layer:**
  The physical layer is made up of all the assets used in the production, transmission and distribution of electricity (Coutinho et al., 2009). It is basically the layer where all its components aid in the provision of the electricity commodity that is then used in the demand markets.
• **Cyber Layer:**
  All information systems described in Table 4.2 belong to the cyber layer. They are used to monitor and manage the processes involved in the generation and consumption of the electricity, which occur in the physical layer (Coutinho et al., 2009).

• **Operational Layer:**
  As the electricity is basically traded and used as a commodity provided by a company, the operational layer introduces all the business management activities involved in the management of electric power distribution. The operational layer is also where one finds the operators who are responsible for using the information systems in the cyber layer in order to ensure the power grid runs in a safe and reliable manner (Coutinho et al., 2009).

Although, the structure of the power grid has proven to work for society from its inception, modern technology and a very large focus on the environment demanding efficient usage of resources in the 21st century has put a strain on the regular power grid technologies used (Khattak, Mahmud & Khan, 2012). Such trends have pushed for change in the way electricity generation, distribution and consumption are viewed.

The focus on alternative methods of generating electricity that are more sustainable and less damaging to the environment, coupled with the drive for more efficient use of electricity; has created the need for the development of a power grid where these objectives are taken into account (Green, Wang and Alam, 2013). In order to achieve this, the use of information communication technologies (ICTs) was deemed to be of crucial importance. Therefore through the wide application of ICTs across the regular power grid, the ‘smart grid’ concept was created. The following section will go on to describe the smart grid.
Figure 4.3 – Power System Control Centre Interactions (Coutinho et al., 2009)
4.3 – The Smart Grid

The smart grid has been considered by researchers to be the evolution of the regular power grid (Singhal & Saxena, 2012). It is an evolution that has brought about many changes that fit the concerns of modern society. Some of these concerns existed before the smart grid, but they are perceived to be better dealt with through the use of a power grid that makes use of advanced information technology, enabling intelligent decisions to be made during energy generation and delivery.

Advances in technology have added a component for high-level information processing into the electric power grid in an effort to better manage energy resources, provide better control of electricity usage, reduce the environmental impact of electricity usage and, among other benefits, reduce the costs of electricity to the consumers.

As illustrated in Figure 4.4, the addition of the information processing layer to the traditional electrical power grid has created what is called a 'smart grid' that Fang, Misra, Xue and Yang (2012) have stated is 'an enhancement of the 20th century power grid'.

![Figure 4.4 – Basic Composition of the Smart Grid](image-url)
Section 4.3 begins by defining the smart grid, before outlining what the objectives of its development are and how research and implementation efforts have advanced the concept. The underlying information processing infrastructure requirements will now be discussed in order to explain the information technology foundations that allow the smart grid to exist. As is with every technology that deals with many stakeholders, standards have to be put in place in order to govern and regulate its usage. These standards are briefly outlined and discussed at the end of the section.

4.3.1 – Definition

Although many have realised the need for an intelligent power grid, and its implementation has already begun in different parts of the world, there is still no single definition that every entity uses to describe the smart grid. The United States, the European Union countries, the Republic of China, South Korea and Canada are some of the players in the field of smart grid research and implementation (Gungor, Sahin, Kocak, Ergut, Buccella, Cecati & Hancke, 2011).

The following are definitions used to describe the smart grid:

**US Department of Energy (Veldman, Slootweg, Van der Meijden, Knigge, 2011):**

“A smart grid is the electricity delivery system (from point of generation to point of consumption) integrated with communications and information technology for enhanced grid operations, customer services, and environmental benefits.”

**European Technology Platform for the Electricity Networks of the Future (CEER/ERGEG, 2011):**

“A smart grid is an electricity platform that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.”
The definitions of the smart grid, although worded differently, attempt to convey the same message and express the same goals. Both define the smart grid around the generation and consumption of electricity and the use of information communication technologies in order to enhance all provided services in a reliable manner, while taking into account the environmental impact of electricity usage.

Taking the shared aspects of the definitions into account, one could still investigate what some of the main objectives of implementing a smart grid are in more specific terms. Section 4.3.2 looks at some of the objectives envisaged to be reached through the smart grid initiative.

4.3.2 – Objectives of the Smart Grid

According to Hashmi, Hanninen & Maki (2011), implementation projects across Europe aim towards creating greater reliability in the operation of power grids (through the increased degree of interaction between operators and consumers) and to improve the efficiency of energy usage. These objectives also go hand-in-hand with the increased focus on the environmental impact of electricity generation and usage. The environment has been a driver of a lot of research conducted to make the smart grid a much more vivid and realistic concept.

The vision of an improved power grid deemed to be fit for the modern 21st century lifestyle is based on a set of properties that the smart grid has to achieve for it to be considered successful. According to the US Department of Energy’s vision, the smart grid can be defined by a list of characteristics and operational behaviours that it can achieve (He, 2010). Figure 4.5 shows a depiction of the expected characteristics that should accompany the successful implementation of a smart grid project.
In a thorough study on the smart grid and all the improvements it brought to the regular power grid, Fang et al. (2012) listed the following as some of the management objectives researchers intended to achieve through the use of the technology:

- **Energy efficiency:**
  The ability to produce electric power in a manner that limits the waste of resources.

- **Demand profile improvement:**
  The ability of better forecasting the use of electricity at demand centres in order to make better decisions on how to manage production and distribution.

- **Utility optimisation:**
  The ability to increase the value obtained in the consumption of electricity. Value may come in the manner of better utilised resources.

- **Cost optimisation:**
  The ability to limit the expenses incurred in the generation, transmission and consumption of electricity.

- **Emission control:**
  The ability to control the amount of damage caused by the gas emissions created in the generation of electricity.
With the use of information technology to improve the running of the power grid come many benefits that are usually associated with most system automation projects. One of the most crucial benefits is the increased control through activity monitoring, resulting in the discovery of other opportunities that could only come to light by monitoring trends and small changes in energy consumption. The latter and several other benefits of the smart grid for different stakeholders are shown in Figure 4.6 (Bossart & Bean, 2011).

The promise of potential smart grid benefits has introduced many research initiatives to achieve the full scale utilisation of information communication technologies in the power grid. The combination of research from different fields has been brought together in order to understand the different spectrums that smart grid development affects. Many challenges have been discovered during these studies. Schantz, Beal, Loyall, Pal, Rohloff and Bestavros (2009) identified the following to be some of the challenging aspects in the research and the creation of the smart grid:

- The creation of set methodologies, frameworks and protocols for inter-operable smart grid design;
- Information services designed to work in the smart grid environment;
- Integration and cross-domain issues in a smart grid system of systems;
- Scalability, reliability and survivability of a smart grid system.

<table>
<thead>
<tr>
<th>Electric Utility Companies</th>
<th>Consumers</th>
<th>Society as a whole</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improved operations</td>
<td>• More reliable service</td>
<td>• Improved security of electricity delivery</td>
</tr>
<tr>
<td>• Reduced electrical losses</td>
<td>• Reduced business losses</td>
<td>• Creation of new jobs in the smart grid industry</td>
</tr>
<tr>
<td>• Improved maintenance and planning</td>
<td>• Potential savings</td>
<td>• Reduction in fossil fuel consumption</td>
</tr>
<tr>
<td>• More accurate metering and billing</td>
<td>• Access to real time information</td>
<td>• Reduced environmental emissions</td>
</tr>
</tbody>
</table>

Figure 4.6 – Benefits of Smart Grid Implementation (Bossart & Bean, 2011)
The current section was devoted to describing the main objectives of the smart grid to give a better idea of its purpose and the reasons why this prospect should be investigated. The next section looks at the different technology components that are then necessary to exploit the potential benefits of the smart grid.

4.3.3 – Smart Grid Infrastructure

The infrastructure of the smart grid consists of all the necessary machinery and tools for energy generation and distribution, and the information communication technologies needed to improve the power grid. The technologies required include advanced communication technologies, advanced metering technologies and all improved electricity generation technologies (Dan & Bo, 2012).

The National Institute of Standards and Technology (NIST) developed a conceptual model of the smart grid which could be used when analysing the different aspects inherent in the grid (2010). The conceptual model includes the seven main ‘actors’ involved in the smart grid and shows the connections between each one. An illustration of this conceptual model is shown in Figure 4.7.

In NIST’s conceptual model of the smart grid, the infrastructure should be able to provide two-way communication of information as well as a two-way flow of electric power. This would allow the real-time transfer of information and electric power, from any generation source in the grid, in whichever direction desired.

The infrastructure suitable to support the smart grid needs to be able to support: the generation of energy; the extraction of information in every occurrence across the smart grid; and the communication between the seven main actors involved in the arrangement of the smart grid (as shown in Figure 4.7). Fang et al. (2012) explained that the smart grid infrastructure can be divided into three subsystems that work together to support the grid.
The three subsystems used to create the smart infrastructure are (Fang et al., 2012):

- The smart energy subsystem;
- The smart information subsystem;
- The smart communication subsystem.

The following subsections are devoted to briefly discussing each of the three subsystems necessary in a smart infrastructure, which would form the foundation for systems used to control and maintain the smart grid.

Figure 4.7 – Conceptual Model of the Smart Grid (NIST, 2010)

4.3.3.1 – Smart Energy Subsystem

The smart energy subsystem is made up of the regular electric energy flow already existent in the regular power grid. This is the part of the infrastructure that provides all services for the generation, transmission and distribution of electric power across the grid (NIST, 2010). The use of alternative energy resources is more emphasised in the smart grid and forms part of the smart energy subsystem. In Figure 4.7, bulk generation, transmission, distribution and customers form the energy subsystem’s main components.
One of the major developments introduced by the smart grid is the generation of electricity from distributed resources. The distributed generation of electricity basically means that electricity used in the grid can come from multiple generation sources. Coupled with the two-way power flow ability, the smart grid’s distributed generation feature enables distributed energy resources such as end-consumer’s solar panels to add energy to the grid in an effort to enhance power quality and reliability (Fang et al., 2012).

4.3.3.2 – Smart Information Subsystem

One may look at the power grid and only focus on all the technical components responsible for the generation of electric power and its transmission. In the regular power grid, this simplistic method of analysing the grid would not necessarily be wrong; but, in the smart grid, the supporting information technologies must also be looked at to get a holistic view of the grid. The smart grid depends heavily on the technologies that allow for the monitoring of its different components for processing and analysing all the information generated on the grid (Khattak et al., 2012).

The huge concern regarding the analysing of information is due to the fact that other control systems make use of the analysed information in order to tune the smart grid to function in a stable manner given any current circumstance that it might be facing. For this reason, information systems exist for the generation and processing of data. Fang et al. (2012) identified the following to be amongst the most important aspects of the smart grid’s infrastructure in the information subsystem:

- **Smart metering:**
  This is the infrastructure in place to enable automated meter readings. The set of technologies and devices used for smart metering are said to be part of the advanced metering infrastructure (AMI).

- **Monitoring and measurement:**
  The provision of real time data measured accurately is very important in the smart grid as systems use these to make automated intelligent decisions.
• **Information management:**
  Defining the data structures, the method of information transfer and storage, the algorithms used for analysing and mining all gathered data form part of the information management activities carried out in the smart grid.

### 4.3.3.3 – Smart Communication Subsystem

As the smart grid is filled with a myriad of information gathering devices, this information needs to be shared across the whole grid in order to make sure that well assessed decisions are made with real-time information. The smart grid is composed of many information generation nodes. Therefore, in some cases, a single type of network and communication technology will not suffice and different types of computer networks have to be combined (Fang et al., 2012). Fang et al. (2012) listed the following to be some of the types of networks that the smart grid uses:

- **The enterprise bus:**
  Connects control centre applications, markets and generators.

- **Wide area networks:**
  These networks connect different nodes that are geographically dispersed regions.

- **Field area networks:**
  These networks connect intelligent devices used to monitor electric power equipment such as transformers.

- **Premise networks:**
  Are close range networks usually found within the customer domain. Home area networks (HAN) are considered to be premise networks.

Communication between the different nodes in the smart grid information network can be achieved by either using wireless or wired technologies, or even a combination of the two. When using wireless communication, some of the technologies used are cellular communications systems, Wi-Fi networks and satellite communication systems (Fang et
The choice of which communication medium to use is often dependent on the potential financial costs and the security that it provides.

On the other hand, wired communication methods include the use of fibre-optic technologies and power line communication technologies. Fibre-optic communication is used by power companies for its resistance against radio and electromagnetic interference (McGranaghan & Goodman, 2005). Fang et al. (2012) define power line communication as a ‘technology for carrying data on a conductor also used for electric power transmission’. The latter communication method is often favoured as the costs of implementation are not as high as other methods since it makes use of the already existent power line infrastructure. Power line communication can be split into two different types: narrowband and broadband (Aalamifar, Hassanein & Takahara, 2012).

4.3.4 – Smart Grid Standards

With the fast paced developments in the power industry aiming towards a move to the smart grid, one of the biggest challenges has been the creation of standards that will allow the different power utility companies to bring forward an industry wide consensus (Farhangi, 2010). Because the smart grid relies heavily on the convergence and interoperability of a wide variety of systems, standards need to be put in place in order to facilitate the integration process.

The creation of standards will emphasise the sense of common understanding in the field of smart grid research. For example, Farhangi (2010) points to the need of setting a standardised framework that will allow end-to-end command and data exchange across the different components of the smart grid.

In the United States, the National Institute of Standards and Technology (NIST) has been a major driver of the standardisation effort on the smart grid. In 2009, the NIST released a report titled “NIS Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0”, where many of the aspects of the smart grid were studied, explained, and issues that needed addressing were discussed.
Other professional bodies have also been included in the design of international standards for the smart grid, one of these being the Institute of Electrical and Electronics Engineers (IEEE). Some of the biggest areas of concern surround the use of communication technologies and all the security and privacy issues associated with them. Table 4.3 is a list of some communication standards identified in a study carried out by Gungor et al. (2011).

Table 4.3 – Communication Standards in the Smart Grid (Gungor et al., 2011)

<table>
<thead>
<tr>
<th>Name of Standard</th>
<th>Description</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61970 and IEC 61969</td>
<td>The common information model (CIM): IEC 61970 works in the transmission domain and IEC 61969 works in the distribution domain</td>
<td>Energy management systems</td>
</tr>
<tr>
<td>IEC 61850</td>
<td>Flexible, future proofing, open standard, communication between devices in transmission, distribution and substation automation systems</td>
<td>Substation automation</td>
</tr>
<tr>
<td>IEEE P1901</td>
<td>High speed power line communications</td>
<td>In-home multimedia, utility and smart grid applications</td>
</tr>
<tr>
<td>HomePlug</td>
<td>Power line technology to connect the smart appliances to a home area network</td>
<td>Home area network</td>
</tr>
<tr>
<td>SAE J2836</td>
<td>Supporting cases for plug-in electric vehicles communication</td>
<td>Electric vehicles plugged into the smart grid</td>
</tr>
<tr>
<td>m-Bus</td>
<td>European standard and providing the requirements for remotely reading all kinds of utility meters</td>
<td>Advanced metering infrastructure</td>
</tr>
<tr>
<td>ANSI C12.19</td>
<td>Flexible metering model for common data structures and industry vocabulary for meter data communications</td>
<td>Advanced metering infrastructure</td>
</tr>
</tbody>
</table>
4.4 – Conclusion

The evolution of the regular power grid seems very fitting to society’s natural development into exploring more reliable, safe, affordable and environmentally friendly lifestyles. The smart grid brings about many benefits that will help society to continue to prosper. Although not yet widely applied across the world, current research will make the anticipated benefits of smart grids a more interesting proposition.

Information communication technologies are the foundation cornerstone of smart grid development. Although there are still many alignment, feasibility, standardisation, privacy and security issues to be solved, there are ways of overcoming these. The further technology is developed, the further the benefits of the smart grid. The ultimate goal of the 21st century power grid is to provide consumers with affordable, reliable and sustainable power; and all developments are geared towards achieving these goals.

The aim of this chapter was to address the main aspects of the smart grid in detail, in order to bring forth why it is said to be an important development in the power grid. It was also necessary to briefly touch on the different components that together make the foundation on which the smart grid is based. The following chapter also discusses the smart grid, but it addresses aspects that make the smart grid a Critical Infrastructure.
Chapter 5
The Smart Grid as a Critical Infrastructure

Chapter 1:
Introduction

Chapter 2:
Critical Infrastructure

Chapter 3:
Critical Information Infrastructure Protection

Chapter 4:
The Smart Grid

Chapter 5:
The Smart Grid as a Critical Infrastructure

Chapter 6:
Software Agents

Chapter 7:
Intelligence Enabling Machine Learning Models

Chapter 8:
Intelligent Agents and Complex Adaptive Systems

Chapter 9:
Agent Technology and Critical Information Infrastructure Protection

Chapter 10:
Multi-Agent Model for Smart Grid Security (MA-SGS)

Chapter 11:
MA-SGS: Node Agents

Chapter 12:
MA-SGS: Process Monitoring Agent

Chapter 13:
MA-SGS: Security Response Agent Structure

Chapter 14:
MA-SGS: Interoperability Agent Structure

Chapter 15:
MA-SGS: Attack Agent Structure

Chapter 16:
MA-SGS: Smart Grid Simulation & Model Implementation

Chapter 17:
MA-SGS: Model Results

Chapter 18:
Conclusion
5.1 – Introduction

The development of the smarter, more environmentally friendly and cleaner power grid was briefly outlined in the previous chapter. The smart grid’s most basic foundations, standards, benefits and objectives were discussed. Chapter 5 looks at the intricate components of the technology enabled power grid, this way considering all layers that support the smart grid and some of the security issues that arise from its development.

According to Slootweg et al. (2011), the smart grid can be divided into a set of layers that together make all the benefits of an upgraded power grid possible. These layers can be seen in Figure 5.1. The application, communication and power layers work in conjunction in order to run the smart grid. Together these layers conform to the physical, operational and cyber layers described by Coutinho et al. (2003) in Figure 4.3.

The creation of the smart grid is dependent on the combination of different fields of knowledge. Each layer of the smart grid taps into the use of both proven modern technologies and technologies under development. Seeing that the layers in the smart grid fit the necessary aspects of an information system used in a Critical Infrastructure, such as the power grid, the smart grid should also be studied as a Critical Infrastructure to better understand its complexities which could vastly affect the demand centres’ adhering to its technologies.

Chapter 4 served as an introduction to the smart grid and how it serves as a new power grid, which, apart from attempting to be more environmentally friendly, also gives more control over power to both producers and consumers. The current chapter is now devoted to discussing some of the more inherent components of the smart grid, and how these components make the smart grid a relatively complex Critical Infrastructure that has to be constantly monitored. The following sub-sections of the chapter will analyse each of the smart grid’s layers before discussing the security aspects that burden the smart grid when viewed as a Critical Infrastructure.

59
When taking its most basic components for generation, transmission and distribution into account, the power layer of the smart grid can be said not to be too different from the old power grid. Where the smart grid initiative differs is in terms of the new customer behaviour towards electricity usage and the increased focus on the use of renewable energy resources and efficient methods for energy storage and utilisation (Zhang, Wang, Niu, Song, Chen, & Li, 2012).

The power layer in the smart grid is developed with a much broader and cumbersome set of goals which include increased use of renewable energy resources while...
attempting to optimise efficiency of energy delivery at all times. Although to a small
degree, certain initiatives were introduced to make the smart grid’s power layer different
to the regular power grid. New ways of generating and storing energy are used in order
to make the intelligent power grid a more environmentally friendly infrastructure that still
satisfies the requirements of modern society (Pratt, Balducci, Gerkensmeyer,
Katipamula, Kintner-Meyer, Sanquist, Schneider & Secrest; 2010).

Technological developments have promoted the harnessing of renewable energy
sources, and, with new usage and processing techniques, their costs of management
and operation have become lower (Tucker & Negnevitsky, 2011). There are many types
of renewable energies available for use in electric power generation, the most sought
after being (Zahedi, 1994):

- Solar power;
- Wind power;
- Hydro power;
- Tidal energy;
- Wave power;
- Landfill gas as an energy source;
- Geothermal energy;
- Bio-fuel power (e.g. wood, straw).

The most important and enticing characteristic that drove research into the use of
renewable sources of energy is its self-replenishing property. The sources of energy
listed above have been researched and some have been used to support the smart grid
in achieving its objectives of producing cleaner energy for the masses. Furthermore,
due to escalating economic pressures of the sources of energy currently used (such as
the oil prices), many renewable energy projects have been boosted in the search of
much less costly energy that can be commercialised while meeting the environmental
The next challenge to bear in mind then is how these different power generation techniques can be used together to support one smart grid. Subsections 5.2.1 and 5.2.2 cover how the smart grid’s power layer can be divided to support the use of multiple power generation techniques that support its goals.

5.2.1 – Distributed Generation

As the drive for more efficient energy generation is pushed by the smart grid initiative, research has been focusing on reducing the production of green-house-gases (GHGs) while achieving economies of scale in the generation of energy. Distributed generation (DG), where electric power is fed to a small demand centre by a set of renewable energy sources, provides such a method that aids smart grid research to get closer to its goals.

Li, Li, Liu, Chen and Chen (2011) defined distributed generation as ‘a technology for electric power supply produced by using a wide variety of dispersed energy resources’. Furthermore, Cespedes, Parra, Aldana and Torres (2010) explained DG as being a method for ‘power generation at a small scale that connects to a distribution system near a site of consumption’, which is not directly connected to the main power grid system that supplies energy to the major region where this consumption site is situated.

The smart grid’s two-way communication paradigm, which characterises its exchange, transfer and usage of both information resources and electrical power, is one of its characteristics that make distributed generation possible. The U.S. Department of Energy (2008), a major supporter of the initiative, reported, in an awareness research document, that the smart grid’s disposition to using many different energy sources also makes it possible to use distributed generation.

The use of distributed power generation facilities also helps in the creation of distributed energy storage places. Storing energy is very important during situations where the current power needs of demand centres far exceed the current production of electricity, as the stored energy can then be fed back to the grid in order to meet the volume of
demand and relieve pressure on the grid. Such a process is referred to as 'peak shaving' (Nourai & Schafer, 2009).

Less environmental impact, improved control on electricity used, and better reliability are amongst the main benefits of the smart grid initiative. In addition to the aforementioned main benefits, Cespedes (2010) also identified the following to be amongst the value additions obtained from distributed generation and energy storage in the smart grid:

- It reduces the peak of the demand profile;
- It reduces the cost of other equipment, such as transformation, by reducing the maximum demand;
- It improves voltage and frequency regulation;
- It provides better use of renewable energy sources.

In order to better utilise the different generation methods, the smart grid's power layer includes the use of microgrids and virtual power plants to organise its different components to achieve better control and reliability. The following subsection briefly describes microgrids and virtual power plants.

5.2.2 – Microgrids and Virtual Power Plants

The use of distributed generation to supply electric power to small demand centres, which may sometimes be away from main power grid infrastructure, creates what is referred to as a 'microgrid'. Farhangi (2010) defined microgrids as “interconnected networks of distributed energy systems that can function whether they are connected to or separate from the electricity grid”.

A microgrid is able to, on its own, work as a major power grid where generation, transmission and distribution of power takes place. It has the ability to work either autonomously or combined with the regular power grid infrastructure in order to serve its
demand centre (Farhangi, 2010). Figure 5.2 shows the structure of a microgrid used in the smart grid.

Figure 5.2 – The Topology of a Smart Grid microgrid (Farhangi, 2010)

Microgrids can be seen as the building blocks of the smart grid, as, when these are connected, a more robust power grid, which makes use of power generation and consumption technologies that are more environmentally friendly, is formed. All the characteristics one would expect to find in the smart grid can be found in the smaller scale microgrid that functions for a smaller number of demand centres. Some of the features that a microgrid has include (Farhangi, 2010):

- Co-generators and power plants able to meet local demand and store power can be fed back to the grid if necessary;
- An ability to service a variety of loads;
- Making use of local and distributed power storage capabilities;
- Incorporating smart meters and sensors capable of measuring a multitude of consumption parameters;
- Incorporating a communication infrastructure that enables system components to exchange information and commands securely and reliably;
- Incorporating smart terminations, loads and appliances capable of communicating their status and accepting commands to adjust and control their performance and service level based on user and/or utility requirements;
- Incorporating an intelligent core, which is composed of integrated networking, computing and communication infrastructure elements that appear to users in the
form of energy management applications that allow command and control on all nodes of the network.

Virtual power plants (VPPs) are another interpretation of aggregation of features of the smart grid initiative. The terms, ‘virtual power plant’ and ‘microgrid’, are often used interchangeably. Through the use of information systems, virtual power plants combine the different energy sources and energy consuming demand centres into one centrally controlled energy system regardless of physical location (Asmus, 2010). Figure 5.3 shows an illustration of how virtual power plant systems work in the smart grid.

![Image of Virtual Power Plant in the Smart Grid](VCharge Energy, n.d.)

A virtual power plant is integrated with an existing power grid network and provides value adding services to the supply side of the network that satisfy the needs of the demand side (Asmus, 2010). A microgrid, on the other hand, is a more self-contained mode of operation where the services it provides serve geographically close demand centres, as there is a drive of making these centres autonomous in power generation, transfer and usage.
According to Bayar (2013), a virtual power plant works as an aggregator of small scale power grid network components. A virtual power plant has a set of small power generation sources, and operates them all as one single flexible resource for the energy market, or demand centre it serves.

As microgrids and virtual power plants are riddled with features that are highly integrated in order to work together efficiently, software is used as the bondage component for such integration tasks. As most complex systems such as these are made up of many features, different software is used to control each feature, thus meaning that if they are to work together, the various different software systems have got to be able to communicate with each other. The following section briefly discusses the communications layer of the smart grid environment.

5.3 – Communications Layer

All modern systems are made up of components able to interact and exchange information with each other. The smart grid is no different, as, although it still makes use of the existent power grid infrastructure, it also adds to it a layer of information processing, which is then aided by a secure communications layer which allows for the exchange of information (Fang et al, 2012). The different connections shown in Figure 4.7 (page 52) are supported by these modern communication technologies. As mentioned in Chapter 4, the most commonly used network methods/types were: the enterprise bus, wide area networks, field area networks and premises networks.

Advances to the power grid network have been heavily reliant not only on the use of new power generation methods, but also on the ability of each of its nodes to communicate using, among others, some of the aforementioned network technologies. According to Zurborg (2010), the information generated by each software system can be shared between them, as well as fed to the supervisory control and data acquisition (SCADA) or distribution management system (DMS) to better control and monitor the smart grid.
The use of digital communication technologies has been at the crux of all the developments in smart grid technology as the efficient energy generation and usage benefits can only come from the use of systems that are able to exchange information that is processed and used by intelligent decision control systems. Figure 5.4 shows some of the different communication technologies that provide the basis to enable the smart grid (Budka & Deshpande, 2010).

Figure 5.4 – Integrated Communication Network for the Smart Grid (Budka et al., 2010)
As illustrated in Figure 5.4, the integrated network uses internet protocol (IP) for the exchange and transfer of data across the different nodes of the network. All communication data is routed from its origin to its destination for processing. Budka et al. (2010) lists the following smart grid technologies that the integrated network supports:
- Smart metering;
- Automated demand response;
- Rapid inter-substation response;
- Distribution automation;
- Synchrophasors;
- SCADA;
- EMS;
- Microgrid connectivity.

The smart grid network is built to support two-way communication where it can be seen as a mesh network where each node is able to receive and send information. The use of a two-way communication mesh network can make way for security issues that need to be addressed if the network is to be successfully implemented (Liu, Peng & Liu, 2011). Two-way communications in the smart grid would occur between smart meters, microgrid controllers and generation substations. Figure 5.5 shows the classification of the different security risks that the technology can create.

![Malicious Threats Diagram]

Figure 5.5 – Classification of Security Threats towards Communication Networks in the Smart Grid (Lu et al., 2010)

Network availability is of high importance in the smart grid, as its major potential is based on the ability of different information systems that control the grid to communicate with each other. Since these information systems are highly synchronised, it is also of vital importance that the data transferred between them is not maliciously altered in any way or form if the systems are to work well together (Fang et al., 2012).
Information in the smart grid is not only numbers and figures being generated in the generation stations. Since customers also actively participate in using these information systems, their private information is also to be protected if people are to trust them and continue to contribute to the smart grid initiative (Slootweg et al., 2011).

In order to manage the different components of the smart grid, the software systems used need to be able to continuously and autonomously work out the most appropriate power generation and distribution settings, as well as provide the human actors on the smart grid with an interface that can be used to change certain preference settings (Tang, 2011). As pointed out in the previous section, these systems need to be able to work together to be able to provide a smart grid that meets its objectives.

The power layer of the smart grid essentially refers to the physical structures necessary to create the grid, and the methodologies used to manage electric power. The communications layer describes how each of the components of the smart grid network exchange information (Fang et al., 2012).

Another layer is still necessary to provide the software programmes needed to monitor and control the different mechanisms operating at each node of the smart grid network. The following section is devoted to discussing the applications layer of the smart grid that contains all the systems used.

5.4 – Applications Layer

A good communication network layer and an advanced power layer form only the basic underpinnings of the smart grid. Having these simply means that power can be produced easily for usage in demand centres; and, through the communication network, every element of the smart grid can be kept in check. The applications layer of the smart grid though is what brings everything together.
It is in the application network where all the systems that enable the control, monitoring and management of the smart grid are situated. These applications need to be able to closely monitor the smart grid’s components, provide the grid’s human operators with enough information to make decisions as well as enable operators to manage and monitor the electricity market of the demand centre being served (Slootweg et al., 2011). In order to meet these requirements, the applications need to exhibit the following requirements (Jarventausta, Repo, Rautiainen & Partanen, 2010):

- **Being interactive:**
  This enables interactions between consumers and services providers;

- **Being adaptive and scalable:**
  This enables flexibility in the operation of the smart grid’s functions, thus allowing the grid’s operation to be more dynamic;

- **Being optimised:**
  This enables the smart grid to use the available resources in a manner that enhances each resource’s per unit utility;

- **Being proactive:**
  This enables the smart grid’s systems to produce immediate responses to imminent emergencies;

- **Being self-healing:**
  The automation systems on the smart grid enable it to attempt to restore its operations after moments of disruption.

- **Being integrated:**
  Monitoring, control, protection and other advanced systems are merged and able to work together;

- **Being secure and reliable:**
  This enables the smart grid to secure its different information systems and maintain availability of the grid’s services.
Given the amount of information processed by the smart grid, the applications layer needs to be capable of processing large amounts of data. Such applications process the information in order to maintain the flow of electric power efficiently and effectively during both its production at the power layer and its delivery at demand centres.

The communication networks help in coordinating the two-way flow of electric power that the information systems in the application layer are responsible for managing. Such a two-way transmission of electric power is supported by the two-way flow of data that these information systems process and pass through analysis algorithms in order to determine the most optimal action at each point in time (Belkacemi, Babalola, Ariyo & Feliachi, 2013).

The following are some of the different information systems that can be found in the application layer of the smart grid (Tang, 2011):

- A distributed generation system;
- An advanced metering infrastructure;
- Substation automation;
- Demand response systems;
- A utility-side control and management system;
- An end-user-side data and management system.

The information systems in the application layer enable the smart grid to integrate all the different energy generation techniques, monitor the use of each generation technique, as well as monitor how it is being used at its demand centre in real-time.

Depending on the rate of electricity used in the demand centre, the applications also help forecast the amount of power required in order to produce enough power to maintain a balanced demand-supply match (Tang, 2011). Furthermore, the information systems allow their human operators (utility companies and consumers) to manage the manner in which they use power.
The application layer therefore deals with a vast amount of information being generated and exchanged by the different information systems. Such information is crucial for these systems to work together, and thus must be kept secure using methods that will not disrupt the smart grid. Any model for ensuring smart grid security and reliability needs to take into account the information exchange models used by the information systems in the application layer to address the possible threats the grid faces. The following section briefly discusses some of the vulnerabilities and security considerations existent in the smart grid Critical Infrastructure.

5.5 – Vulnerabilities and the Smart Grid Critical Infrastructure

A report written by the IEEE-supported Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failure defined the term ‘vulnerability’ in a power system as follows (2009):

“A measure of the system’s weakness with respect to a sequence of cascading events that may include line or generator outages, malfunctions or undesirable operations of protection relays, information or communication system failures, and human errors.”

The task force’s exhaustive definition highlights the major threats faced by all types of electric power Critical Infrastructures. Electric power systems are usually under threat from different types of (intentional or unintentional) disruptions that should be closely monitored (Cepeda, Ramirez & Colome, 2012). Any Critical Infrastructure, if not designed and secured appropriately, can also be deemed a vulnerable system, where the threat of outages and failures are possible.

Vulnerability is not a one dimensional concept that is only analysed by the level of impact a threat event has towards the entity at risk. According to Bouchon (2006), vulnerabilities to an infrastructure should be evaluated using a three-fold set of criteria. An infrastructure’s vulnerability assessment should be done to identify the possible risks for each type of threat the infrastructure faces.
The three-fold criteria for how each instance of vulnerability has to be analysed is as follows (Bouchon, 2006):

- The amount of damage to an infrastructure that a threat may cause if realised;
- The amount of exposure an infrastructure has to the possible threat;
- The degree of resilience an infrastructure has against the threat.

All Critical Infrastructures are prone to multiple threats that range from natural disasters, weather, technical failures, human factors, labour conflicts, sabotage, terrorism, to acts of war (Chopade & Bikdash, 2012). Since different Critical Infrastructures within a nation are essentially linked to each other, the disruption of service in one could go on to threaten the functioning of another, thus resulting in a cascading failure.

Such hazardous situations which propagate from one Critical Infrastructure to another are referred to as ‘cascading failures’ (as discussed in Chapter 2). When evaluating Critical Infrastructure, an important aspect of the evaluation is an understanding of which components of the infrastructure are more susceptible to the different kinds of disruptions that have been identified (Liu, Mashayekh, Kundur, Zourntos & Butler-Purry, 2012). Such evaluations are performed so as to prioritise the points of vulnerability that require immediate security measures to be established.

The smart grid is mainly enabled by the use of multiple information communication technologies to improve on the regular power grid. The use of such technologies created a wide number of benefits that spanned from increased control of electricity consumption to cleaner methods of managing electricity. Along with such benefits, though, the highly networked technologies have also introduced vulnerabilities by creating access points for cyber intrusion (Srivastava, Morris, Ernster, Vellaithurai, Pan & Adhikari, 2013).

The vulnerabilities introduced by the communication technologies also come from the increased interaction complexity between the different systems (Yang, McLaughlin, Littler, Sezer, Im, Yao, Pranggono & Wang, 2012). A breach into any of the points
connected to the grid could give one access to multiple subsystems that could disrupt the smart grid.

The smart meters used as part of the advanced metering infrastructure (AMI) of the smart grid have been the subject of research as a possible point of access that may be used to create disruptions (Rana, Zhu, Lee, Nicol & Shin, 2012). According to Erol-Kantarci & Mouftah (2013), apart from the AMI and SCADA systems, threats to the smart grid could also come from the different energy storage subsystems, distribution automation subsystems, and electric transportation infrastructures. Table 5.1 shows a list of some of the challenges to the security of the smart grid by looking at each of the applications that are used.

Table 5.1 – Applications and Challenges in the Smart Grid (Erol-Kantarci & Mouftah, 2013)

<table>
<thead>
<tr>
<th>Applications</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced metering infrastructure (AMI)</td>
<td>Privacy of information and secured data collection and storage</td>
</tr>
<tr>
<td>SCADA network</td>
<td>Scalability and lack of online analysis tools</td>
</tr>
<tr>
<td>Measurement control systems</td>
<td>Data processing and storage and secure data collection and storage</td>
</tr>
</tbody>
</table>

Compromising and gaining access to the systems of the smart grid give a perpetrator multiple options as to how to disrupt the operation of the grid. Barnes, Johnson and Nickelson (2004) listed the following as some of the attack scenarios the smart grid can be vulnerable to if a security breach is successful:

- A shut down and/or control of the devices at substations or power generation plants;
- An insertion of a malicious code set to be executed after certain events or at a random time;
- The creation of system ‘back doors’ to make future attacks easier;
- The corruption of data so as to disrupt other information systems that use it;
- The changing of data values to reflect current operational values that do not represent the grid’s actual operational status;
• Making resources unavailable to use by the grid’s information systems.

The two-way communication enabled by sensing, measurement and control systems used in the smart grid, as well as obsolete cyber-infrastructure (i.e. legacy systems\(^1\)) are the main entry points that make the enhanced power grid susceptible to cyber-attacks (Huang, Esmalifalak, Nguyen, Zheng, Han Li & Song, 2013). Each of the applications listed in Table 5.1 are based on two-way communication technologies and thus need to be designed with security in mind in order to operate efficiently and securely. Such considerations would help detect and respond to attack scenarios such as those listed above.

5.6 – Conclusion

Being a complex system, the smart grid’s power, communication and application layers need to always work together in order to bring forward all its proposed benefits. At the centre of the three layers, is the information exchanged between each layer to form a single cohesive system. It is crucial to establish methods in which the information exchanged between the different layers is protected. Each layer needs to have security measures built in to secure the smart grid as a whole. As the smart grid exhibits characteristics as those of a Critical Infrastructure, it then becomes an even more important initiative that must be kept reliable if society is to benefit.

Given that the smart grid is indeed a Critical Infrastructure, and taking into account that it also is, to most nations, a generally new endeavour; the smart grid becomes a prime candidate to be the underlying topic of this dissertation. The dissertation aims at creating a model that attempts to mitigate the risks identified in Figure 5.5, which directly relate to the challenges faced in the smart grid (listed in Table 5.1), in order to ensure the continued running of a smart grid network.

---

\(^1\) A legacy system is an old piece of software that, over time, remains vital to an organisation (Sommerville, 2008).
The proposed model in the dissertation is based on the use of software agents that monitor the smart grid. The following chapter introduces and addresses the topic of software agents and whether multi-agent systems are indeed suitable for use in protecting Critical Infrastructure (namely the smart grid).
6.1 – Introduction

Due to the significant human-input overhead produced by computing systems used to control complex operations, the drive towards creating autonomous systems has been monumental. When looking at human beings, autonomy is seen as the key aspect necessary for people to be able to live in a common social environment, where each individual is able to engage in multiple forms of social interactions by their own accord (Zhang & Zeng, 2009). Achieving autonomy in computing systems is enabled by the artefacts introduced by the artificial intelligence field.

Autonomy in computing systems can be defined as an entity’s ability to act upon its own decisions, which are deliberated by its own decision-making process, without the help of other entities (Ball & Callaghan, 2012). Software agents have been used to build autonomous systems in order to lessen the burden of using human-input to control complex systems that deal with massive amounts of real-time data (Bologa & Bologa, 2011). Chapter 6 is devoted to discussing software agents in terms of their basic infrastructure, characteristics, environment, the different types of agents that can be built and how different software agents can be built to work with others within the same environment.

6.2 – Agent Systems

Agent systems have been interpreted differently by many in the computer science field. More theoretical artificial intelligence proponents view them as a combination of independent and autonomous entities of processing that, given appropriate input values, have specific abilities to flexibly and autonomously execute tasks (Alonso, 2002). On the other hand, software developers view them as composite pieces of software systems that are able to act for themselves and interact with each other, thus minimising the need for human input (Pakdeetrakulwong & Wongthongham, 2013).
For the purposes of the dissertation, the ‘agent’ definition set by Russell and Norvig (2010) will be followed:

“An agent is anything that can be viewed as perceiving its environment through sensors and acting upon that environment through actuators.”

Russell and Norvig’s interpretation of an agent is illustrated in Figure 6.1. The definition is generic enough to apply to any agent, independent of its nature. It could apply to both agents of a physical nature (i.e. robots) and software agents. For the purpose of the dissertation, only software agents will be focused on.

![Figure 6.1 – Agent Definition (Russell & Norvig, 2010)](image)

According to Newell and Simon (1972), a software agent is: an autonomous information processing system composed of devices used for capturing and publishing information; a logical unit used for processing information; and, lastly, a memory unit used to store data about its environment. Through perceiving its environment, an agent is able to retrieve the necessary readings available to it within its problem domain. These readings vary in type and range and are determined by the scope of values existent in the environment in which the agent works. Agents basically monitor these sensory inputs for processing using dynamic algorithms that give the agent the ability to act on its environment (Fougeres, 2012).
The results of the algorithm are used to determine the action the agent should take, therefore allowing the agent to behave in an autonomous manner as it is able to retrieve input from its environment, process it, and, based on the result of the deliberation, take any necessary action all on its own (Huber, 2007). Table 6 provides the definitions for each concept shown in Figure 6.1.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>The autonomous unit of software.</td>
</tr>
<tr>
<td>Sensors</td>
<td>These are the components the agents use for receiving values from their environment.</td>
</tr>
<tr>
<td>Environment</td>
<td>The environment in which the agent finds itself is, in essence, in the problem domain where it works to achieve its intended purpose(s).</td>
</tr>
<tr>
<td>Percepts</td>
<td>These are signals or values occurring within the problem domain, which the agent receives via its sensory components. Percepts may be naturally occurring in the environment or may be the result of actions taken by the agent.</td>
</tr>
<tr>
<td>Effectors</td>
<td>The tools made available to the agent, which allow it to act on its environment.</td>
</tr>
<tr>
<td>Actions</td>
<td>The activities taken by the agent using its effector components, after deliberating through its algorithms by using the percepts which it sensed from its environment.</td>
</tr>
</tbody>
</table>

The use of agent technology in complex systems has been widely researched since its conception due to the possible benefits of using autonomous software to achieve completion of tasks assigned. In certain environments, single agent systems often do not suffice to achieve an optimal solution, or one that satisfies all constraints coherent with the problem at hand due to the chaotic dependencies or relationships between all the different parts of the problem.

For units of software to be recognised as agents, they have to meet certain agent-identifying characteristics such as the following (Leung, 2012; Jones, 2008; Horn, Kupries & Reinke, 1999):
- **Persistence:**
  In order to achieve its intended purpose, an agent must ensure to continue working within its environment;

- **Rational**
  Given a possible condition, a software agent is said to be ‘rational’ if it is able to carry out an action that best meets its acceptable performance criteria;

- **Reactive:**
  An agent's ability to act autonomously has to be aided by its inherent ability to act at the right time when responding to a stimulus;

- **Proactive:**
  Software agents that are classified as ‘intelligent’, should, apart from reacting to a stimulus, also actively pursue actions that will satisfy its evaluation criteria;

- **Autonomous:**
  Intelligent software agents should be able to act on their environment by their own means, and not by user-guided instructions;

- **Communicative:**
  In order to capitalise on its modularity property, software agents should be able to work with other agents, which can only occur if an appropriate communication medium exists;

- **Adaptive:**
  Given that environments are often prone to change, software agents should be able to adapt to these changes in order to still meet its set goals.

In order to function, software agents need to be deployed to an environment. Such an environment would be a computational representation of the field for which the agent is designed. Environments can often differ based on the availability of information they contain. The following subsection briefly discusses a few types of agent environments.
6.2.1 – Types of Environments

Agents mostly differ in terms of their construction based on the goals they are made to achieve and the conditions according to which they work. The environment in which the agent is placed is a major determinant of how it is built, what kind of sensors and actuators it is equipped with, as well as what kind of goals it has to achieve and how it achieves them.

There are many types of agent environments, the properties of which affect the manner in which the agent works. The following is a list of some of the different characteristics agent environments may exhibit (Russell & Norvig, 2010):

- **Fully observable or partially observable:**
  An environment is deemed to be fully observable when a software agent in it is able to get all information about the environment at all times, and partially observable when this is not wholly the case.

- **Deterministic or stochastic:**
  When a new environmental state is fully predictable by the agents working within it, the environment is then said to be deterministic. It is seen as stochastic when current actions can’t be used to speculate the resulting changes in the environment.

- **Episodic or sequential:**
  Environmental states that do not carry on affecting an agent’s subsequent decisions define what is called an episodic environment. In sequential environments, an agent’s actions may affect the environment in such a way that this may, at a later stage, affect the agent’s decisions.

- **Static or dynamic:**
  A constantly changing environment is said to be a dynamic environment. Such a dynamic environment constantly presents the agent or agents working in it with
different conditions. A static environment’s state does not necessarily change, and, therefore, an agent is able to assume the environment’s status.

- **Discrete or continuous:**

  An environment’s state can also be determined by the manner in which time is handled. When each environmental state is allocated a specific amount of time, where for each unit a specific state is prevalent; the environment is said to be discrete. When time is seen as a property that does not stop, and conditions may change as time passes; the environment is said to be continuous.

Just as there can be different environments, there can also be different types of agents created. It would be up to the designer to evaluate the type of environment for the software agent, and to then decide on the most suitable form of software agent. The next subsection briefly looks at the different types of agents.

### 6.2.2 – Types of Agents

Given that agents are designed for a specific purpose, the manner in which they perceive their environment, and how they use this information to determine their course of action; can determine how different types of agents can be identified. The choice of agent type is selected depending on the nature and complexity of the problem domain or environment. Multiple authors have defined different types of software agents that can be used. The current subsection will look at a few of these types.

Rasmussen (1983) analysed the use of information systems to conduct repetitive activities performed by their human counterparts. In order to conduct certain activities in their place of work, Rasmussen (1983) identified three behavioural modes human participants needed to have. Such behavioural modes were based on: signals (data representing the dynamic configuration of an environment); signs (values indicating the state of an environment); and symbols (other environmental information that may be processed) that had to be taken into account for one to be able to do work. The three behavioural modes are as follows (Rasmussen, 1983):
• **Skill-based Behaviour:**
  The skill-based behavioural mode is necessary when an entity is required to have certain abilities that allow it to use environmental information to be able to seamlessly act on its environment. The entity may evaluate its performance based on how the actual state of the environment differs from the intended state.

• **Rule-based Behaviour:**
  Rule-based behaviour is used in a familiar and well recognised environment where work is basically done according to a sequence or a set of guidelines that have to be followed strictly. Such guidelines or set of rules need to be adhered to by the entity working in the environment.

• **Knowledge-based Behaviour:**
  When a dynamic environment constantly produces new information to be interpreted by an entity, it is useful for the entity to have a set of goals it needs to strive to achieve. The entity should also have the ability to understand and generalise different situations that enable it to make appropriate decisions even in unrecognised conditions. This way, the entity needs to be able to formulate new knowledge based on its understanding of its environment.

Given that software agents are often used to take on activities that would otherwise be carried out by human operators, identifying the behaviour modes processed by human operators is important to determine the features a software agent needs to have. Based on Rasmussen’s (1983) behavioural models for entities working in an environment, Fougeres (2012) derived four different types of agents that could be constructed. Such agents would possess features consistent with the behavioural modes. The following are the four derived agents (Fougeres, 2012):

• **A Reactive Agent:**
  A reactive agent is one that exhibits skill-based behaviours in order to use its abilities to deal with different environmental conditions;
• **A Routine Agent:**
  Such an agent would obey rules imposed on it that would help it determine the repetitive tasks it needs to execute after recognising the environmental conditions;

• **A Cognitive Agent:**
  Such agents are equipped with the ability to identify and interpret an environment, and, based on its set goals and current knowledge plan; execute the most appropriate course of action.

• **An Actor Collective Agent:**
  Such an agent would be derived from the different abilities of the previous three, but also equipped with the ability to work with other agents in the same environment.

Nwana (1996) took a different approach at describing the different types of software agents that can be built. This approach is based on the agent’s abilities to act on its own, communicate with other agents within a shared environment, as well as an agent’s ability to learn from its previous experiences. Figure 6.2 shows Nwana’s (1996) classification of different agent types. The figure is elaborated on in the following chapter.

![Figure 6.2 – Agent Classification (Nwana, 1996)](image-url)
Russell & Norvig (2010) determined the following to be amongst the basic kinds of agents that can be designed and implemented in agent-based systems:

- **Simple Reflex Agents:**
  Such an agent has a pre-set selection of actions that it can execute based on the current state of the environment. After capturing information on its environment, it queries its actions to identify which one it should select, while completely ignoring any action it has ever taken before. Therefore it completely disregards its historic action record and treats each situation individually.

- **Model-based Reflex Agents:**
  The model-based reflex agent essentially adds the ability to keep track of the state of the environment to the simple reflex agent. The agent uses a model as a description of how its environment works. The internal state of the agent is affected by the history of previous events. Thus, such an agent makes use of previous events when selecting its pre-set collection of actions.

- **Goal-based Agents:**
  Goal-based agents build on model-based reflex agents. Besides being able to keep track of the state of the environment, and have a description of how the environment changes; a goal-based agent is also equipped with information about desirable states. The information on desirable states aids the agent to use its knowledge about how the environment changes to help it select the most appropriate action based on how it creates a desirable environment state.

- **Utility-based Agents:**
  Often setting deterministic goals may not allow an agent to select the most appropriate agent. Therefore, given the characteristics of an environment; an agent can be given the ability to use a utility function that helps it evaluate each action by how much it can possibly improve the state of the environment. The utility-based agent is then allowed to select an action that best optimises the agent’s utility function. Any action that deteriorates the value obtained from the utility function is not executed.
Agents can be used in numerous domains. Agent systems can be used in, amongst others: networked systems, e-commerce, critical safety systems, and Critical Infrastructure systems. In order to ensure their success in achieving their goal, software developers need to make sure that their actuators fit the environment that they are in. Their actuators need to be properly mapped to handle the data which will be used in the working of the agent.

Wooldridge (2009) stated that, amongst others, ubiquity, interconnection, intelligence, delegation and use of human orientation are the most influential trends that caused agent systems to emerge. The versatility of agent technology was mostly aided by the trends in the computing field where software systems needed to be more embedded in their environments in order to function with less human interference. Such independent technology resulted in the creation economically feasible and integrated systems, while having less overhead to bear in terms of human input.

Since certain environments are often composed of a wide array of features that an agent has to be able to capture, it can sometimes be unfeasible, from a performance point of view, to allow just one single agent to process so much information. The addition of more than one agent to an environment, in order to divide tasks between them, could be a solution to overworking one agent in a complex environment. The next section discusses the use of more than one agent in a single environment.

6.3 – Multi-Agent Systems

By definition, agents are autonomous software units that can work independently of other units within an environment (Nagwani, 2009). Given that agent design principles encase single units of software functionality within agents, there can be times where complex problems need to be solved at different granular levels, thus making it inappropriate to encapsulate the entire solution by using a single agent.
Multi-agent systems could be seen as the solution to this conundrum, as these call for the use of multiple agents that can be used to achieve a single complex problem. The different agents in the system are given different tasks or parts of the problem, so that, through communication and coordination with the other agents within the system, an optimal solution for the problem being dealt with can be achieved. Hallenborg (2008) stated that multi-agent systems can also be referred to as ‘Distributed Artificial Intelligence’.

Altogether, a multi-agent system can still be seen as being an autonomous system. Each agent’s properties contribute to the multi-agent system setup, therefore allowing it to exhibit its autonomous property. Apart from autonomy, multi-agent systems are also known to have flexibility, distributed processing, fault tolerance and flexibility as their defining properties (McArthur, Davidson, Catterson, Dimeas, Hatziargyriou, Ponci & Funabashi, 2007).

The goal in multi-agent environments is to give each participating agent simple and modular rules that it needs to follow during the solving of a problem. This way one can observe the complex emergent behaviour exhibited by the system as a whole during the interaction of these different agents equipped with simple rules when solving a problem. Figure 6.3 illustrates how different agents are set up in a multi-agent system.

Figure 6.3 – Typical Multi-Agent System Setup (Nagwani, 2009)
Coordination of the independent and collaborative actions of agents has been one of the biggest issues in the design of multi-agent systems. According to Nwana, Lee and Jennings (1996), coordination is of utmost importance for the following reasons:

- Preventing anarchy or chaos;
- Efficiency;
- Meeting global constraints;
- Distributed information or resources;
- Dependencies between agents’ actions.

Methodologies such as ‘decision control theory’ and ‘computational game theory’ have been used to define models of communication and coordination in multi-agent environments. Other multi-agent coordination models include data-driven, control-driven and hybrid approaches, which can have synchronisation, planning, reaction and regulation as their different forms of implementation (Jiang & Liu, 2006).

6.4 – Conclusion

Although a modular and flexible manner of building software, the agent-based approach cannot be seen as a silver bullet for developing all types of systems. The environment for which it is intended to be used should be carefully analysed. If it is discovered that the components to be built should be able to work independently of each other while perhaps still exhibiting a certain degree of collaboration; an agent based approach could be suitable for use (Oja, Tamm & Taveter, 2001).

Certain environments could require an agent to be both autonomous, in terms of making its own decisions; as well as be able to use a certain degree of intelligent computation that guides it in selecting the most suitable action it should perform. The following chapter looks at how agents can utilise a variety of models of computation that enable them to work more effectively in their given environment.
Chapter 7
Intelligence Enabling Machine Learning Models
7.1 – Introduction

As the previous chapter indicated, agents are defined as autonomous units of software that act within an environment using their actuators (Russell and Norvig, 2010). This definition of agents and agent systems does not indicate how agents are able to know exactly what is to be done at any point in time. How are agents able to make decisions as to what actions to take? How do they know what to take into account?

When building agents that work in rather complex environments, one has to define dynamic methods that will give an agent the ability to deliberate on a given situation within its problem domain. This way, it can be stated that an agent is made to behave in an intelligent manner. According to Fogel & Fogel (1995), intelligence is not necessarily restricted to biological beings as it can be a property possessed by any given decision-maker.

Fogel (1964) defined intelligence as “the capability of a system to adapt its behaviour to meet its goals in a range of environments”. Lefton, Brannon, Boyes and Ogden (2005), however, defined it as the ability of an individual to act objectively and deliberate rationally to deal with changes within its environment. Given that an agent is a software unit built by a software designer, its environment and purpose are already specified. This way, an agent’s intelligence can be determined by how well it satisfies its purpose, given the values it senses within its environment.

The current chapter will briefly touch on what intelligent agents are and how they are made intelligent in order to behave or respond to percepts in a more objective manner to allow them to adapt to their environment. Different types of learning will also be briefly discussed to see how agents get to understand the inner functioning of their environment. Lastly, some of the defined models that were designed to help agents use different forms of abstraction in order to break down complex problems to allow them to find suitable solutions, are reviewed.
7.2 – Intelligent Agents

When one speaks of environments while discussing agent technology or any other paradigm of software construction, it has to be understood that this environment is merely a computer based representation of what would be encountered if a biological being were to be taken as the subject within it.

Since the coining of the concept, there have been many definitions of what an intelligent agent is and what makes an agent intelligent. The following are definitions that take into account how an agent can be seen to be intelligent.

**Maes (1995):**

"Computational systems that inhabit some complex dynamic environment, sense and act autonomously in this environment, and by doing so realise a set of goals or tasks for which they are designed."

**Singh and Gupta (2009):**

"An intelligent agent can be defined as an identifiable entity which can sense the environment around it, have its own beliefs and goals, is autonomous in choosing its actions, is flexible in learning and able to adapt to the changes in the environment."

Both definitions focus on the fact that, for an agent to demonstrate some degree of intelligence; it would need to find itself in an environment that changes over time. Meaning that with every environmental change, the agent would be faced with different situations with which it must be able to work. The agent should then be able to adapt its strategies in order to keep its performance as close as possible to the intended goals.

Wooldrige and Jennings (1995) defined intelligent agents by looking at the agent’s reactivity, proactiveness, and social ability. Using these criteria, an agent is seen as intelligent if it is able to react to changes within its environment in a timely manner, as
well as actively use the strategies available to it to achieve its objectives. Lastly, an agent is intelligent if it is also capable of co-operating with other agents, within the same problem space, to achieve its goals.

Russell and Norvig (2010) used the rationale as a defining factor for an agent that is able to adapt itself to its environment. Instead of defining ‘intelligent agents’, they defined a ‘rational agent’ as one that works to reach its best possible outcome in a known environment space; or, its expected best outcome in the event that the environmental space is unclear or relatively unknown.

Figure 7.1, which was already briefly introduced in Chapter 6, illustrates the different types of agents identified by Nwana (1996), based on the three minimum characteristics of co-operation, learning ability and autonomy. In Figure 7.1, Nwana’s version of an ‘intelligent agent’ is known as a ‘smart agent’. For an agent to be considered such, it would need to be able to exhibit some form of learning ability that would allow it to improve itself as time progressed and the agent acquired more experience.

The agent would also need to be able to share its information with other agents within its vicinity, as well as draw on information produced by other agents with which it can work. Lastly, the agent would need to be able to work without any external assistance in
order to prove itself an entity that is able to self-sustain. For an agent to be able to sustain itself, it has to, to a certain degree, have the ability to learn from its environment. The following section discusses how agents can be made to learn from their environment, and, possibly, from other agents it either works with, or competes against.

7.3 – Learning

The Merriam Webster Online Dictionary defines learning as the “activity or process of gaining knowledge or skill by studying, practising, being taught, or experiencing something”. In agent-based systems, Plaza, Arcos and Martin (2005) defined learning as the tasks an agent engages in to improve its awareness of its environment to improve in any criteria of performance. For the purpose of the dissertation, the current section will briefly elaborate on learning and how agent systems can create generalisations of an environment.

All learning activities involve its actor to actively engage in activities containing some form of feedback system that is a direct result of the actor’s actions. With the obtained feedback, new generalisations of the actor’s current situation can be made, thus allowing the actor to continuously perform actions that achieve better results, depending on the actor’s perception of the results (Plaza et al., 2005). In the world of software agents, learning happens in the very same manner when an agent is built to learn from its environment in order to better select its action strategy and improve the outcomes of its action.

Another point to take into account is that agents might not necessarily find themselves to be the only entities in an environment. Learning in multi-agent systems is also possible and might involve changes in an agent’s structure that allow it to gain knowledge from other agents it either collaborates with or competes against. For these reasons, Ren and Williams (2003) described three main categories of learning that a designer needs to evaluate when creating a learning agent.
Regardless of the type of learning method used, agents can still be classified in one of the three categories of learning. The following are the three main categories of learning (Ren & Williams, 2003):

- **Pure Single Agent Learning:**
  This applies to an agent that learns purely from changes in its own environment without the need to communicate with any other external component. This environment would contain only a single agent.

- **Multi-agent Learning in a Weak Sense:**
  Agents in this category learn not only from the changes to their environments, but also from observations made by other agents present in the environment. No interaction with the other agents is necessary as the agent only observes the behaviour of others and how the environment changes over time.

- **Multi-agent Learning in a Strong Sense:**
  Multi-agent learning in a strong sense requires communication between the different agents in the environment. The learning agent need not only observe, but also interact with other agents in order to learn their responses to different stimuli and how the environment changes over time.

According to Russell and Norvig (2010), every component of a software agent can be enhanced through learning. The major factors necessary in building learning include: the components in the agent selected to benefit from learning; the pre-learned data the agent has built-in; how the data can be used and represented in the agent; and, lastly, the feedback information the agent can use to enhance its knowledge. Learning can be attained by using one, or a combination of models.

The following are the four models of learning as explained by Russell and Norvig (2010):

- **Unsupervised Learning:**
  Occurs when the agent attempts to learn from an environment that provides no feedback on its performance.
• **Supervised Learning:**
  Occurs when an agent is able to pair its actions with their results in the environment, therefore learning the relationships between them.

• **Reinforcement Learning:**
  Is used primarily in multi-agent systems, with agents of the same type, where they are either rewarded or punished for their actions. Such a setup creates a form of competition between the agents, where they attempt to out-do each other by receiving rewards from the learning algorithm.

• **Semi-supervised Learning:**
  Occurs when software agents are supplied with datasets about their environment from which they must attempt to learn and then act.

After briefly discussing learning activities by software agents, the following subsections will be devoted to describing a few machine learning models used to help these software agents learn from their environment and make predictions of the outcomes of their actions possible.

### 7.4 – Machine Learning Models

According to Wang and Tao (2008), machine learning can be defined as a set of algorithms used to work on a real-world problems’ model by evaluating all the data readings of the model to a certain degree of probability. These are algorithms used to interpret the generic trend of events in a problem space that do not seem to be immediately noticeable. By creating a mathematical model of the problem space and obtaining data relevant to the model, machine learning algorithms are able to generalise the data to give an overview of the current situation, and, in some cases, help predict possible changes within that environment. The current section briefly describes a few machine learning models that have been used over the years.
7.4.1 – Neural Networks

Neural networks (or artificial neural networks) have been defined in many ways over the years. According to Lakshminarayam, Weckman, Marvel and Snow (2008); an artificial neural network is an "information-processing paradigm inspired by the methods by which the mammalian brain processes information". Their architecture is based on the way that the human brain is able to learn from experience. Many studies have been carried out on the use of neural networks for time-series forecasting (Crone & Dhawan, 2007).

A neural network is made up of interconnected computing units (called neurons) that send and receive signals from one another (Coupelon, 2007). This organisation of computing units is said to mimic the design of the human brain. The neurons in artificial neural networks are usually grouped into layers (namely, an input layer, a hidden layer and an output layer).

Coupelon (2007) states that neural networks were made to gain knowledge through learning. According to Kaastra and Boyd (1996), results produced by neural networks are rather insensitive to error term assumptions and they can tolerate noise better than most other statistical methods. Neural networks are designed in different manners depending on the number of layers and way in which they are organised. The following subsections briefly describe two forms of neural networks.

7.4.1.1 – Feed-Forward Neural Networks

Feed-forward Neural Networks, also called ‘Perceptron Networks’ and ‘Back-Propagation Networks’, are usually composed of a single hidden layer. The term ‘feed-forward’ serves to indicate the direction of the information flow across the network i.e. from the input to the output layer (Kaastra & Boyd, 1996). Information is processed in a one-way direction. Feed-forward Networks use supervised learning rules in their training phase.
Kaastra and Boyd (1996) define supervised learning as a process in which each of the network’s estimates are compared with already known actual values to continuously adjust the weights of the input nodes based on the estimation error in order to minimise the error function.

7.4.1.2 – Self-Organised Maps Neural Networks

Since their introduction by Kohonen (hence sometimes also called Kohonen Networks), self-organised maps (SOMs) have also been under research in a wide variety of applications (Hsu, Saeed & Halgamuge, 2009). Unlike Feed-forward Networks, this neural network model uses unsupervised learning methods.

SOMs try to reduce the number of hidden layers. They are made up of only a single input and an output layer of nodes. According to Khan, Bandopadhyaya and Sharma (2008), SOMs form part of a class of neural networks where nonlinear regression techniques are applied to discover relationships between inputs and outputs.

Lakshminarayanan (2005), states that “unsupervised algorithms perform clustering of the data into similar groups based on the calculated attributes serving as inputs to the algorithms”. Unlike Feed-forward Networks, SOMs learn from examples of the input data. Its unsupervised learning algorithm organises the network in order to find similarities in the data samples. An advantage to using SOMs comes from their ability to reduce the number of hidden nodes needed for pattern classification during training (Lawrence, 1997). Regardless of type, though, there are certain factors that limit the effectiveness of neural networks. The following subsection briefly lists some of these limitations.

7.4.1.3 – Limitations of Neural Networks

Although neural networks have proven to be very efficient, there are still some limitations when it comes to their use. Zekic (1998) identified the following limitations:

- Neural networks often require the use of large amounts of training data;
For relatively more complicated networks, the reliability of results may decrease;
- The 'best' network architecture has not yet been found.

Given the limitations of neural networks, other methods of using theorems derived from biological processes were devised. The following subsection is devoted to discussing Artificial Immune Systems as another paradigm that can be used to infuse intelligence into an agent-based system.

7.4.2 – Artificial Immune System

Artificial Immune Systems (AIS) are based on models that abstract the way the Biological Immune System (BIS) works. Development in AIS theory required the creation of different computational models that attempt to replicate the mechanisms used by immune systems when dealing with threatening pathogens. According to Dasgupta and Niño (2009), the immune system’s ability to respond faster to antigens it has faced before is one of the characteristics that has driven researchers to create different computational models that attempt to mimic the mechanism used by these systems.

In order to reach the maximum utility in the abstraction of the human immune mechanism into computational immunity, artificial mechanisms in AIS need to mimic biological processes as much as possible. The following sections will briefly discuss some of the computational models that have been created to reach this goal.

7.4.2.1 – Clonal Selection Theory

Clonal selection theory was developed to explain the process through which immune cells multiply during an immune response triggered by a recognised antigen. According

---

2 Pathogens are infectious organisms that cause disease.*
3 A substance that triggers an immune response.*
to Dasgupta & Niño (2009), clonal selection theory states that a lymphocyte⁴ in a large group of lymphocytes is selected or induced to produce clones by specific antigens. A cell (e.g. B cell⁵, T cell⁶, etc.) in the immune system that is stimulated by or, in other words, recognises an antigen, is deemed suitable for cloning in order to deal with the antigen as efficiently as possible.

The clones produced for the lymphocyte, which recognise a dangerous antigen, have the same genetic make-up as the original lymphocyte. Thus, more lymphocytes capable of dealing with the antigen are made available for a more effective immune response. Clonal selection allows for more destructive adaptive immune responses towards dangerous antigens that may invade the immune system as only cells that are able to fight it are produced in large numbers during the retaliation (Timmis, Andrews, Owens & Clark, 2008).

### 7.4.2.2 – Immune Network Theory

Immune network theory was introduced by Jerne in 1974. According to Dasgupta & Niño (2009), immune network theory attempts to explain how memory in the immune system is formed over time. The base hypothesis for this theory is that all elements in an immune system (e.g. antibodies, lymphocytes, etc.) are connected through their binding sites (i.e. epitopes and paratopes) to form what is referred to as an ‘idiotypic’ network. In this network, every entity (e.g. antibody, antigen etc.) can be bound by any other.

In an immune network, all nodes represent antibodies and anti-antibodies. As all these entities recognise each other and are not isolated from each other during immune responses (Dasgupta & Niño, 2009). Therefore, immune memory is created from all the

---

⁴ A white blood cell responsible for an immune response.*

⁵ Otherwise called B-lymphocytes and are responsible for detecting antigens.*

⁶ Otherwise called T-lymphocytes and are responsible for executing immune responses against detected antigens.*

interactions these cells have with each other based on the experience obtained during immune responses.

Timmis (2006) stated that immune networks are possible because “the paratopes located on B cells match against idiotypes on other B cells”. Therefore, the paratopes on B cells are stimulated by the idiotypes on similar B cells. This behaviour would be the same if it were dealing with a recognised antigen. In order to keep the network in a stable state, the immune cells stimulate and suppress each other during responses, and cells that recognise antigens are cloned and added to the network, while those that no longer serve a purpose are replaced by newly generated cells (Wu & Banzhaf, 2009).

7.5 – Conclusion

Chapter 6 introduced the topic of software agents on which the proposed model of the dissertation is based. To meet the dissertation’s research objectives on intelligent agents and learning techniques, the current chapter extended the discussion from Chapter 6 by examining what makes a software agent ‘intelligent’, and discussed the learning abilities of software agents. Two common overall machine learning models were briefly discussed as techniques that intelligent agents can use to learn from their environment’s data.

As discussed in the current chapter, there are multiple ways to build intelligence into agents that help them transform from being regular reflex type agents into those that are able to objectively analyse the information provided in order to make the best possible decision given the current condition of the environment.

The point is not to say that reflex agents are not good. Since they don’t use a huge degree of intelligent information processing methods, these agents can still be useful in certain deterministic environments. An analysis of intelligent agent deployment is necessary to determine how well they fit the current problem space. The next chapter is
devoted to looking at intelligent agents, and how they can be used in constantly changing environments that need them to be able to adapt to the changes.
Chapter 8
Intelligent Agents and Complex Adaptive Systems

Chapter 1: Introduction

Chapter 2: Critical Infrastructure

Chapter 3: Critical Information Infrastructure Protection

Chapter 4: The Smart Grid

Chapter 5: The Smart Grid as a Critical Infrastructure

Chapter 6: Software Agents

Chapter 7: Intelligence Enabling Machine Learning Models

Chapter 8: Intelligent Agents and Complex Adaptive Systems

Chapter 9: Agent Technology and Critical Information Infrastructure Protection

Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS)

Chapter 11: MA-SGS: Node Agents

Chapter 12: MA-SGS: Process Monitoring Agent

Chapter 13: MA-SGS: Security Response Agent Structure

Chapter 14: MA-SGS: Interoperability Agent Structure

Chapter 15: MA-SGS: Attack Agent Structure

Chapter 16: MA-SGS: Smart Grid Simulation & Model Implementation

Chapter 17: MA-SGS: Model Results

Chapter 18: Conclusion
8.1 – Introduction

One of the main characteristics of relationships is that they tend to form between independent and autonomous units working with each other within a specific environment or system, whether it is in nature or in computing systems. In a computing system, such a relationship comes about through the reactions and actions that each component has in response to a different component’s actions.

The actions taken by an individual component in a system can either be a request made to a different component in the system or a response to another component’s request. These actions always aim at achieving a specific goal. Depending on the nature and purpose of the component, such goals produce benefits to either the requesting component, the system as a whole, or the benefit of a secondary component.

Systems can be built from autonomous components that are able to interact with each other. The interactions between the autonomous components give rise to relationships between them. Such relationships can be categorised by taking into account how each autonomous component is affected (either directly or indirectly). Each autonomous component thus attempts to adapt its relationships with others in order to maintain its own optimal equilibrium or the equilibrium of the system as a whole (Sommerville, 2008).

The interactions occurring between all the different components often become complex. As each component looks for the best way to respond to changes within its environment and how much these changes can affect it, these interactions can grow. The complex behaviour developed and exhibited by each individual, when summed up with every other individual’s actions, forms a rather complex behavioural system (Tuzhilin & Kedem, 1989).

With careful analysis, patterns can be discovered in such complex behaviour, although one might still not be able to tell the exact resulting consequences of changes within the
environment (Wildberger, 1997). The current chapter is devoted to a brief study on complex adaptive systems and how intelligent agents can be used in systems such as these.

The chapter begins with an introduction to complex adaptive systems and their characteristics, and then follows on to briefly explain how such systems can be modelled. Furthermore, it looks at how intelligent agents (discussed in Chapter 7) can be modelled to fit into complex adaptive systems.

**8.2 – Complex Adaptive Systems**

Holland (1995) coined the term ‘complex adaptive systems’, defining these as those in which “the whole is more than the sum of its components”, while Greer & Martinez (2012) stated that they are “ever changing collections of non-hierarchical, distributed interacting components”.

Although a specific definition has not yet been agreed on, all focus on the point that a complex adaptive system cannot be explained by studying its individual components. Furthermore, their main defining characteristic is the emergent properties exhibited when all components work with each other in their shared environment.

The inherent complexity demonstrated through the emergent properties of a complex adaptive system is directly and positively proportional to the diversification of the agents/components in the system, as well as the degree of the interaction between them (Sherif & Xing, 2006). Figure 8.1 shows the basic architecture of a complex adaptive system. The components in the system behave in a nonlinear fashion, where their actions are not always sequential, as the most appropriate action, depending on the current condition of the environment, is taken.

Complex adaptive systems may be found in many different domains (for example, sociology, economics, biology, social networks etc.), as well as at different levels of
granularity within a domain. The biological ecosystem is one of the best examples of a complex adaptive system. Pickett & Cadenasso (2002) describe an ecosystem as a multi-dimensional concept involving the existence of mutually existing entities in an environment that strives to maintain stability. Such entities are bound to specific rules allowed by the dynamics of the environment, and are able to interact with each other to stimulate the environment. The Merriam Webster Online Dictionary defines the ecosystem as a “complex community of organisms and its environment functioning as an ecological unit”.

Figure 8.1 – Complex Adaptive System Architecture (Chuan-Jun, Hong-Bing & Shi-Yao, 2008)
Within the ecosystem, evolution is the defining process that all the different organisms went through in order to survive and keep the ecological balance in the system. Therefore, it stands to reason that, for a complex system to be adaptive, its interacting components must be able to adapt to change (Lints, 2012). Given the dominating circumstances in an environment, the components need to be able to change for an optimal and desirable equilibrium to be maintained.

Holland (1995) listed the following to be amongst the main elements that characterise complex adaptive systems:

- **Aggregation:**
  Refers to the emergent behaviour exhibited by the collection of entities included in a complex system. Behaviour in a complex adaptive system is created by the sum of the parts of the system, rather than the individual.

- **Tagging:**
  The tagging element enables each entity of the complex adaptive system to combine with others, therefore causing aggregate behaviour.

- **Non-linearity:**
  Each entity in a complex adaptive system is involved in a series of non-linear interactions with other entities in the same system.

- **Flow:**
  The flow element represents the pathways between one or more entities (created by the tagging element) that facilitate the communication between the entities. The flow element also shows the relationship between two or more entities in the complex adaptive system.

- **Diversity:**
  The diversity element refers to the wide array of entities found in a complex adaptive system. Given the nature of the system, entities of different types are necessary to work in the environment.
• **Internal models:**
  Each entity in the complex adaptive system keeps track of the internal model of the environment, which helps each entity (each to its own capacity) to predict possible responses for each of its actions.

• **Building blocks:**
  The building blocks element provides information on the basic structure of the complex adaptive system. This basic structure is used by each of the entities so that no matter how changes occur in the environment, the fundamental rules and purpose of the environment are both still maintained.

When combined, the different elements of complex adaptive systems give rise to complex emergent behaviour. Each complex adaptive system may exhibit such behaviour in different manners. Although different behaviour emerges from system to system, the main elements of such systems guide them to converge on a set of properties that define them. According to Greer and Rodriguez-Martinez (2012), the following are some of the key properties of complex adaptive systems:

• **A nested system:**
  Through careful analysis, complex adaptive systems may be referred to as systems of systems. Given all the interactions between each entity of the system, groups of elements close together can be seen as a subsystem enclosed in the complex environment.

• **Self-organisation:**
  Emergent behaviour would point to the ability of each entity in the complex adaptive system to place itself in the most appropriate level in the system, therefore re-organising itself to provide the greatest benefit to either itself or the system as a whole.
• **Connectivity:**
Through the tagging element described earlier, each entity tends to display a relationship with the others with whom it has to interact. This relationship may either be one of competition or collaboration.

• **Emergence:**
Although each entity in the complex adaptive system may seem to act randomly, emergent behaviour, not previously known, may be developed from all the interactions on the system over time.

• **Rules:**
The building blocks and internal models of the complex adaptive system may also generate certain rules that are to be followed by each entity in the environment.

• **Co-evolution:**
As the environment changes from time to time, each entity may also need to evolve to adapt in order to cope with the new environmental conditions. This evolution occurs in all entities in order to create benefit to the environment as a whole in order for each entity to simply remain relevant.

• **Sub-optimal:**
Achieving a state of perfection in a complex adaptive system is not the ultimate goal of the system. The complex adaptive system works instead to achieve optimal states given the constant changes occurring in the environment. At every environmental change, a range of states are achieved and possibly maintained for as long as the system is not at threat of collapse.

In order to understand the functioning of many different types of complex adaptive systems, researchers resort to creating computer based simulations where they attempt to model the rules that exist within these systems. Therefore, understanding the properties of a complex adaptive system is crucial if one is to design a computational
model to replicate it. The next section of the chapter briefly looks at how complex adaptive systems can be modelled.

8.3 – Modelling Complex Adaptive Systems

Modelling complex adaptive systems, and their environments, requires a method of creating individual components that are able to interact with each other. Agent-based models have been viewed as an appropriate approach to represent complex adaptive systems (O'Reilly & Ehlers, 2006). The ability to create agents to work as the individual components within complex systems is one of the main reasons why they have been used.

Studies of complex systems whose rules are not derived from other rules dominant in natural systems (e.g. thermodynamics, biology etc.) cannot be studied by popular laws. To address this, Haghnevis & Askins developed a framework for designing and studying complex adaptive systems as shown in Figure 8.2.

The framework in Figure 8.2 basically looks at the individual properties of the components in complex systems, and from there shows how the emergent properties and characteristics of the system as a whole are defined. Table 8.1 describes the main features of Hagnevis & Askin's (2012) framework that should be considered in the design of a complex adaptive system.

When designing a complex adaptive system, the features described in Table 8.1 can be used as the elements to consider. The features can also be used to make decisions regarding the interactions between the different autonomous components in the complex system in question. With this in mind, the following section examines how intelligent agents can be modelled to work in complex adaptive systems.
Figure 8.2 – Framework for Engineered Complex Adaptive Systems (Hagnevis & Askin, 2012)

<table>
<thead>
<tr>
<th>Framework Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Takes into account the individual components of the system and their internal properties and diversities that make them different from each other.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The communication and interaction between each of the individual components of the system give rise to the overall emergent properties of the complex system. On the interoperability profile of the system, one can identify how the system behaves based on how the components work with each other.</td>
</tr>
<tr>
<td>System Traits</td>
<td>On the traits’ profile, designers include the possible ways in which new states of equilibrium can be achieved, while taking into account how each of the individual components evolve. Certain values that can be measured are included in the system’s design in order to determine the magnitude of the changes to the system.</td>
</tr>
<tr>
<td>Learning</td>
<td>Flexibility, robustness and the adaptability of complex adaptive systems owe their existence to the system’s ability to learn from its previous situations in order to deal with its dynamic and unpredicted states.</td>
</tr>
</tbody>
</table>

8.4 – Modelling Intelligent Agents for Complex Adaptive Systems

Given the framework discussed in the previous section, complex adaptive systems need to be modelled using components with the capability to act independently, based on changes to the environment, as well as work with other components within the system. These components need to be able to adapt to their environment and follow set rules that may change, given their current knowledge of the environment. Figure 8.3 shows
how the author of the dissertation proposes the features taken into account during the study, design and analysis of complex adaptive systems can be fulfilled through the use of intelligent agents.

![Figure 8.3 – Suitability of Agents for Complex Adaptive Systems](image)

When looking at the features necessary for each component to work in a complex adaptive system, software agents possess the necessary properties. A software agent has the ability to capture information on its environment, and, through its rationality component, make an appropriate deliberation based on its purpose and its current knowledge on how to best select its actions. A software agent has the ability to consistently go through this process whenever required to act upon its environment (Khalil, Abdel-Azizm, Nazmy & Salem, 2014).

As discussed in section 8.2, complex adaptive systems are composed of a diverse set of entities that can work together in the environment. Software agents are capable of working in an environment shared with other agents. Such agents are able to work in a
multi-agent environment, where each agent is able to react both to changes in the environment as well as other agents with which it is related.

As discussed in Chapter 7, an agent may be given the ability to learn from its actions, changes in the environment or actions by other agents in the environment in order to increase its effectiveness. Multiple models for learning have been developed in order to allow software agents to learn, adapt and respond to changes in a complex adaptive system. If working in a collaborative complex system, a software agent may share the knowledge, which it has gathered over time, with others in the environment.

The traits exhibited by complex adaptive systems demonstrate that the components of the system exhibit emergent behaviour that makes way for multiple paths to reach a sub-optimal equilibrium. With the ability to either work with others, compete or communicate, software agents may also demonstrate emergent behaviour in their quest to satisfy the goal they were built to achieve.

The literature study carried out until this stage uncovered the properties of software agents that allow them to be used in an appropriate methodology to check the boxes of the features existent in complex adaptive systems. Although the properties of agents make them suitable for designing and modelling these complex systems, one should still consider the defining characteristics of the problem domain (or environment) in order to determine the properties which should be more prominent to the individual agent point of view.

8.5 – Conclusion

Given the nature of complex adaptive systems, using intelligent agents can be seen as an appropriate solution or method for creating the complex interactions between the systems’ components where different events can be triggered. Apart from being used in creating plausible simulations, intelligent agents can also be used to model the different
entities that are often found in such environments, although one needs to first understand the goals of different entities in order to create an appropriate model.

Seeing that Critical Infrastructure Information Systems are bolstered by a wide range of autonomous systems that work together to keep the functioning of the system as a whole stable, these can be seen to behave as complex adaptive systems. Therefore understanding complex adaptive systems, which was the purpose of the current chapter, is crucial if one is to design any model to work on Critical Information Infrastructure Systems.

Multi-agent systems were identified as an appropriate model to design systems that mimic the inner workings of complex adaptive systems. Thus it can be said that multi-agent models can be used to design systems that work on Critical Information Infrastructure, whether it is to simulate the workings of a Critical Infrastructure, or perhaps monitor and actively work to keep the Critical Infrastructure stable. The following chapter is devoted to looking at a few examples of Critical Information Infrastructure Systems that made use of agent technologies in one way or another to help manage the infrastructure.
9.1 – Introduction

As discussed in Chapter 8, agent technology can be seen as a viable paradigm to use in the design of complex adaptive systems. Taking the complex nature of Critical Infrastructure into account, agent-based models used for modelling and simulating these Critical Infrastructures have proven to be useful in the understanding of Critical Infrastructure interdependencies (Casaliccio, Galli & Tucci, 2007).

The flexibility in the design of agent-based models is one of the main reasons why they can be used to simulate complex behaviour in Critical Information Infrastructures. According to Lin, Sedigh & Hurson, agent-based systems provide the ability to concentrate various aspects of complex operations into a single agent, while still allowing the use of multiple other agents. When combined, the agents are able to produce the interdependencies observed in complex environments (2011).

Another less popular reason for the use of intelligent agents on Critical Information Infrastructures has to do with the cost savings. The total cost of ownership can be greatly reduced by automating system controls using agent-based systems. Maintenance can be carried out without much intervention of human controllers since the agents on the system can perform all the necessary tasks (Logan, 2005).

The current chapter is devoted to looking at a few other research projects in which agent-based models were used to different degrees in Critical Information Infrastructure protection. The chapter begins by briefly describing a few research studies where agent technology has been looked into as the implementation platform for Critical Information Infrastructure protection. The chapter goes on to describe agent frameworks that have been designed for the Critical Information Infrastructure protection.
9.2 – Application of Agent Technology in Critical Information Infrastructure Protection

The flexibility property of agent-based models requires their users to begin by understanding the problem domain and structure it in such a way that each feature of the domain can be packaged in an independent and autonomous software agent. The environmental factors that determine the success or failure of an agent when achieving its goals can be used to create a software agent that is deemed to be intelligent (Baig, 2012).

According to Weiss (1999), multi-agent systems or models based on agent technology can be applied to a wide variety of fields such as, among others, electronic commerce, air traffic control and network intrusion detection. Given the list of applications in which agent technologies have been used, it doesn’t become such a far-fetched idea to apply such technologies in Critical Information Infrastructure.

The Automated Threat Response using the Intelligent Agents System (ATRIA), developed by Quan, Crawford and Shao (2001), is an implementation of agent technology to solve a real-world complex problem. The main aim of the system was to address the rapidly changing communication and asset control needs that occur in a battlefield situation.

The ATRIA system fulfilled these needs by deploying a set of intelligent agents that would take control of each of the assets connected (data resources, weapon systems, scheduling resources) in the communication infrastructure. The agents provided connectivity, interoperability, and control over the allocated assets (Quan et al., 2001).

The Immunity Inspired Smart Grid Protection Model (IISGP), designed by Mavee and Ehlers (2012), interpreted the power grid as a complex adaptive system which could be modelled on the human immune system. Therefore immunity-based methods (such as
those discussed in Chapter 7) were used to monitor and maintain the integrity and stability of the power grid.

Health systems can also be regarded as Critical Infrastructure when the nature of the information being handled and the consequences that could arise, if they are taken down, are taken into account. Bergenti & Poggi made use of recent technology, as well as the Internet, to provide a new variety of health care services as E-health (2009).

E-health systems mainly provide an effective platform for the exchange of information between consumers and service providers. According to Baig (2012), such information systems deal with heterogenous data that requires the use of multi-agent systems to help integrate and disseminate the information effectively. Such multi-agent systems can also be used to protect the important and confidential patient data. Security controls using multi-agent systems could, to a certain extent, be applied in the access control modules of E-health systems.

Multiple applications can be developed for Critical Infrastructures using a multi-agent model. The multi-agent systems may be built differently due to the different characteristics of each Critical Infrastructure. Different design decisions may need to be taken to consider the different attributes of the Critical Infrastructure. Therefore different applications that are based on different principles may need a basic blueprint from which they are built. The following section is devoted to looking at a few agent frameworks created to aid in the development of agent-based applications for different Critical Infrastructures.

9.3 – Agent Frameworks for Critical Infrastructure

According to Mattsson and Bosch, a framework can be defined as “an abstract design and implementation for an application in a given problem domain” (1997). It essentially is a foundation on which solutions for a specific type of field are built.
The framework will contain all the necessary components which the solution must have, or can use if need be, to achieve its goals. Each of these components are standardised enough so that all solutions to the problem domain work well within their environment. When testing for interdependencies between different Critical Infrastructures, simulation systems are built, and disturbances are caused on the simulations in order to analyse any changes in operation. One of the problems with such simulations is that, in order to gather realistic results that would explain what would happen in a real environment, the simulations of all Critical Infrastructures would need to exhibit behaviours that are similar to what happens in real systems (Creese, Goldsmith & Adetoye, 2011).

Frameworks can be developed for multiple fields, and for better granularity at different levels on the same field. Agent frameworks can be developed to create an accepted format in which software agents can be created for an agent-based system.

The same concept holds if a framework is developed to facilitate the creation of agent-based systems that solve a specific problem. The following two subsections briefly look into generic agent development frameworks and agent-based platforms that have been developed to aid research towards securing Critical Infrastructure.

### 9.3.1 – Agent Development Frameworks

According to Rahman, Armstrong, Mao & Marti (2008), most of the simulation frameworks for use in Critical Infrastructure are based on agent technology. During such simulations, autonomous agents take the place of each component in the infrastructure and are set to interact with other components that are related to it.

A trend in the creation of simulated environments is the use of readily existing software tools. The use of readily available simulation tools, and agent based frameworks is referred to as ‘federated simulation’ (Huang & Miller, 1999). Table 9.1 is a list of a few agent-based frameworks and tools that have been used to simulate and build agent-based models.
Table 9.1 – Tools and Frameworks for the Development of Federated Simulations

<table>
<thead>
<tr>
<th>Tool/Framework</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Agent Development Framework (JADE)</td>
<td>JADE is a fully FIPA (Foundation for Intelligent Physical Agents) compliant framework, based on the Java platform that aids in the creation of software agents that are able to work on multiple platforms (Fortino, Garro &amp; Russo, 2007). Furthermore JADE provides a standardised architecture that can be used to build software agents that act as middleware to integrate a distributed platform composed of heterogeneous components (Zhao, Bekkiynm, Kaatm, Adriaans &amp; Hertzberger, 2007)</td>
</tr>
<tr>
<td>Java Intelligent Agent Componentware (JIAC)</td>
<td>JIAC is an agent development framework made to support multiple standards and custom extensions to aid in the development of multi-agent systems (Lutzenberger, Konnerth, Kuster, Tonn, Masuch &amp; Albayrak, 2014)</td>
</tr>
<tr>
<td>Nessi2</td>
<td>Nessi2 is an agent-based simulation environment used to test possible network security scenarios on different network setups (Grunewald, Lutzemberger, Chinnow, Bye, Bsufka &amp; Albayrak, 2011). Nessi2’s software agents are based on the JIAC framework, and the simulation tool can be used to build scenarios witnessed in Critical Information infrastructure to test how resilient the system can be.</td>
</tr>
</tbody>
</table>

Each of the frameworks and tools listed in Table 9.1 allows for the creation of multi-agent systems. When considering which one to use, one should first look at the problem domain, while also considering Wooldrige’s (2003) four requirements for any multi-agent system:

- **Situated behaviour:**
  All agents in the environment should be able to detect any event to which they must be able to promptly respond;

- **Goal-directed behaviour:**
  All agents should be able to have a set collection of achievable goals that are easily verifiable after any action has been executed;
• **Efficiency:**
  All agents should be equipped with all necessary features that allow them to carry out their actions within the constraints that bind them;

• **Coordination:**
  Any individual agent should be able to either cooperate or compete with other agents in the same environment.

Agent technology presents designers with a wide array of tools that can be used to develop flexible systems to test different theories and scenarios that affect complex systems such as Critical Information Infrastructures. The following subsection briefly touches on some platforms that have been developed to evaluate Critical Information Infrastructure.

### 9.3.2 – Critical Infrastructure Security Platforms

Being such an attractive model for designing systems for Critical Infrastructure, agent based models have received attention from researchers building systems to both monitor and protect such important assets. Yusta et al. (2011) noted that another reason why agent technology has gotten so much attention is due to its ability to expose certain interdependencies between Critical Infrastructures that may have not been clear before.

The following list briefly looks at a few agent based platforms created to model and simulate Critical Infrastructure as identified by Yusta et al. (2011).

- **Agent-based Infrastructure Modelling and Simulation (AIMS):**
  AIMS is a software tool developed by the University of New Brunswick to assess water systems in urban areas to identify vulnerabilities caused by the interdependencies existent between Critical Infrastructures.

- **Critical Infrastructure Protection Modelling and Analysis (CIPMA):**
  CIPMA is a software tool developed by the Government of Australia to identify and evaluate relationships and dependencies between Critical Infrastructures, and how failures can cascade from one to another in case of a disruption.
Critical Infrastructure Simulation by Interdependent Agents (CISIA):

CISIA is a software tool also developed by the University of New Brunswick used to simulate Critical Infrastructures through the use of software agents in order to identify the effects of decisions made on Critical Infrastructure or any kind of disruptions.

In order to appropriately secure Critical Infrastructures, complex system behaviour must be studied under different conditions (e.g. interactions, stress, or attack) to enable system designers to develop solutions that are able to get to the root cause of the problem that initiates such system behaviours (Casaliccio, Galli & Tucci, 2007).

The agent platforms seen in the current section, and many others which have been developed, were built to discover interdependencies not immediately apparent in an environment. Agent-based methodologies were selected as the main underlying technology of the frameworks for their ability to model the different components found in Critical Infrastructure.

9.4 – Conclusion

According to Ouyang (2014), agent-based models can be used to mimic the behaviours of the main participants in the management of interdependent Critical Information Infrastructure. Such models allow a designer to represent different control structures used by decision-makers as agents in order to better study the effect of any action. Before agent-based models are built, though, frameworks should be consulted to get a better idea of what design decisions should be made.

Having standardised frameworks for designing systems to work on Critical Infrastructures can prove to be very useful as these often come with documentation detailing the reasoning for certain design decisions, helping designers to better structure their models. Understanding the main requirements of an agent-based system is necessary to make sure that all aspects are covered when designing a model.
The current chapter briefly discussed agent frameworks and how they are seen to be suitable for use when building models to work on Critical Information Infrastructure. The following chapter introduces the proposed agent-based model to be applied in Critical Information Infrastructure protection, using the smart grid as the critical infrastructure environment.
Chapter 10
Multi-Agent Model for Smart Grid Security (MA-SGS)

Chapter 1: Introduction
Chapter 2: Critical Infrastructure
Chapter 3: Critical Information Infrastructure Protection
Chapter 4: The Smart Grid
Chapter 5: The Smart Grid as a Critical Infrastructure
Chapter 6: Software Agents
Chapter 7: Intelligence Enabling Machine Learning Models
Chapter 8: Intelligent Agents and Complex Adaptive Systems
Chapter 9: Agent Technology and Critical Information Infrastructure Protection
Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS)
Chapter 11: MA-SGS: Node Agents
Chapter 12: MA-SGS: Process Monitoring Agent
Chapter 13: MA-SGS: Security Response Agent Structure
Chapter 14: MA-SGS: Interoperability Agent Structure
Chapter 15: MA-SGS: Attack Agent Structure
Chapter 16: MA-SGS: Smart Grid Simulation & Model Implementation
Chapter 17: MA-SGS: Model Results
Chapter 18: Conclusion
10.1 – Introduction

The literature review carried out until this point set to add background information for the model defined in the dissertation. The current chapter is devoted to describing the overall components of the multi-agent model. The following chapters, on model construction & overview, of the dissertation will further explain each aspect of the model. Before the model is first introduced, a brief re-visit to the research questions of the dissertation is in order.

In the creation of the model for the defined problem statement, the dissertation attempts to answer the following questions:

- **Question 1**

  *Can intelligent agents in multi-agent systems be used in Critical Information Infrastructure protection?*

  Up to this point of the dissertation, one could say that it is plausible that multi-agent systems can be used in Critical Information Infrastructure protection. Critical Infrastructure was determined to be a form of a complex adaptive system, and from Chapter 8 it was discussed how software agents are suitable to work within a complex adaptive system environment. Given that complex adaptive systems are composed of many entities, multiple communication software agents may be deployed within one to enable the exchange of information between the entities.

  The versatility of software agents was discussed in Chapters 6 and 7, therefore noting that such agents may be deployed in multiple fields in different forms. Security is one of the purposes which software agents could be built to enforce. Since Critical Infrastructure requires adequate and consistent security measures, software agents developed to enforce security could be deployed within Critical Infrastructure information systems. Question 1 will be re-visited at the end of the dissertation.
• **Question 2**

*How can multi-agent system theory be applied to the smart grid?*

As discussed over Chapters 4 and 5, the smart grid can be seen as a Critical Infrastructure due the services it provides to all those that are connected to it as well as the effects it has on the demand centres to which it supplies electric power. As a relatively new paradigm of Critical Infrastructure, its protection is of the utmost importance if the smart grid is to succeed the traditional power grid.

Since software agents can be deployed in Critical Infrastructure Information Systems, the smart grid is a prime candidate for the use of multi-agent systems. A multi-agent system can be used to control the dispersed multitude of components found in the smart grid, and can also be used to maintain the security and integrity of the smart grid. Question 2 is re-visited at the end of the dissertation describing how a multi-agent environment was made to work within the smart grid and some of the practical implications of such an approach.

• **Question 3**

*As a follow up of Question 2; how would the security, resilience and robustness properties of the Smart Grid’s Critical Information Infrastructure be improved with the use of a multi-agent system?*

At the current point of the dissertation, multi-agent systems seem to be a solution that will indeed add to the security, resilience and robustness properties of the smart grid’s Critical Information Infrastructure. Question 3 is also re-visited at the end of the dissertation to report on the suitability of the proposed multi-agent model in the protection of the smart grid’s Critical Infrastructure.
The following sections of the chapter introduce the model by first discussing the rationale behind the characteristics of the model. An overview of the model is then introduced. The model is then broken down into its main components and further discussed.

10.2 – Model Construction Rationale

Multi-agent systems could be seen as a plausible solution when looking at complex systems composed of multiple features. Complex systems call for the use of multiple agents that can be used to solve a single problem. Different agents deployed in the system (or environment) are given different tasks associated with solving the problem so that, through communication and coordination with the other agents in the system, an optimal solution for the problem being dealt with can be found.

Complex adaptive systems need to be modelled using components with the capability of acting on their own based on changes to their environment, as well as working with other components within the system. These components need to be able to adapt to their environment and follow set rules that may change, given their current knowledge of their environment.

For the purposes of the dissertation, based on the literature study of the problem domain and the use of software agents, the following steps were identified to be necessary in the construction of the resulting model:

- **Step 1**: Define the network environment;
- **Step 2**: Identify the different components that exist in the environment;
- **Step 3**: Define a measure for equilibrium, and what is deemed an acceptable state within the environment;
- **Step 4**: Define each component’s set of goals, sensors, actuators and performance measures;
• **Step 5:** Identify and define the direct and indirect relationships between each of the existing components of the system in order to establish the necessary communication lines;

• **Step 6:** Define the ability for knowledge-creation and application;

• **Step 7:** Determine and initiate the sequence of activities that give way for dynamic actions with the aim of keeping an acceptable environment state.

The first version of the MA-SGS model was first defined and designed in the paper entitled “Enhancing Security on the Smart Grid Environment – A Multi-agent Approach”. The paper was written by the author of the dissertation and was presented at the Tenth Tools and Methods of Competitive Engineering (TMCE) 2014 International Symposium.

The chapter continues on to provide an overview of the Multi-Agent Model for Smart Grid Security (MA-SGS) followed by a brief introduction into the different software agents that are used in the model by discussing their purposes and how each is structured to achieve these.

### 10.3 – Model Overview

The multi-agent model uses a series of agents to support communication and coordination actions that aid the security tasks of the smart grid’s information system. Achieving these goals with the use of multiple agents enhances the ability of the smart grid to provide better control of the usage of electricity, thus taking a step forward in providing sustainable energy.

In order to set up the multi-agent model, the smart grid would need to be broken down into a set of components that can be computationally modelled to be the working environment of the agents. The setup of the smart grid environment is based on a version of the conditions used in the study done by Dong, Xiong, Hou, Dong and Nyberg (2011).
The set-up of the environment is as follows:

1. **Smart Grid Components:**
   Each of the components on the smart grid (the generation plant, the distribution substations, transformers, and consumption centres) is represented as a node of the network with relevant data structures that show differences in their basic properties.

2. **Network Edges:**
   The transmission lines, branching from each of the components of the smart grid, are represented as the edges connecting each of the network’s nodes. The edges represent the two-way communications that exist on the smart grid, therefore forming a mesh network.

3. **Topological Features:**
   The topological features, of all the electric power transmission lines connecting each node, are considered to be the same (e.g. length, material, etc.). Therefore, the focus of the environment is purely based on the information transfer capabilities of the grid. The inherent differences existent in the properties of the physical communication lines are not taken into account in the model.

4. **Smart Grid Power Transmission Effects:**
   Both the effects of power transmission networks and distribution networks are considered, given that the nodes existent in the network represent most components on the grid.

5. **Physical Structures:**
   The physical structures of the transmission lines and real-life electric parameters of the smart grid are ignored in order to simplify the simulation environment.
6. **Simulated Graph:**

The model will use a simplified graph in order to remove any self-loops on each node. As the graph should support two-way communication between each node, it will work as a mesh network.

7. **Smart Grid Component Connections:**

The model takes into consideration the main information exchange connections existent in the smart grid network. All grid components that are connected to each other are capable of exchanging data. The exchange of data defines the form of interaction between the network’s nodes.

10.3.1 – **Overall Model Simulation**

The multi-agent model is tested on a simulated smart grid environment, where each node is made to behave as a part of the smart grid. Each node of the simulated smart grid represents either a power generation plant, transformer substation, microgrid substation or a consumer. Each node operates as an independent unit that is still able to communicate to others adjacent to it.

At each node of the simulation network, the MA-SGS model deploys a combination of the following three agents:

- Process monitoring agent;
- Interoperability agent
- Security response agent.

The agents work towards maintaining an acceptable state within the node in which they are deployed. Figure 10.1 shows the simulation environment of the MA-SGS model with multiple agents deployed at each node.
The model begins with an initialisation of the simulation environment and the component nodes of the system. After initialisation is complete, each node works towards analysing the existing demand-supply ratio of power within and outside the node in order to identify any trends. Commands and events executed at each node are logged and monitored.

Trends are analysed by the MA-SGS agents within the node in order to determine the current status of the node and any actions necessary to keep the node’s status as functional. Any changes within the environment that are detected by the agent are stored for reference should situations of the same kind occur again.

The MA-SGS agents work on each node to keep the simulation smart grid network stable. In order to test whether the model’s agents work according to their purpose and are capable of maintaining stability in the simulated network, another agent is introduced to test the model. The following subsection briefly describes the test agent.
10.3.2 – Attack Agent

In order to test the model’s ability to keep the simulated smart grid environment stable, a proof-of-concept agent is developed to introduce disruptions into the operation of the smart grid. The attack agent’s purpose is to create situations within the environment that can cause the model’s agents to engage courses of action to restore the smart grid back to its functioning equilibrium state.

The attack agent creates disruptions which should be overcome by the node. The red node in Figure 10.1, showing a single agent, is an illustration of an attack agent deployed in the simulated smart grid environment. Chapter 15 provides a further discussion on the purpose and functioning of the attack agent. The current section introduced an overview of the MA-SGS model and the attack agent. It described the aspects of the model to make the concept clearer. The following section discusses how the model is designed to work at the node level of the simulated smart grid network.

10.4 – Network Node Structure

As mentioned in section 10.3, each node in the simulated smart grid receives a set of three agents. Each agent in the node is responsible for a specific task. Together these agents monitor the node’s internal operations as well as the interactions with the adjacent nodes.

Each agent within a node can be said to be generic. During a simulation, each node agent will be tuned to work with the defining properties or characteristics of the node in which it is deployed. For example, agents working on a power generation node will work differently from those working on a power consumption node. The reason why the agents are generic is so that they have a similar structure which makes it easier to change their adaptations in the model. Figure 10.2 shows the agents that are found in each node.
In other research projects where the power grid was studied and simulated, each node on the network was assumed to be a single agent that then connects with other adjacent node agents in order to create the grid (Dong et al., 2011). The method is efficient when testing the reliability and survivability of the network when unexpected events eliminate nodes on the network (Dong et al., 2011).

In contrast, the MA-SGS model taps into the self-regenerating and knowledge-sharing capabilities of agent systems. It infuses a series of agents, which, given simple rules, are able to work with each other in order to manage a single node. This way, every existent node on the network is constructed with the same set of agents, although emergent behaviour might result in each one. The following subsections give a brief introduction of each of the components found in each node and how they are classified based on their purpose and behaviour in the given environment.
10.4.1 – Process Monitoring Agent

The process monitoring agent (PMA) is the agent in charge of monitoring internal processes and commands on the node that owns it. The agent is built to analyse all event and command logs created in the node in order to flag possible actions that could threaten the stability of the node.

10.4.2 – Security Response Agent

The security response agent (SRA) records information produced by the process monitoring agent in order to determine an appropriate course of action to keep the node functioning normally. All operations initiated by the SRA are logged in the node’s data store.

10.4.3 – Interoperability Agent

The interoperability agent (IA) is in charge of coordinating the actions between each of the agents within the node, as well as facilitating communication with other adjacent nodes.

In addition, the interoperability agent keeps track of node states. The agent monitors both the state of the node and of the adjacent nodes. This way, the node is informed of the states of its adjacent nodes, and any changes may warn it of a possible situation it should avoid.

10.4.4 – Database Store Module

To keep track of historical events in the simulated smart grid network, each node has access to a data store where all event and command logs are stored. The IA is responsible for storing such data for use by the SRA and PMA.

The data available in the data store is recorded across simulation runs to be used as training data for the SRA and PMA. Both agents can learn data patterns from previous
simulations to help improve their performance in detecting and responding to events and commands that can possibly compromise the stability of the node in which they are deployed.

The current section briefly described the different types of agents and components found in the MA-SGS model. Given that all the MA-SGS agents are said to be generic in terms of structure, the following section introduces the structure which all agents are built on.

**10.5 – Individual Agent Structure**

Through this setup, one finds a multi-agent system at the node level where each agent has a specific purpose to contribute towards the overall goal of the system. Each agent is equipped with internal components that make them autonomous in terms of their activity, but still social as they are able to liaise with the other agents within the node. Figure 10.3 shows the internal structure of each of the agents in the proposed model.

![Figure 10.3 – Internal Agent Structure](image-url)
10.5.1 – Sensor Component

Each agent needs to be able to sense changes within its environment. The sensor component is then used to retrieve environmental values that are relevant to the agent.

10.5.2 – Information Processing Component

Agents should be able to process and evaluate information before making decisions. Therefore the information processing component will be configured with the aim of the agent as well as with the type of information each specific category of agent will be using.

The information processing component will allow agents to communicate with each other through a standardised communication interface. The component should also allow the agent to be given a simple set of rules that it can execute based on its current state.

10.5.3 – Internal State Component

The agent needs to be able to indicate its current state. Information about the agent’s state can be made available to other surrounding agents in order to help detect whether it is available for any computation or not.

10.5.4 – Actuator Set Component

The rule set embedded in a software agent is mostly useful when the agent is able to act on the decisions deliberated. The actuator set component includes the methods the agent can use to change values that contribute to it achieving its intended goal(s), given the rule set that is to be followed.
10.6 – Conclusion

Although a relatively new technology, which at the moment is not yet widely used around the world, the smart grid is proving to be the next step in power grid development. With a new mindset of how electric power should be managed and distributed, as well as a more integrated strategy on making use of cleaner energy, it can be classified as a Critical Infrastructure.

As the developments on the smart grid push forward in providing valuable services to consumers, concerns of how reliable it will be and how secure it is always arise. Given the complex nature of the smart grid and its inherent ability to sustain its grid-wide operation through self-healing and robustness properties, it is a subject that draws many researchers to continuously improve it (Greer & Rodriguez-Martinez, 2012).

The MA-SGS model applies a multi-agent setup as a new strategy to improve reliability on the smart grid’s ability to handle strenuous situations. At the lowest level of granularity, the model uses the multi-agent environment at each node in the smart grid network. Furthermore, the model enables each node of the network to work with others, by allowing them to communicate with other closely surrounding nodes.

At the innermost level, the model applies a multi-agent environment at each of the nodes of the network, then, at outer level, all nodes are able to interact with each adjacent node in order to exchange information and energy between them. Chapter 11 goes on to describe each of the agent types in the multi-agent model. Chapters 12, 13, 14 and 15 describe each of the agent types found in the model at length. Chapter 16 describes the implementation of the smart grid simulation environment and the prototype of the MA-SGS model.
11.1 – Introduction

The proposed model is based on the use of multiple agents to monitor and secure the information infrastructure of the smart grid. Chapter 10 gave an overview of the proposed model, paving the way for more defined descriptions of each model component in the subsequent chapters.

The network is modelled in such a way that each node within it is composed of a set of agents that will manage its internal functions to provide methods for securing each node as well as for creating information that can be used across the entire network.

Information used by the different components refers to messages, commands and event logs recorded at each node of the network. For the purpose of this study, these will be referred to as data records for the remainder of the dissertation. Only if necessary will such data records be explicitly called by their respective type.

Figure 11.1 illustrates the agent structure of each node in the network. Each of the following sections will briefly describe each of the agents in the model in terms of its purpose and its own internal structure.

![Figure 11.1 – Internal Node Structure](image-url)
11.2 – Node Agent Types

Given that the MA-SGS model uses multiple agents at each of the nodes in the smart grid, each agent takes a specific responsibility in securing the network. Each type of agent in the model is composed of a sensor, information processing, internal state and actuator set component. The following subsections briefly describe each agent, and, furthermore, explain the function of each component of the agent (as shown in Figure 10.3).

11.2.1 – Process Monitoring Agent

The process monitoring agent (PMA) is a reflex and knowledge based agent in charge of checking internal processes and commands sent to and sent by the node in which it is deployed. It monitors them in order to classify information exchange within the node and actions on the node. The following subsections briefly describe the components of the PMA.

11.2.1.1 – Sensor Component

The process monitoring agent analyses internal records processed by the node, as well as records passed to the node from external sources. Its sensor component has the ability to retrieve information from the record stack kept by the node’s interoperability agent. It is essentially used to communicate with the node’s IA to make data requests.

11.2.1.2 – Information Processing Component

Through examining the records processed by the node, the process monitoring agent’s information processing component learns the data patterns it observes and matches these data patterns to the operational status of the node.

Analysis of the node’s data patterns allows the PMA to create a profile of the node. Any new stream of records that deviate from the node’s profile, or a stream that does not match the node’s regular data patterns, may be flagged as a potential anomaly to be analysed by the security response agent.
11.2.1.3 – Internal State Component

The agent’s internal state component keeps track of the operations of the PMA. The operations of the PMA are applied to the records logged by the agent’s information processing component.

Results obtained by analysing the records determine the agent’s current internal state. The results may indicate whether the agent has detected a potential threat to the node or if records show no signs of an imminent security issue.

11.2.1.4 – Actuator Set Component

The process monitoring agent’s task is to monitor internal and external data records passing through the node. In order to carry out these tasks, its actuator component is built to enable it to carry out the following actions on the node:

- Retrieve data records;
- Initiate learning;
- Classify data records;
- Analyse data records;
- Flag records based on analysis results;
- Store newly found knowledge;
- Query previously created knowledge;
- Update agent internal state.

11.2.2 – Security Response Agent

The security response agent (SRA) is a reflex, knowledge and goal based agent in charge of performing security analysis on records that have been flagged by the PMA. From analysing flagged records to determining whether the node is indeed under a possibly compromising situation, the agent determines the course of action to take to keep the node’s appropriate operational status. The SRA does this by also making use of an adaptive rule set which is determined by the type of node in which the agent is deployed.
11.2.2.1 – Sensor Component

The security response agent monitors the internal state information kept by the PMA in order to determine when it should act. The SRA’s sensor component regularly requests the interoperability agent for any internal state changes in the PMA that may warrant the SRA to act.

Changes in the PMA’s internal state that indicate the existence of a flagged data record trigger the sensor component to request the record from the interoperability agent for analysis.

11.2.2.2 – Information Processing Component

The agent’s information processing component retrieves log records flagged by the PMA. When retrieved, the component analyses the records based on its current situational awareness of the node to classify the flagged records. Analysis of flagged records is based on: their attributes, time of occurrence, origins of records and the current status of the node.

After analysing the record, the information processing component updates the data store with the newly discovered classification information. The information processing component of the SRA is responsible for learning to classify and identify records that can compromise the functioning of the node. The component learns to determine if flagged records are part of the following classification of messages:

- True positives (flagged records that indeed could compromise the operations of the node); or
- False positives (flagged records that were classified not to affect optimal operations of the node).

11.2.2.3 – Internal State Component

The internal state keeps track of common features that the agent’s information processing component’s classification algorithm has identified. This is done to make the information readily available when continuously processing new data. Such data can
also be used to make information available to the external MA-SGS environment to share knowledge between different nodes.

The SRA’s internal state component also provides the current security status of the node in which the agent is deployed. This information is made available to the interoperability agent in case an external node requests for the status of the node.

11.2.2.4 – Actuator Set Component

The actuator component needs to be able to take action based on any result of the information processing component. The SRA acts on the flagged command and processes it in order to determine what is to be done on the node in order to keep it functioning at an optimal state. Depending on the information processing component output, the agent undertakes a particular action as outlined in Table 11.1.

<table>
<thead>
<tr>
<th>Output</th>
<th>Possible Action</th>
</tr>
</thead>
</table>
| **True Positive** | Identify message properties and update knowledge base for value ranges found on messages identified to be malicious;  
Identify appropriate action to restore node to optimal operating status. |
| **False Positive**| Identify message properties and update the knowledge based for value ranges found on records that would not have any effect on the operation of the node.  
Make the information available in the data store so records that fall in the same threshold are no longer flagged. |

11.2.3 – Interoperability Agent

The interoperability agent (IA) is a reflex agent in charge of the internal and external communication of the node. The IA is there to handle all communication between each
of the agents on the node in order to help coordinate their actions. It also works as the agent that receives and forwards commands in the node.

The interoperability agent also keeps track of the current state of the node, as well as the state of flagged messages by the process monitoring agent on the node. The state of the node is made available for access by both internal and external agents. The content flagged by the agent is always indicated for the agents in the adjacent nodes on the system. The following subsections describe how each of the components of the IA works together.

### 11.2.3.1 – Sensor Component

The IA’s sensor component keeps track of the nodes connected to the one in which it is based. The agent keeps track of the types of surrounding nodes as well as their current operation status. The sensor component monitors the state information on the nodes adjacent to the node in which it is situated. It constantly checks on the state of the other nodes in order to keep track of the changes they go through.

In order to enable communication, the interoperability agent’s sensor component also listens for internal and external communication requests. Internal communications refer to those where the PMA and SRA need to exchange information. External communications are those where information exchange requests come from the surrounding nodes.

### 11.2.3.2 – Information Processing Component

The IA exists purely to keep track of the model’s messages. The IA’s information processing component is used whenever the sensor component has a communication request to execute. Before information is exchanged, the information processing component checks whether the request can be completed at that time.
The IA constantly requests the state information for each of the surrounding nodes, and monitors the changes of the state of these nodes. The agent then builds a state profile for each of these nodes in order to attempt to identify changes. Information on the surrounding node’s generated profile is available to the SRA and PMA within the node. This information is used as part of the exploratory process of determining a course of action by MA-SGS agents within each node in the simulated smart grid.

11.2.3.3 – Internal State Component

The IA agent can have one of two possible internal states. It can either be active or inactive, therefore indicating its ability to handle messages. An inactive communication agent could be a signal for a non-functioning node.

Apart from collecting status information from different nodes, this agent is also used to maintain its node’s internal state. This state can then be accessed by adjacent nodes’ interoperability agents. This setup creates an environment where each node watches over the other for changes in behavior. Therefore, changes are capable of affecting a node’s own performance and it can take action to try minimise any negative impact that may occur on the smart grid network.

11.2.3.4 – Actuator Set Component

The IA allows the transmitting of messages from one agent to another. If this information has an outbound destination, it will then be in charge of pushing it directly to the agents of the destination node. As soon as a communication request is received, it establishes an exchange of information between a sender and recipient of the information.

Whenever communication requests need to be fulfilled, the IA’s actuator component identifies the sender and recipient(s) of messages in order to actively push messages through. Messages handled by the IA can either be one-way or two-way. One-way messages are simply captured by the IA and forwarded to the recipient. Two-way messages involve forwarding a message to a recipient and then listening for a response
message from the recipient agent. Therefore, if a response is requested, the IA’s actuator set listens for a response message that can be returned to the sender.

11.3 – Conclusion

The agents described in Chapter 11 are those that are directly part of the model’s attempt to help increase security and robustness in the smart grid network. The agents are all configured to work together at the node level, as well as at the network level. In order to evaluate their suitability to the task, an attack agent that puts the model to the test is included in this dissertation. The attack agent is elaborated on Chapter 15.

The aim of the chapter was to briefly discuss the agent composition of the MA-SGS model, giving the reader an overall understanding of the intents and purposes of each of the agents working in the model. Before the implementation of the model is discussed, the next set of chapters, in the current phase of the dissertation, describes each node agent type’s composition.
Chapter 12
MA-SGS: Process Monitoring Agent
12.1 – Introduction

Before the process monitoring agent is initialised, the simulation environment itself must be initialised in order to create all components that it will be working with. The current chapter is devoted to how the process monitoring agent is activated in the first phase of initialisation of the MA-SGS model.

Each component of the agent identified in the internal agent structure in Chapter 10 has to work with the other in order to aid the agent in meeting its intended purpose in the environment in which it is deployed. The current chapter will now explain how each component of the process monitoring agent is configured to help understand how each contributes to the purpose of the agent.

12.2 – Environment Simulation

The simulation begins by retrieving user set details of the components within the environment. These details in the configuration setup would contain information about the nodes required to be in the smart grid network, as well as the connections and message exchange information between the nodes. Figure 12.1 shows an overview of the first phase of the process in which the environment is initialised.

From the configuration set up, each of the specified nodes are created. For each of the created nodes, a multi-agent setup is created, containing all the necessary agents as specified by the MA-SGS model. At this point, each of the agents at the node is not in its active state as each one will be activated at a specific phase of the MA-SGS initialisation.

Within the group of agents working at a specific node, the process monitoring agent is the first to be initialised with its internal components enabled in order to get the agent to begin working. Figure 12.2 shows the components found within the process monitoring agent’s environment.
Initiate Simulation

Simulation Configuration Setup

Retrieve Smart Grid Nodes

Node 1

Node 2

Node 3

Node n

Initiate Node Agents

Process Monitoring Agent

Monitor Node Information

Simulation Environment – Phase I

Figure 12.1 – Phase I Environment Setup
12.3 – Process Monitoring Agent Internal Environment

As discussed in Chapter 10 when the MA-SGS model was introduced, each of the individual agents at each smart grid network node is made up of a set of standard components. Each of the components, though, will differ in functioning between each of the different agents in the MA-SGS model. Figure 12.2 illustrates the particular functioning for the process monitoring agent.

![Process Monitoring Agent Environment Diagram](image)

**Figure 12.2 – Process Monitoring Agent**

Each of the components is packaged together as a process monitoring agent. Figure 12.3 shows the structure of the PMA’s components using the unified modelling language (UML) to show the relationships between each of the components. Each of the PMA’s components is described in the subsections that follow.
12.3.1 – Sensor Component

As described in section 11.2.1, the process monitoring agent’s sensor component is responsible for analysing all internal and external commands that have to be processed by the node in which it is based. The external commands originate from other nodes within the network.

The following is a list of the sensor component’s units of processing, which together allow the agent to be able to get command information from its environment:

- **Sensor Configuration:**
  Used to keep track of what data the agent is supposed to watch for and retrieve from relevant data sources;

- **Query Component:**
  Used to query the set data sources for the information the agent needs to work on in its environment;

- **Information Reader:**
  Used to parse information retrieved by the agent’s query component;
- **Information Processor:**
  Applies any needed information processing methods to make the information usable to the agent.

### 12.3.2 – Information Processing Component

The information processing component in the process monitoring agent is responsible for profiling each of the commands that is executed by the agent. The processing of each command is done according to the rules the component has, and is then logged. The following is a brief description of each of the component’s units:

- **Rule Base:**
  Keeps track of the agent’s independent set of rules that need to be used when processing information;

- **MessageProfiler:**
  Classifies messages based on the agent’s rules set;

- **Message Logger:**
  Stores messages received by the agent on the agent’s analysis log, which is part of its internal state component.

### 12.3.3 – Internal State Component

The internal state component in the process monitoring agent keeps track of all the messages logged by the information processing component. The log can be queried by the other agents within the node. The following is a brief description of each of the component’s units:

- **State Log:**
  Records the agent’s current state during execution. The State Log of the PMA is used to track the operations that have been executed by the agent;
• **AnalysisLog:**
  Records the results of the analysis executed by the agent’s information processing component.

• **LogQuery:**
  Used to provide querying capability to the agent’s state and analysis logs.

### 12.3.4 – Actuator Component

The actuator component in the process monitoring agent constantly evaluates the results of the information processing component in order to determine which action to do based on the results obtained from the profiling.

It is made up of a single DataDecisionAnalyser which decides whether messages that have been classified by the MessageProfiler unit of the information processing component should be flagged for analysis or simply logged as a regular occurrence.

### 12.4 – Conclusion

In order to manage the operations carried out on the node accordingly, the MA-SGS model includes a process monitoring agent that is responsible for checking on all messages that pass or originate from the node. As these messages are analysed, they are labelled as either part of a regular set of messages or recorded as messages that represent some kind of threat to the node.

The current chapter focused on providing the internal structure of the monitoring agent and its various components. The creation and initialising of the monitoring agent form part of phase I in the initialising of the entire simulation of the smart grid. The following chapter proceeds to phase II during which the security response agent is initialised.
Chapter 13
MA-SGS: Security Response Agent Structure
13.1 – Introduction

The security response agent (SRA) is the agent responsible for performing security analysis on the flagged information detected by the process monitoring agent. The security response agent uses its rule set to identify the types of threats it discovers, evaluates the current state of the node on which the SRA is deployed and selects the most appropriate action to take in order to produce an acceptable node state.

The current chapter describes how the security response agent is activated in the second phase of initialisation of the MA-SGS model, as well as how it is structured in the model. As the SRA uses information produced by the PMA, it can only be initialised in the second phase. The chapter begins by describing how the security response agent is initialised in the simulation environment.

13.2 – Environment Simulation

Figure 13.1 shows an overview of phase II of the process in which the environment is initialised. As in phase I, the simulation begins by retrieving user set details of the components within the environment. These details in the configuration setup would contain information about the nodes required in the smart grid network, as well as the connections and message exchange information between the nodes.

Phase II entails the initialisation of the security response agent (SRA) within each of the existent nodes. Once the SRA is initialised within the node, the agent initialises each of its individual components that will allow it to work within the node.

The SRA begins by setting up its user defined rule set and initialising its user set knowledge base. From this point onwards the SRA’s analysis component helps it adapt the rule set and knowledge base according to the environment and the best possible conditions for the node at each point in time. The following section discusses each of the components of the security response agent.
Simulation Environment – Phase II

- Initiate Simulation
- Simulation Configuration Setup
- Create Smart Grid Nodes
- Node 1
- Node 2
- Node 3
- Node n
- Initiate Node Agents
- Process Monitoring Agent
- Monitor Node Information
- Security Response Agent
- 1 Initialise Rule Set
- 2 Initialise Knowledge Base
- 3 Analyse Flagged Messages
- 4 Initialise Security Analysis Component

Figure 13.1 – Phase II Environment Setup
13.3 – Security Response Agent Internal Environment

The security response agent works as the main actuator of response processes to restore the operational stability of a node in the simulated smart grid to its optimal status. The SRA works with the process monitoring agent which flags data records which could indicate the possibility of a disruptive event in the smart grid node being protected.

A disruptive event is one that threatens the operational stability of the smart grid by causing a node to either become an unavailable network, or by compromising the operation of the node so it does not meet its specific functions in the network.

Figure 13.2 shows the components found within the security response agent’s environment. The agent’s components are configured to analyse possible threats identified by the process monitoring agent, determine their possible effects on the smart grid and execute response strategies against data records the SRA confirms to be possibly threatening to the smart grid simulation.
Flagged records that the SRA confirms to indeed be compromising to the smart grid simulation are acted on by the agent in order to restore the desirable state in the node. If the operation of the smart grid node is already compromised, the SRA attempts to decrease the restoration time of the node’s operations in order to prevent the occurrence of cascading failures in the grid. The following subsections are devoted to describing each of the components found in the security response agent. Figure 13.3 shows the UML specification of the Security Response Agent.

Figure 13.3 – Security Response Agent High Level Static Class Specification (UML Design)

13.3.1 – Sensor Component

Although possessing the same sensory components as the process monitoring agent, the sensory components of the SRA are set up differently to fit the purpose of working with security specific information that the agent will be retrieving. The following is a list of the units found in the sensor component of the SRA:

- **SensorConfiguration:**
  Listens for events on the smart grid node that indicate the existence of data records flagged by the process monitoring agent;
• **QueryComponent:**  
  Used to query the set data sources for the information the agent needs to work on its environment;

• **InformationReader:**  
  Used to parse information retrieved by the agent’s QueryComponent;

• **InformationProcessor:**  
  Works with the SensorConfiguration, QueryComponent and InformationReader units in the sensor component to retrieve flagged data records and process the records for use by the agent’s information processing component described in the following section.

### 13.3.2 – Information Processing Component

The Security Response Agent’s information processing component analyses the flagged data records retrieved by the sensor component. The information processing component's units are set to analyse flagged information to help the agent decide on how to best handle any records it detects would threaten the operations of the node. The following list is a description of each of the units found in the SRA’s information processing component:

• **The Dynamic Rule Set:**  
  The dynamic rule set keeps track of the conditions which are used to check the validity of flagged data records. The rule set is dynamic as attacks can occur in different manners and new attacks can materialise, making it necessary for the rule set to be adaptable.

• **Security Analysis:**  
  Makes use of the set algorithms to evaluate the components and content of flagged messages in order to make a final deliberation on the safety of making use of the data record. The security analysis component also updates the agent’s knowledge base given the information that it discovers through the analysis of messages.
13.3.3 – Internal State Component

The internal state component of the SRA is made up of a single unit. The KBAccessLayer manages the agent’s knowledge base where all data collected during the information processing component’s analysis process is kept. The agent’s knowledge base is kept as part of the node’s data store described in section 10.4.4.

The knowledge base contains a description for each of its entries on whether the state of the analysis is desirable or not. Such data in the knowledge base can then be used to speed up decisions on certain situations that may have occurred before in highly similar conditions. The KBAccessLayer enables the component to both request and write data to the knowledge base.

Data stored in an SRA’s knowledge base is made available to other SRA agents securing nodes of the same type across the simulated smart grid environment. This knowledge is shared to prevent the occurrence of repeat attacks on different nodes in the network.

The internal state component of the SRA also keeps a log of the node’s current security status. The current security status is determined by an analysis done by the actuator component of the agent. The analysis entails checking on the current operational status of the agent and checking against the optimal operational requirements. The following section discusses the SRA’s actuator component.

13.3.4 – Actuator Component

The actuator component of the SRA uses its DataDecisionAnalyser to evaluate any situation where it is determined that a malicious command has been detected. The DataDecisionAnalyser then matches the situation with the most appropriate security measure to take.
The security measures it can take are adaptable, meaning they are prone to change depending on changes that occur to the model. The most basic of measures is to cancel the execution of a command. A more drastic measure would be to disconnect the current node from whichever node was the source of a malicious command.

13.4 – Conclusion

To enhance the MA-SGS model’s ability to address security concerns more precisely, the security response agent is included at each node in the simulated smart grid environment. The agent has the capability to make the final analysis and deliberation on whether any flagged message is indeed a threat before it takes counteractive actions to protect the node.

The current chapter gave a more detailed explanation on how the security response agent is constructed. The following chapter discusses phase III of the initialisation process of the MA-SGS model, where the interoperability agent is activated to liaise all interactions between all agents at both the node level, as well as the surrounding nodes.
Chapter 14
MA-SGS: Interoperability Agent Structure
14.1 – Introduction

In order to standardise and better control how agents within a node communicate, the interoperability agent (IA) was added to the MA-SGS model. The IA enables the process monitoring and security response agents to work together, and also helps the agents to coordinate their actions.

Furthermore, the IA allows agents within a node to communicate with those from the surrounding nodes. The IA also keeps the node’s state logs which are made available to surrounding nodes. The state information it keeps gives surrounding nodes an indicator of whether the node in which the agent is based is available or not. The IA also monitors the state information on the nodes adjacent to the node in which it is situated, constantly checking on the state of the other nodes in order to keep track of the changes they go through.

The current chapter looks at how the IA is initialised in phase III of the MA-SGS initialisation process, and goes on to describe each of the components of the agent. Each of the agent’s aspects is briefly discussed. The following section looks at how the IA is initialised in the simulation environment.

14.2 – Environment Simulation

Figure 14.1 shows phase III of the MA-SGS model’s initialisation process. On each of the nodes on the smart grid network, each interoperability agent is initiated to survey its node’s current status and also initiate the communication module in order to start processing internal and external messages.

The IA constantly requests the state information for each of the nodes adjacent to it and monitors the changes of state of these nodes. The agent then builds a state profile for each of the surrounding nodes, attempting to identify major changes on these nodes. Information on the profile of these surrounding nodes is then made available to the
other agents within the node. This information is used as part of the exploratory process of determining a course of action by the MA-SGS agents in the IA’s node.

**Figure 14.1 – Phase III Environment Setup**
The following section describes how each of the components of the interoperability agent work together to help it meet its purpose in the MA-SGS model.

14.3 – Interoperability Agents’ Internal Environment

Figure 14.2 illustrates the components found in the interoperability agent’s environment. The IA’s components are configured to aid the agent in combining the interactions between the agents around it. The IA again is structured in the same manner as the process monitoring and security response agents, but its components are geared to enable internal and external agent interactions. Figure 14.3 shows the UML specification of the interoperability agent.

Agent interactions occur when the need to exchange information occurs. Internal agent interaction refers to when the process monitoring agent and the security response agent in a smart grid node need to exchange information on records being analysed. External interactions occur when the interoperability agent either sends or requests information from the interoperability agent in a surrounding node.
The IA essentially works as a service provider agent in the MA-SGS model. Its services help keep track of the operations of each node in the simulated smart grid network. The following sections discuss each of the components of the interoperability agent.

14.3.1 – Sensor Component

The interoperability agent’s sensor component is equipped with processing units configured to wait for information exchange requests as well as information retrieval commands.

The following is a list of the units found in the agent’s sensor component:

- **SensorConfiguration:**
  Upon initialisation, the sensor configuration for each interoperability agent is populated with the categories of information the agent should be able to work with. As an example, the configuration would help the agent determine what information it should ask for from the surrounding nodes.
• **QueryComponent:**
The QueryComponent uses the information stored by the SensorConfiguration component to determine the data sources that it has to query for the data the agent can work with.

• **InformationReader:**
Used to parse information retrieved by the agent’s QueryComponent.

• **SensorEndpoint:**
The SensorEndpoint works as a gateway for information that is sent through to the agent. The gateway can be used for receiving and sending information from the agent.

14.3.2 – Information Processing Component

The interoperability agent’s information processing component is built to keep track of all the information passing through the agent’s sensor component. It logs all the information passing through the agent. The following is a list of the units found in the component:

• **MessageLogger:**
Records all messages sent from the agent and those received by the agent. The messages are stored for analysis as part of the record data processed by the process monitoring agent.

• **MessageProcessor:**
Provides the mechanism for sending and receiving messages. The MessageProcessor also uses the MessageLogger unit to record the messages processed by the interoperability agent.

14.3.3 – Internal State Component:

The interoperability agent’s internal state component provides the agent with the ability to keep track of the functioning of the node in which it is based. The agent also makes data on the operational status of the node available to surrounding nodes.
The following is a list of the units found in the component:

- **Node State Log:**
  Maintains the history of the node’s status which is made available to surrounding nodes which may require status information from the current node.

- **Notification Log:**
  Records the different notifications that may have been the trigger of specific node statuses. These are saved for further processing.

- **LogQuery:**
  This is the query component used to retrieve log information (either node state or notifications) from the node’s internal state component.

**14.3.4 – Actuator Component**

Like the process monitoring and security response agents, the interoperability agent’s actuator component is just composed of a single DataDecisionAnalyser unit. The DataDecisionAnalyser retrieves information produced by the information processing and internal state components to help the agent decide on which state the agent is in so it can be set, and published to external nodes. The DataDecisionAnalyser also uses the agent’s components to process the message requests during internal or external communication in the MA-SGS model.

**14.4 – Conclusion**

The MA-SGS model includes the interoperability agent to manage the inter-agent communications carried out in the node. The IA is also responsible for monitoring and keeping track of the node’s state, the information of which is essentially produced by the interaction between the agents that the IA monitors. State information can be used by any surrounding node querying the node’s state. It also provides a medium for internal and external communications of the current node.
Chapter 14 concludes the series of chapters on the agents situated in each node of the smart grid. The process monitoring, security response, and interoperability agents collaborate to secure the operations of each node of the network. The agents also help to secure the manner in which different nodes work together to maintain the network’s stability and resilience to attacks. The ability of the model to resist attacks, and improve the robustness to the smart grid is put to the test by introducing the attack agent. The following chapter is devoted to discussing the attack agent.
Chapter 15
MA-SGS: Attack Agent Structure
15.1 – Introduction

The goal of the MA-SGS model is to maintain a state of equilibrium on the smart grid even if under attack from external components. These attacks attempt to disrupt the services provided by the grid. The efficacy of the model is tested on its ability to keep the grid functioning. The attack agent is not part of the main group of MA-SGS agents that are found at each node of the network as it is treated as an external agent with the task of straining the MA-SGS agents working within a node in the smart grid.

The current section is devoted to discussing the attack agent included in the dissertation as a testing tool used to check whether the MA-SGS model is functioning as intended to protect the smart grid network. The chapter begins by describing the purpose of the agent and the different modes it will use to test the MA-SGS model. The chapter follows on to briefly discuss how the attack agent is activated during the MA-SGS initialisation process.

15.2 – MA-SGS: Attack Agent – The Proof of Concept Agent

According to Maata and Raty (2012), models are used as an appropriate method of abstractly defining and specifying different events that occur in a given environment. Applying such an analysis to the MA-SGS model creates the notion that the model's purpose is to define the different security driven events that occur in the smart grid to better analyse methods in which security can be upheld in the Critical Infrastructure.

Taking into account that the model uses an agent-based approach, the behaviour of the agents in their environment is an aspect that has to be closely monitored and evaluated to determine whether the agents are meeting their original purpose. The interactions between the agents in multi-agent systems give rise to complex behaviour that both affects and is affected by their complex environment (Parks, Jung & Ramotowski, 2004). Such complex behaviour could result in events that either harm or benefit the environment, therefore making it even more important to monitor such behaviour.
The aim of the MA-SGS model is to bring benefits to the system in terms of improving the resilience and robustness of the smart grid. According to Kundur, Feng, Liu, Zourntos & Butler-Pury (2010), a system’s security is ‘only as strong as its weakest link’. Therefore if one is to evaluate the security efforts of the MA-SGS model, there needs to be a proof of concept tool that will put the functioning of the model to the test to help identify its weaknesses.

The attack agent is introduced into the dissertation as an entity that is set to create disruptions in the smart grid. Disruptions which, if unattended, can cause a collapse in the smart grid Critical Infrastructure. The agents used in the MA-SGS model have to be able to detect and attempt to protect the smart grid from the disruptions created by the attack agent.

Agent-based systems, just like other kinds of systems, are subject to attacks, especially if connected to a network such as the Internet. Attacks on agent-based systems can be categorised as either conventional or infrastructure attacks (Parks et al., 2004). Conventional attacks are those which would work against any other kind of system (e.g. privilege removals, SQL injection etc.), and infrastructure attacks, otherwise called ‘system-of-systems attacks’, are those that affect the environment (e.g. a network, an operating system etc.) on which the agent-based systems depend.

Attacks on the smart grid protected by the MA-SGS model will attempt to either destabilise a single node on the network, or create a disruption that changes the topology of the network to replicate a cascading failure that has to be countered. The topology of the network refers to the manner in which nodes in the smart grid network are organised and interconnected. Cascading failures (described in section 2.3) refer to failures that begin at a node in the network and propagate through each of the interconnections possessed by the node.
In order to test the model, the attack agent can, at random, select at least one node in the smart grid network from which it will initiate a disruption. Figure 15.1 illustrates a smart grid network where a node has been taken over by the attack agent. In order to test the model, the selected node may have its MA-SGS model agents disabled in order to determine whether the connected surrounding nodes are able to detect a threat.

Figure 15.1 – Example Simulated Network with an Attack Agent Node
As introduced in section 11.3, the attack agent should be able to conduct test disruptions that include: de-activating a random node on the network, de-activating a node of high importance in the smart grid network, and sending erroneous information from a random node. The following section looks at how the attack agent is activated in the simulation of the MA-SGS model.

15.3 – Agent Environment

The model begins with an initialisation of the simulation environment and the component nodes of the system. After initialisation is complete, each node works towards analysing the existing demand-supply ratio of power within and outside the node, commands to be executed on the node, as well as node states in order to keep track of any trends.

These trends are analysed by the agents within the node in order to determine the best course of action to keep the agents’ statuses functional. Any changes within the environment detected by the agent are then stored in the knowledge base in the event
of the same kind of recurring disruptions. Figure 15.2 shows phase IV of the initialisation process of the attack agent.
Initialisation only occurs in the last phase of the simulation environment setup. This is because the attack agent is meant to work on a known environment in which it has information on the topology of the network in order to determine strategies for how to disrupt the MA-SGS model.

Disruptions in the smart grid network can be caused by changes in the form of: erroneous information being inserted into the system, bad commands being executed by a node in the smart grid, or by a node being taken down on the network. The severity of disruptions would depend on the criticality of nodes affected by an attack. The attack agent may create such situations by: carrying out deleterious data injection attacks, executing 'denial-of-service' attacks, as well as replaying attacks which may distort the functioning of each node.

In a bad data injection attack, the attack agent may intercept communication between different nodes and alter the information being sent in messages with erroneous data. A denial-of-service attack would involve the attack agent working actively to disable a node in the grid. The disabled node remains in such a state until the MA-SGS model agents are able to return it to normal functioning. A replay attack involves the attack agent recording a series of messages sent to a selected node and resending the same messages in the same order at a time in which the messages are not valid.

Since the attack agent requires prior knowledge of the environment in order to work, it first has to retrieve information about the smart grid network before it can begin running tests on the MA-SGS model. Such information would include: the list of nodes available, each of their types, as well as all the interconnections between them. In order to carry out an attack, the agent may have the ability to select a node that it can use as the source of its disruptions.

The attack agent may collect information for a period of time in order to best look for a method to cause an undesirable state in the smart grid. After each disruption, the attack agent may collect data on changes in the smart grid to evaluate how the MA-SGS
model responds to the anomalies caused. Chapter 16 adds further detail on how the
attack agent introduces disruptions into the simulated smart grid environment where the
MA-SGS model is deployed.

15.4 – Conclusion

The introduction of the attack agent plays an essential role in the dissertation as it
replicates test events necessary for evaluating the MA-SGS model’s ability to withstand
real-world attacks. A secondary benefit of the attack agent is that it can serve as a
training tool that allows the various agents of the MA-SGS model to learn and adapt to
evolving scenarios. Therefore attack agents’ inclusion in the dissertation allows for both
testing the model, as well as getting the agents to learn. The attack agent creates forms of attacks that test the MA-SGS model’s ability to work
against information security concerns in the smart grid network. Such concerns would
include confidentiality, integrity and availability. Each one may, in its own right, create
undesirable states in the smart grid network. The following section of the dissertation is
devoted to discussing the prototype implementation of the model as well as the results
obtained from the simulation of the smart grid environment.
Chapter 16
MA-SGS: Smart Grid Simulation & Model Implementation

Introduction

Chapter 2: Critical Infrastructure
Chapter 7: Intelligence Enabling Machine Learning Models

Chapter 3: Critical Information Infrastructure Protection
Chapter 8: Intelligent Agents and Complex Adaptive Systems

Chapter 4: The Smart Grid
Chapter 9: Agent Technology and Critical Information Infrastructure Protection

Chapter 5: The Smart Grid as a Critical Infrastructure

Chapter 6: Software Agents

Chapter 10: Multi-Agent Model for Smart Grid Security (MA-SGS)
Chapter 11: MA-SGS: Node Agents

Chapter 12: MA-SGS: Process Monitoring Agent
Chapter 13: MA-SGS: Security Response Agent Structure

Chapter 14: MA-SGS: Interoperability Agent Structure
Chapter 15: MA-SGS: Attack Agent Structure

Chapter 16: MA-SGS: Smart Grid Simulation & Model Implementation
Chapter 17: MA-SGS: Model Results

Chapter 18: Conclusion
16.1 – Introduction

After the discussion of topics involved in the dissertation’s research objectives, and the introduction of the Multi-Agent Model for Smart Grid Security (MA-SGS) in the previous sections, a discussion of the implementation of the simulation environment and the MA-SGS model is necessary. Chapter 16 introduces and discusses the proof of concept prototype implementation of the model to serve as a test bed for evaluating the effectiveness of the model in achieving smart grid security through multi-agency.

The chapter begins by discussing the smart grid simulation environment named SmartGridSim, constructed to test the multi-agent model. The discussion of the environment introduces the concept of an energy agent used within the simulation. The chapter then follows on to describe the implementation and the functioning of the MA-SGS model’s agents within the environment. In order to report on the results of the implementation, the chapter describes simulation scenarios to generate statistics about the model.

16.2 – Prototype Implementation Layers and Tools

The Multi-Agent Smart Grid Security model as well as its simulation environment, was developed in C#, using the .NET 4.5 framework in the Microsoft Visual Studio 2012 Integrated Development environment. The prototype made use of a Microsoft SQL Server Express database with LINQ to SQL as the method of interacting with the system’s database.

In order to add flexibility to the system and simulate the message exchange services used in the smart grid network, the prototype makes use of the Windows Communication Foundation (WCF). WCF is a unified model containing a set of Application Programming Interfaces (APIs) used to build service-oriented applications. Figure 16.1 illustrates the main components of the prototype (Microsoft MSDN, n.d.).
Figure 16.1 – Prototype Implementation Layers

For the prototype to be able to perform its functions, and visualise the simulation-generated data the following external components were used:

- **Extreme Optimisation Library**: Used to process time series data for forecasting and trend analysis. This library is packed with a wide range of mathematical models used for numeric data analysis and forecasting (ExtremeOptimization.com, n.d.). Available at [http://goo.gl/lPIrv1](http://goo.gl/lPIrv1).

- **AForge.NET and Accord.NET**: AForge.NET and Accord.NET are class libraries containing a wide variety of ready-made and very adaptable algorithms used in computer vision and artificial intelligence (AForgeNet.com, n.d.). The libraries’ learning algorithms are used by the MA-SGS model to learn and classify data patterns. The library is available at [http://goo.gl/oav6bK](http://goo.gl/oav6bK).
• **GraphSharp Network Visualisation Library**: Used to display the smart grid network on the visualisation layer of the prototype. The GraphSharp class library contains a generic user control for Windows Presentation Foundation that can render different forms of graphs (Graph#, n.d.). The class library also comes with a series of algorithms that may be used to organise each node in the visualised graph. The modified version of the GraphSharp library used can be found at [http://goo.gl/xW1a7f](http://goo.gl/xW1a7f).

• **Visifire Charts**: Used to render the results generated by the prototype in real-time on the visualisation layer of the prototype. The class library contains a wide range of charts which can be used to display data (Visifire.com, n.d.). The tool also allowed the extraction of the graphs to be used within the dissertation.

• **ConsoleWidget**: Used to display all events occurring at each agent in the entire smart grid simulation as well as the MA-SGS model’s agents. The ConsoleWidget tool enabled the display of all simulation events in the visualisation layer of the prototype. The ConsoleWidget tool can be found at [http://goo.gl/3rQGvT](http://goo.gl/3rQGvT).

The following sections will describe each of the layers in the prototype implementation of the MA-SGS model and its supporting components. The sections begin by describing the underlying SmartGridSim environment on which the implementation is based, before describing the MA-SGS agents’ layer which works hand-in-hand with the communication layer. The prototype includes a visualisation layer used to monitor all operations and events that occur in the smart grid’s simulation in real-time.

### 16.3 – Smart Grid Simulation

According to Othman and Mustafa (2012), a simulation can be described as one of many methods used to create abstract environments that aid designers building real systems in making decisions that may affect their final product. Simulations may be used across fields such as engineering, manufacturing, science etc.

Simulation techniques are used at all stages of planning, design, development and operations of power systems (Ling, Nai-qiu, Yun-ping, Chun-ming & Min, 2006). The
use of multiple components and different technologies that need to work together make it vital that they are theoretically capable of working together before resources are invested to implement the physical systems. Building a proof of concept simulation may help designers approximate their decisions to produce their intended results in a real environment.

Taking all the different components into account, simulating of power systems is essentially a two-fold task due to, firstly, their electrical infrastructure, with physical devices; and, secondly, their information technology infrastructure, which runs complex information systems (Chiaradonna, Giandomenico & Lollini, 2009). For this reason, the implemented SmartGridSim environment is built to represent the physical components of the smart grid, as well as the information systems that make the energy consumption and/or generation decisions at each node of the smart grid. Figure 16.2 illustrates the types of nodes found in the smart grid simulation layer of the prototype.

![Figure 16.2 – Smart Grid Simulation Area Node Types](image)
Given that the simulation layer creates the base environment that the MA-SGS model works on to maintain its security, a set of states needs to be identified in order to guide the actions of the MA-SGS agents to always move the simulated SmartGridSim environment, as a whole, to an acceptable state. Such states take into consideration the confidentiality, integrity and availability requirements of smart grid security. The simulation environment uses a slightly revised classification scheme defined by Gustavsson & Stahl (2009) shown in Table 16.1.

Table 16.1 – Classification Scheme of Operational States of a Power System (Gustavsson & Stahl, 2009)

<table>
<thead>
<tr>
<th></th>
<th>ADEQUATE</th>
<th>INADEQUATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>STABLE</td>
<td>Normal</td>
<td>Temporarily inadequate</td>
</tr>
<tr>
<td></td>
<td>Potentially unstable</td>
<td>Temporary emergency</td>
</tr>
<tr>
<td></td>
<td>Potentially inadequate and unstable</td>
<td>Potentially unstable</td>
</tr>
<tr>
<td>UNSTABLE</td>
<td>Cascading failure possible; power system collapse also possible</td>
<td></td>
</tr>
</tbody>
</table>

The situations indicated in Table 16.1 take into account the ability of the power grid to generate enough power to satisfy the amount required by the demand centres that the grid services. The states also take into account the consistency, which the power demand exhibits when met by the power supply, as an indication of whether power use is adequate or inadequate for the power grid to continue working appropriately.

A power grid is, in essence, adequately stable if all of its nodes are fully functioning and the power demand-supply is stable. A power grid may also be seemingly stable if all of its nodes are functioning, yet they may actually be working in an inadequate manner if the power demand is not appropriately matched by the power supply. Such instability on the power grid may push it to an unstable state which may cause a collapse in the power grid as a whole. Table 16.2 reflects the meaning of the different states in the simulation layer.
An ‘acceptable’ state is one that is most desirable in the simulation layer. It essentially indicates that the majority of the nodes in the power grid are currently active and working in a stable manner, and the power generated in the simulated smart grid is sufficient to meet the demand of the demand centres in the simulation.

A ‘cautionary’ state would indicate: a small decline in either the efficient working of the simulated smart grid nodes; a slight imbalance in the power demand and supply; or a combination of both. In a cautionary state, the simulated smart grid may still function, but at a gradually declining state that requires action to restore the grid to the ‘acceptable’ state.

An “emergency’ state indicates a considerable decline in the number of functioning nodes on the simulated smart grid, accompanied by a considerable imbalance between power demand and supply, which can then cause cascading failure between the different nodes in the SmartGridSim, ultimately causing the grid to collapse. Table 16.3 indicates the margins used to determine the different states of the simulated smart grid.

<table>
<thead>
<tr>
<th>State</th>
<th>Active Node Percentage</th>
<th>Power-Demand Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable</td>
<td>97% (\leftarrow) \rightarrow 99.9%</td>
<td>95% (\leftarrow) \rightarrow 99.9%</td>
</tr>
<tr>
<td>Cautionary</td>
<td>71% (\leftarrow) \rightarrow 96.9%</td>
<td>71% (\leftarrow) \rightarrow 94.9%</td>
</tr>
<tr>
<td>Emergency</td>
<td>&lt; 70.9%</td>
<td>&lt; 70.9%</td>
</tr>
</tbody>
</table>
The overall state of the simulated smart grid is determined by evaluating the functioning of all of the grid’s nodes. The functioning of each node in the simulated smart grid is determined by the energy agent working within it. Section 16.3.1 is devoted to describing the role of the energy agent working in the different nodes of the simulated smart grid.

16.3.1 – Energy Agent

In order to simulate the smart grid’s information systems used to enable two-way energy flow, power generation and power consumption on each node, the energy agent was introduced. The energy agent simulates the software in control of the information used at the smart grid node, and the hardware used in the different nodes.

Taking into account that the smart grid is composed of multiple types of nodes, each with its own functionality when participating in the power supply and demand dynamics, the energy agent may be any one of several types to serve the purpose of the node in which it resides. The different forms in which an energy agent may be found on the SmartGridSim’s nodes are listed in the following subsections.

16.3.1.1 – Power Station Energy Agent

The power station energy agent essentially simulates the functioning of the SCADA control system running at power stations, which is used to gather data from the entire network. Such data is then used in the generation and transfer of electric power to the transformers connected to the power station so electric power can then flow to the different demand centres that the station serves.

The power station energy agent requires real time, and up-to-date data on all events occurring on the grid in order to properly manage the supply of electric power. Its consistent supply of electric power keeps the simulated smart grid stable.
Corrupting the functions of the power station energy agent may bring the entire simulated smart grid to a system collapse. Corruption of the agent may stop the flow of electric power to the different demand centres. Corruptions could also cause an imbalance between the volume of generated electric power and the load of electric power needed by the demand centre.

16.3.1.2 – Transformer Energy Agent

The transformer energy agent simulates the working of a distribution management system working on a power grid. Such a system is responsible for monitoring the information on the load of electric power demand required by the different demand centres.

Information is then passed along to the systems running on the different power stations that are connected to the transformer station. The simulated smart grid is set up so that a request for electric power is sent to the different power stations connected to the transformer station.

After electric power is transferred to the transformer station, the transformer energy agent then follows up to distribute the power to the different microgrid substations. Such microgrid substations represent the last level before electric power reaches the end consumers of a demand centre.

Before electric power is distributed to the different demand centres, the transformer energy agent is also responsible for calculating and converting the power received from the generation station into power that may be readily used by the microgrid station to distribute to consumers.

Disruptions to the transformer energy agent could distort the balance in the supply and demand of electric power between the demand centres and the transformer stations necessary to request the power from the power stations.
Disabling a transformer energy agent can disable the entire transformer substation node, thereby causing the demand centres that use the station to lose a source of usable power. If a demand centre is connected to a single transformer station that is found in its disabled state, it may cause a collapse in the use of power in the demand centre.

16.3.1.3 – Microgrid Energy Agent

The microgrid energy agent works as a demand-side agent which directly monitors the consumer nodes in the simulated smart grid. Demand of power from the different consumer nodes is gathered up by the microgrid energy agent and a request is sent up to the transformer substations to which the microgrid is connected.

In times of temporary power supply disruption, the microgrid energy agent is responsible for administrating how electric power is distributed to more critical consumer nodes in the simulated smart grid. In the simulated smart grid, the microgrid energy agent essentially acts as a load control and distribution management system which provides up-to-date and real time data on power consumption by the different consumer nodes, and how the electric power should be used.

Disruptions to the microgrid energy agent can cause the availability of real time data on electric power consumption to diminish, thus causing an insufficient supply of electric power, given that demand information is not immediately available. During a disruption, or a temporary loss of electric power, the unavailability of the microgrid energy agent may cause critical nodes not to be considered during the distribution of any available electric power.
16.3.1.4 – Consumer Energy Agent

In the simulated smart grid, the consumer energy agent works as the control system used directly at the consumer node. The agent controls the different devices that are used at the consumer node and simulates this usage to generate the amount of electrical power needed at the node.

The consumer energy agent also works as a simulation of the smart meters used in the smart grid, as part of its advanced metering infrastructure. The agent monitors energy usage and sends requests for power to the control systems running in the microgrid substation to which the node is connected.

16.3.1.5 – Power Generation Consumer Energy Agent

The power generation consumer energy agent is essentially the same as the consumer energy agent, but it extends its functionality to simulate the smart homes in the simulated smart grid. Such smart homes are capable of using alternative power generation methods.

Electrical power from renewable energy sources may be fed back into the node in which the power generation consumer energy agent is based, or fed back to the microgrid substation in the case of emergencies that require critical nodes to receive priority.

When deployed and initiated during the simulation of the smart grid, every energy agent assumes its respective type based on the type of node in which it is deployed. Each energy agent retains information about the current node in which it is deployed, keeps track of the status of the node (which indicates the activity status of the node), and also takes charge of the procedures available to the node. Figure 16.3 depicts the basic structural components of each energy agent.
16.3.2 – Energy Agent and the MA-SGS Model

The energy agent essentially simulates the systems used to operate the consumption and generation of power. Such systems are those discussed in the dissertation, classified as Critical Information Infrastructure, or otherwise known as Critical Infrastructure Information Systems.

In the simulation layer, each node in the simulated smart grid is embedded with the energy agent type which suits the needs and the functionality of the node. Therefore, for example, a power generation station node would be simulated by the power generation energy agent that is responsible for using the resources available to it to simulate the generation of electric power used to feed the demand centres that receive power from the generation station.
The aim of the MA-SGS model is to enhance smart grid protection by monitoring the functioning of the Critical Infrastructure Information Systems running on the grid. On the simulated environment, the energy agent fulfils the system requirement on each node. The energy agent takes the role of controlling the electric power usage at each of the simulated smart grid’s nodes.

Therefore the node agents of the MA-SGS model come into effect in order to monitor the energy agent and ensure the resilience and robustness of the energy agent in order to maintain the simulated smart grid node to work in a stable manner. Figure 16.4 illustrates the generic MA-SGS agent organisation along with the energy agents in the smart grid.

![Figure 16.4 – MA-SGS Agent Setup with the Energy Agent](image)

Upon the generation of the smart grid simulation environment, each energy agent is created for the purpose of its node in the environment. After the energy agent is created and initialised, the agent then waits for a start-up signal sent by each of the MA-SGS agents that are also initialised to work on the same node.
Each MA-SGS agent examines the smart grid node to determine which kind of energy agent it will be working with in order to tune its analysis and actions to work appropriately on the node. Such action occurs due to the differences in operation between power station nodes and electricity consumer nodes in the simulated environment.

Figure 16.4 only demonstrates the types of connections that exist between the different types of nodes in the simulated smart grid environment. Such connections are only of use if the agents working on each node are able to communicate and share information that can be used to better secure the smart grid. The following subsections discuss how communication occurs between each of the agents working in the simulation environment.

16.3.3 – Agent Communication

Communication in the simulated environment occurs on two levels, either internal or external. Internal communication refers to that which happens between the different MA-SGS agents working within a single node. Since such agents share the same environment, exchange of information is done in a more direct medium.

The security response agent (SRA) and the process monitoring agent (PMA) directly communicate through the interoperability agent (IA). The IA essentially works as a liaison agent that allows the two to work together and to co-ordinate their actions to help secure the node. Figure 16.5 illustrates the exchange of information between the internal agents of the MA-SGS model.

![Figure 16.5 – Internal Agent Communication](image)
External communication occurs when one node in the simulated smart grid requests information from another node in the same grid. This may occur when a node requests status information from the nodes surrounding it or when there is an exchange of power or other information necessary to run the simulation of the smart grid.

In order to run such communication between different smart grid nodes, the interoperability agent is packed with the ability to access the node’s communication module. A communication module is used to both send messages to external agents as well as receive and respond to these. Figure 16.6 shows the exchange of information between different nodes in the simulated smart grid.

![Figure 16.6 – External Communication in the Simulated Smart Grid Environment](image)

The external communication medium in the simulated environment is implemented by means of a web service made available only to the interoperability agents in the simulated smart grid. The communication medium is only put to use when external communication is required. The medium is implemented as a Windows Communication Foundation (WCF) web service. Figure 16.7 shows a screenshot of the operating services that wait for requests sent from the interoperability agents.

The use of web services in the simulated smart grid environment essentially reflect the use of communication networks and technologies to integrate the different information systems and devices on the network. The following subsection discusses the attack agent used as a proof of concept tool of the MA-SGS model as well as the controller agent used to manage the smart grid.
Apart from the use of multiple information systems that can be used to monitor and operate the functioning of all components in the power grid, a certain degree of human interaction is still necessary. Such human interaction is provided through the use of human control operators.

Such control operators are often required to intervene in the functioning of the power grid to change operational parameters that need to be modified for the grid to remain operational. In order to recognise such a requirement, the simulated smart grid introduces the use of a simulation controller agent (SCA) that oversees the smart grid and has the ability to change operational parameters such as the following:

- Resource availability for the generation of power at power plants;
- Resource costs in the generation of power at power plants;
- Minimum and maximum loads supported by power plants, transformers and microgrids;
• Power request capacity of different consumer nodes in the demand centre, and;
• Availability of nodes in the simulated smart grid environment.

![Simulation Controller Agent Operating Environment](image)

**Figure 16.8 – Simulation Controller Agent Operating Environment**

Such operations can be done by the simulation controller agent (SCA), but their lasting effects are monitored by the MA-SGS agents in order to prevent actions that may destabilise the simulated smart grid environment. The simulation controller agent is built to only select actions that are more likely not to destabilise the simulated environment. It is included in the simulation as a control component that aids in the optimal operation of the simulated smart grid environment.

In order to test the MA-SGS model’s ability to monitor actions on the simulated environment and secure the environment, the simulation controller agent can be disabled in order to allow the attack agent to attempt to adjust the smart grid with operational parameters which cause instability. Therefore, the attack agent can test the ability of the MA-SGS model since its actions cannot be overridden by the controller agent’s ability to adjust operational parameters in a way that a human controller would. The following section discusses the functioning of the attack agent.
16.3.5 – Attack Agent on the Simulated Smart Grid

As introduced in Chapter 15, the attack agent serves as a proof of concept agent built into the Smart Grid simulation to help test the effectiveness of the MA-SGS model. Its sole purpose is to introduce instability in the simulated environment to monitor how the MA-SGS model is able to respond to its actions.

Figure 15.1 (page 174) illustrated the topology of a sample smart grid network where one node has been taken over by an attack agent. Under the simulation environment, the attack agent can create disruptions in two different ways. The agent can either disrupt the functioning of the node which it is controlled by or disrupt the nodes surrounding the network node which it controls.

The following two subsections briefly describe the two scenarios that the attack agent may use to test the MA-SGS model. Selection of either disruption scenario to test the model is randomly selected in the implementation, although the prototype’s user interface will enable one to initiate a disruption at will.

16.3.5.1 – Scenario 1 Attack Agent Disruption: Single Node Disruption

When using scenario 1, the attack agent essentially works as though it were the simulation control agent. The attack agent works externally from the simulated smart grid environment and selects a node which the agent can attempt to disrupt. The disruption approach the attack agent may take will depend on the type of node it will select from the simulated smart grid. Figure 16.9 illustrates the process followed in a scenario 1 attack agent disruption. Table 16.4 briefly describes each step.

A scenario 1 disruption strategy has the ability to test the resistance of the MA-SGS model against the possibility of single node failure. Resisting a single node failure may help in the prevention of a more serious cascading failure that could put the entire smart grid at risk of corruption.
Figure 16.9 – Attack Agent Scenario 1 Strategy Selection
Cascading failures were discussed in Chapters 2 and 15 of the dissertation. The following subsection describes the second disruption form the attack agent uses to stress the functioning of the MA-SGS model.
16.3.5.2 – Scenario 2 Attack Agent Disruption: Multiple Node Disruption

Under a scenario 2 disruption method, the attack agent works as though a node within the smart grid is already compromised. The attack agent selects a node from the simulated smart grid to use essentially as a host whose systems it has been able to take over. The MA-SGS model is then evaluated on its ability to determine when a node in the simulated environment is compromised.

The simulated smart grid takes on the interconnectivity concepts seen in the real-life smart grid. As discussed in Chapters 4 and 5, the smart grid makes use of two-directional flows not only of power but also information in order for the grid to maintain its stable generation and delivery of power. Such two-directional information is also necessary to maintain stability in the electricity markets operated by Smart Grid Critical Information Infrastructure.

The simulated smart grid environment developed and used in the evaluation of the MA-SGS model mimics such two-directional flows of information by allowing each node in the grid to communicate with its surrounding nodes. This communication is enabled so each node in the simulated smart grid can keep track of any change in the operational status of its surrounding environment that may warrant it to affect any changes to its own operations.

During communication, the intercommunicating node types determine the nature of communication that can occur between nodes in the smart grid. Taking such a form of interaction dynamics, the simulated smart grid allows communication between the different nodes in the simulation. Communication between nodes may be either an information request (e.g. status information), or a command to be executed by the receiving node (i.e. to replicate the commands that may occur between higher level nodes, such as power stations; and lower level nodes, such as transformer stations). Figure 16.10 illustrates the process followed in a scenario 2 attack agent disruption.
Figure 16.10 – Attack Agent Scenario 2 Strategy Selection

1. Random Node Selection

2. Retrieve Node Information
   - Node Type, event data, operation log and connections

3. Get Information on Surrounding Nodes
   - Node types and description data

4. Select multiple node disruption strategy

5. Disrupt Node Communication
   - Listen to external node commands
   - Respond with erroneous messages

5A. Broadcast Disruptive Commands
   - Select disruption type for each surrounding node
   - Send disruptive commands

5B.
A scenario 2 disruption from the attack agent will test whether the MA-SGS model is capable of sustaining and keeping the simulated smart grid environment stable and working adequately when the functioning of a series of nodes are at risk.

As indicated in Figure 16.10, the attack agent can cause disruptions by manipulating the response data generated by the compromised node when responding to information requests or received commands. In such a case, the MA-SGS model is tested on its ability to detect whether the messages received by a node are legitimate or compromised. The result of the message analysis should determine if the received data should be used by the node or rejected on the basis that the data could negatively affect the functioning of the node.

On the other hand, when the attack agent compromises a higher level simulated smart grid node (e.g. a power station) – with the ability to send commands to be executed by the receiving nodes (e.g. transformer stations) – the agent can generate disruptive commands. These commands can be forwarded to surrounding nodes with the aim of disrupting the connected nodes.

In such a situation, the MA-SGS model agents are tested on their ability to analyse commands received by higher level nodes to determine whether such commands are legitimate. After data analysis, if commands are determined to possibly be jeopardised, the MA-SGS model agents are required to block their execution as it would create a possible disruption in the lower level node.

In order to generate commands or messages, as well as analyse and determine the validity of such; the power agents in the simulated smart grid environment and the MA-SGS model agents require data. The following section briefly discusses the usage of data in the implemented prototype. The section describes the rationale of the manner in which data is used by the MA-SGS model to help secure the simulated smart grid’s stable and adequate functioning.
16.4 – Simulation Environment and MA-SGS Model Data Integration

Control systems used in Critical Information Infrastructure are heavily reliant on the generation, dissemination and consumption of accurate data if they are to operate at appropriate levels. The data collected in such information infrastructure enables the identification of possible use cases for the Critical Infrastructure (Pradeep, Thomas, Sabari, Balijepalli, Narashimhan & Khaparde, 2011). Therefore system design decisions, development, maintenance and diagnosis procedures take into account how data is collected and disseminated in order to apply correct control methods.

In order to make the simulated smart grid more realistic to the real infrastructure, each node embedded in the simulation has the ability to generate data that can be collected for analysis by other components. Seeing that Critical Information Infrastructure protection methods may be used to analyse data patterns to evaluate the security status of a Critical Infrastructure, the data generated and collected in the simulated smart grid is also used to determine whether the grid’s information systems may have been compromised.

As previously discussed, in order to test the MA-SGS, the simulation environment was developed. The simulation environment contains abstractions of main nodes found in the smart grid environment. In order to work with the simulation environment, data has to be generated and collected by the MA-SGS model agents for analysis. The following subsections briefly describe how data is used by the simulation environment and the MA-SGS model agents.

16.4.1 – Simulation Environment Data Integration

Just as the case would be in the real smart grid, each node in the simulated smart grid network generates data. The type of data generated at each node depends on the type of node in question. The nodes in the simulation environment generate and store data
to keep track of trends and patterns. Such data can be used by nodes in the network to determine the internal operations and status of surrounding nodes.

The data generated and collected from the simulated smart grid environment is used to enable the effective functioning of the grid. For example, electricity supply and demand data can be used to determine the percentage of the grid which is currently being served. Such data can also be used to make decisions on how much power is necessary at each point in time in the simulation. Table 16.5 shows the data generated and then collected by the different nodes in the simulated smart grid.

**Table 16.5 – Simulation Smart Grid Data Usage**

<table>
<thead>
<tr>
<th>Power Station Energy Agent</th>
<th>Data Generated:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Power generation resource usage;</td>
</tr>
<tr>
<td></td>
<td>• Electric power load generation;</td>
</tr>
<tr>
<td></td>
<td>• Power distribution data.</td>
</tr>
<tr>
<td></td>
<td>Data Consumed:</td>
</tr>
<tr>
<td></td>
<td>• Power requests from transformer stations;</td>
</tr>
<tr>
<td></td>
<td>• Resource availability data;</td>
</tr>
<tr>
<td></td>
<td>• Generation capacity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transformer Energy Agent</th>
<th>Data Generated:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Power requests for connected power stations;</td>
</tr>
<tr>
<td></td>
<td>• Power frequency and flow data;</td>
</tr>
<tr>
<td></td>
<td>• Electric power request fulfilment data.</td>
</tr>
<tr>
<td></td>
<td>Data Consumed:</td>
</tr>
<tr>
<td></td>
<td>• Power requests from microgrid substations;</td>
</tr>
<tr>
<td></td>
<td>• Power transfer capacity.</td>
</tr>
</tbody>
</table>
Table 16.5 – Simulation Smart Grid Data Usage (cont.)

<table>
<thead>
<tr>
<th><strong>Microgrid Energy Agent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Generated:</strong></td>
</tr>
<tr>
<td>- Power request for connected transformer substations;</td>
</tr>
<tr>
<td>- Power storage metrics;</td>
</tr>
<tr>
<td>- Power flow and frequency at demand centre.</td>
</tr>
<tr>
<td><strong>Data Consumed:</strong></td>
</tr>
<tr>
<td>- Power requested from consumer nodes;</td>
</tr>
<tr>
<td>- Consumer power consumption frequency data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Consumer Energy Agent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Generated:</strong></td>
</tr>
<tr>
<td>- Device usage data;</td>
</tr>
<tr>
<td>- Power request for microgrid substation;</td>
</tr>
<tr>
<td>- Smart meter data stored for consumer analysis;</td>
</tr>
<tr>
<td>- Power flow and frequency generated at the consumer node.</td>
</tr>
<tr>
<td><strong>Data Consumed:</strong></td>
</tr>
<tr>
<td>- Distributed power from microgrid substation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Power Generation Consumer Energy Agent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Generated:</strong></td>
</tr>
<tr>
<td>- Device usage data;</td>
</tr>
<tr>
<td>- Power request for microgrid substation;</td>
</tr>
<tr>
<td>- Smart meter data stored for consumer analysis;</td>
</tr>
<tr>
<td>- Power flow and frequency generated at the consumer node;</td>
</tr>
<tr>
<td>- Power generation metrics;</td>
</tr>
<tr>
<td>- Power storage metrics.</td>
</tr>
<tr>
<td><strong>Data Consumed:</strong></td>
</tr>
<tr>
<td>- Distributed power from microgrid substation;</td>
</tr>
<tr>
<td>- Power generation parameters for the node.</td>
</tr>
</tbody>
</table>
All data generation, collection and exchanges that occur in the simulation environment are recorded for further use. Over the duration of the simulation, the data can be analysed for patterns that determine the behaviour of the simulated smart grid node. Such data patterns can be used by the MA-SGS model’s agents when analysing whether a protected node is working within its acceptable parameters. The following subsection describes the manner in which the MA-SGS model uses data in the simulated smart grid.

16.4.2 – MA-SGS Model Data Integration

According to Govindarasy, Hahn & Sauer (2012), for a security enabled system to work appropriately and protect the asset which it encompasses, it needs to have access to correct information that it can use to detect any threats to its domain. The MA-SGS took this notion into account, so, as a result, every agent is able to access the information it requires to secure the smart grid. Figure 16.11 illustrates some of the potential data sources that a resilient security system can use to help detect threats to a Critical Infrastructure such as a power system.

![Figure 16.11 – Data Sources for Attack-Resilient Control Systems (Govindarasy et al., 2012)](image)

The MA-SGS model uses the data sources suggested by Govindarasy et al. (2012) in Figure 16.11. The prototype of the model draws data from each of the data sources and processes the data to determine the possibility of a threat to the simulated smart grid.
An important factor to take into account is that for each of the potential data sources, the agents at each node will be collecting data that is relevant to its node’s type. The list below describes how the data sources are used by the MA-SGS model:

- **Forecasts**
  A forecasting method such as the Autoregressive Integrated Moving Average (ARIMA) model can be used to evaluate past observations to predict future values of the data in question (Areekul, Senju, Urakasi & Yona, 2009). At each node, the MA-SGS agents collect the prevailing operational numerical data at each point in time.

  An example could be the amount of power generated or consumed at the smart grid node. The MA-SGS agents can use the ARIMA model to forecast the data to create an expectation of what probable values, in terms of power generation of power consumption could be recorded. Values that lie beyond the forecasted threshold trigger the possibility of an attack to the node.

- **Situational Awareness**
  The MA-SGS agents take into account the current situation of the surrounding environment to determine possible deviations from the data patterns that are analysed over time. Information – such as the operation status and average power flow and frequency data of surrounding nodes – allows the node to keep track of any deviations that indicate the possibility of a compromise in the grid.

- **System Data**
  All events occurring on a node in the simulated smart grid are recorded to keep a historical log of all that has happened to the given node. The MA-SGS node uses such data to analyse and continuously learn the regular operation ranges of the node. The model agents identify the optimal operation parameters of the node from the log data. Changes to the node’s operational data that highly deviate from the optimal operational parameters are analysed as a possible compromise to the node.
• **System Resources**

Resource-using nodes such as power stations and consumer nodes with the ability to generate power for the grid present a new tier of data that is used by the MA-SGS model agents. Such resources (e.g. generation reserves, generation devices etc.) can be used as part of the response the MA-SGS agents use to avert emergency situations in the network’s node.

For example, if the transmission of power to a power generation consumer agent is adversely affected, the MA-SGS agents enable the use of the stored power until the power connection of the node is re-established.

• **Attack Templates**

As the simulated smart grid is exposed to different attacks from the attack agent, the MA-SGS agents continuously capture and store data on the various different forms of attack. The MA-SGS agents learn to classify the attack patterns in order to help detect the future early signs of an attack that would trigger response actions. The more attack occurrences the model agents are exposed to, the better their knowledge of attack patterns become.

In order to monitor the events occurring in the simulated smart grid, the MA-SGS model is given access to the data in the system. Each node is deployed with its own set of MA-SGS model agents and the information generated within the node is readily available to the agents in it. If any unavailable information is needed, the MA-SGS agents can request information from the surrounding external nodes by using the interoperability agent.

The following section of the chapter is devoted to discussing the process of initialisation of the model, along with the visualisation layer of the simulated smart grid environment and MA-SGS model's prototype user interface.
16.5 – Visualisation Layer

To this point, the current chapter has discussed the details of the prototype implementation developed to evaluate the use of a multi-agent model to enhance smart grid security. The previous implementation layers, as discussed in the current chapter, work in the background to simulate the smart grid and all of its components as well as the MA-SGS model. Subsection 16.5 now discusses the visualisation layer of the SmartGridSim system, which, by means of a user interface, allows for viewing the current state of a simulation run of the prototype system.

Figure 10.1 (page 132) illustrated an overview of the MA-SGS model by showing the components of the model as well as the overall initialisation steps of the model. Figure 16.12 shows the initialisation steps used in the model. The current subsection follows the structure of the model’s steps and shows the user interfaces that visualise the background events carried out by the other implementation layers.

![Figure 16.12 – Overall Model Initialisation Steps](image)

16.5.1 – Initiate Simulation Environment

To initialise the simulation of the smart grid environment, the simulation layer first requests basic information it will then use to generate a sample smart grid environment. The necessary information includes the following details:

- Number of power stations;
- Number of transformer stations per power station;
- Number of microgrid substations per transformer station;
- Number of consumer nodes per microgrid substation.
The simulation layer takes the supplied details and generates the topology of the simulated smart grid. Each node of the network is generated for the current simulation run and power and information transfer lines are created between each of the nodes. For each node that is generated, the simulation layer randomises the properties that give further detail for each of the nodes in the simulated smart grid. Figure 16.13 illustrates this process. Refer to Appendix A to get a list of the details that are generated for each node of the simulated smart grid.

![Simulation Layer Smart Grid Network Generation Diagram](image)

**Figure 16.13 – Simulation Layer Smart Grid Network Generation**

As the simulation environment generates the simulated smart grid according to the user supplied parameters, the visualisation layer loads and displays the main user interface used to display all simulation details. Figure 16.14 shows the user interface used to collect the parameters necessary to generate the smart grid simulation environment.

The main user interface first loads and then waits for the grid generation to end (and the simulation events to be initiated), before it starts rendering the simulated smart grid environment details. Figure 16.15 shows the main user interface waiting for the simulation environment to be generated and the start of the simulation events.
After the simulated smart grid network is generated, all of the network's details are stored in a database. The simulation environment then waits for a start command from the user to initiate the simulation so that all interaction events between nodes can be...
triggered. The following subsection describes the initialisation of the node agents necessary to run the simulation.

16.5.2 – Initiate Node Agents

After the simulated smart grid network is generated using the user interface in Figure 16.15, the user of the prototype can select to initiate the simulation of the smart grid. Selecting to start the simulation causes the prototype to initialise the energy agents described in section 16.3 for each node of the simulation smart grid network and the MA-SGS model agents that are situated in each node of the same network according to the phases described in Chapters 12, 13, 14 and 15.

The Simulation Controller Agent (SCA) described in section 16.3 is initialised to control the overall operation of the smart grid network nodes. The SCA is only initialised after all other node agents are initialised and working. Figure 16.16 illustrates the initialisation of agents in the simulated smart grid network.

![Diagram](image)

**Figure 16.16 – Simulation Layer Network Node Agent Initialisation**
After the initialisation of the smart grid simulation and MA-SGS agents, the user interface loads the components that render the nodes of the network. The user interface displays all generated network nodes and the connections between each node. In order to help determine the types of nodes in the simulated smart grid network, the visualisation layer's user interface adds detail to each node control to indicate its type and current status. Figure 16.17 shows each of the node user interface controls used for each type of smart grid node in the simulation. Figure 16.18 shows the rendering of an entire generated smart grid.

![Visualisation Layer Smart Grid Node User Interface Controls](image)

**Figure 16.17 – Visualisation Layer Smart Grid Node User Interface Controls**

![Visualisation Layer Simulation Network Network View](image)

**Figure 16.18 – Visualisation Layer Simulation Network Network View**
When large networks (i.e. networks with more than 150 nodes) are generated in the prototype, viewing the information of each node becomes difficult to visualise since the controls used in the user interface display the entire size of the network. The GraphSharp library used to render the network provides zoom functionality to isolate into any of the nodes in the network (Graph#, n.d.). Figure 16.19 shows more detailed zoomed-in views of the network seen in Figure 16.18.

Figure 16.19 – Simulation Smart Grid Network Node Detailed Views
During simulation, the smart grid environment generates data on the current state of each node in the network. Such data is then aggregated to determine the overall status of the network. The status of the network is determined and classified as described in Tables 16.1 and 16.2. Figure 16.20 illustrates the gauge control in the user interface that reports the state of the grid in real time.

![Simulation Smart Grid Network Operational Status Gauge](image)

**Figure 16.20 – Simulation Smart Grid Network Operational Status Gauge**

Figure 16.21 shows the full user interface in the visualisation layer. The user interface shows the smart grid simulation network, as well as real time updates reporting on the state of the grid’s simulation.

The ‘Live Event Log’ button provides a view of all events occurring across the entire grid (e.g. commands executed, messages exchanged, MA-SGS agent events etc.). All events are logged to a database and printed for viewing in the user interface by redirecting the messages printed to the prototype’s console.

The ‘Live Simulation Results’ button gives a real time view on the performance of the MA-SGS model in securing the simulated network. The results of the model are discussed in Chapter 17 (section 17.2) of the dissertation.

The ‘Attack Agent Operations’ button provides information on the simulated attacks performed by the attack agent used to test the model. From this user interface, the agent can also be instructed to perform attacks. The following subsection describes the initialisation and use of the attack agent through the prototype’s visualisation layer.
16.5.3 – Initiate Attack Agent

As discussed in Chapter 15, the attack agent is only initialised during phase IV (seen in Figure 15.2) of the initialisation process of the MA-SGS model. The attack agent is only initialised after each of the network nodes has had their MA-SGS agents initialised. Figure 16.22 shows the initialisation of the attack agent.

![Figure 16.22 – Visualisation Layer Attack Agent Initialisation](image-url)
After the attack agent is initialised, the visualisation layer loads the user interface that allows the user to view events the agent has initiated. The user interface shows a detailed list of all disruption attempts conducted by the agent. Figure 16.23 shows a sample list of disruption attempts in a simulation.

![Sample Attack Agent Disruption Attempt List]

**Figure 16.23 – Sample Attack Agent Disruption Attempt List**

During the execution of the disruption attempts by the attack agent, the user interface displays additional details during runtime in an event log user control. Figure 16.24 shows a sample event log window displaying the details of disruption attempts. The ‘Live Event Log’ of the main user interface displays a log window similar to Figure 16.24 that shows the events initiated by all agents operating in the simulation environment.

![Sample Attack Agent Event Log]

**Figure 16.24 – Sample Attack Agent Event Log**

As described in section 16.3.5, the attack agent carries out disruption attempts by its own means. Such disruption attempts may be initiated by the user of the prototype. The visualisation layer allows the user to launch a disruption attempt at a time of choice. Figure 16.25 shows the user interface that allows a user to launch a disruption attempt.
In order to allow easy control and monitoring of the attack agent’s actions and its effects on the operation of the simulated smart grid network, the visualisation layer organises each of the user controls seen above in a single location. Figure 16.26 concludes the series of the prototype implementation screenshots by showing the complete attack agent operation control interface.
The user interface also includes a graph that shows the current operational status of the simulated smart grid in the duration of disruption attempts to show in real time how the simulation’s stability may have been compromised by the agent.

16.6 – Conclusion

The current chapter provided a more in-depth discussion of the implementation of the simulation environment. The implementation was broken down to four layers. Each layer serves its purpose to support the running and testing of the MA-SGS model.

The smart grid simulation layer provides a test-bed environment for the MA-SGS model. The communication layer provides a pipeline used to exchange information between agents. The MA-SGS layer contains the proposed multi-agent based security model discussed in the dissertation. The visualisation layer provides all necessary user interfaces to run and monitor the execution of the simulation.

Chapter 16 extended the discussion of the design and development of MA-SGS model to further address the research objectives of the dissertation. The chapter also explained the methods used by the prototype system to enhance the security and resilience of the smart grid.

The following chapter reports the results obtained from simulation runs of the MA-SGS model. The prototype was tested over multiple simulations to extract enough results to provide a better observation of the MA-SGS model's performance. The results documented in Chapter 17 help evaluate the effectiveness of the model in meeting the research objectives of the dissertation.
17.1 – Introduction

The visualisation layer of the prototype provides a ‘Live Simulation Results’ user interface. The user interface provides real-time data for the duration of the simulation on the metrics of the environment. The current chapter is devoted to reporting on the results obtained from running simulation runs on the prototype system. A video explaining the use of the prototype can be found on the accompanying DVD of the dissertation.

The chapter begins by describing the settings used to run simulations of the model. A set of metrics demonstrating the results from simulation runs with different settings are then briefly discussed before moving on to Chapter 18 where the conclusion of the dissertation is discussed and the MA-SGS model is evaluated.

17.2 – MA-SGS Model Simulation Results

The results of the prototype implementation are based on a series of simulation runs that allowed the MA-SGS model agents to learn from the results of previous simulations. Table 17.1 shows the criteria used to generate the simulation networks used for each of the prototype’s simulation runs.

<table>
<thead>
<tr>
<th>Network Property</th>
<th>Value Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Power Stations</td>
<td>1</td>
</tr>
<tr>
<td>Number of Transformer Substations per Power Station</td>
<td>2</td>
</tr>
<tr>
<td>Number of Microgrid Distribution Substations per Transformer Substation</td>
<td>2</td>
</tr>
<tr>
<td>Number of Consumers per Microgrid Distribution Substation</td>
<td>3</td>
</tr>
<tr>
<td>Maximum Simulation Duration (not set by user)</td>
<td>2 hours</td>
</tr>
</tbody>
</table>
The values used to generate the test simulation network are intentionally small to ensure the performance of the model in the machine used for the test. Details of the machine used as well as other details of the implemented prototype system are reported on in Appendix B. Running a network of 150 nodes on a single machine, for example, would create at least 600 individual agents. Managing that number of agents can put a rather high computational stress on a single machine running the prototype system.

Apart from the simulation environment using a wide array of agents to simulate events in the smart grid, the MA-SGS model uses sets of three agents in each node of the simulated network. Two additional agents, namely the Simulation Control Agent and the Attack Agent, form part of the prototype system. The results collected on the simulation runs took the following aspects into consideration:

- Agent interaction,
- Agent activity;
- Threat detection;
- Defence strategy selection;
- Operational stability;
- Restoration and recovery ability.

The subsections that follow show the metrics collected for each aspect on simulation runs, and a brief discussion on the results that were obtained to explain their meaning. In order to allow the user to analyse the results of the simulation run in real-time, the prototype provides a live result view. Figure 17.1 shows the test simulation network and a results view of the prototype during a simulation run.

17.2.1 – Agent Interaction

Agent interaction and communication is mainly managed by the Interoperability Agent of the MA-SGS model. In order to test its ability to run within the simulation and correctly pass along information requested between the Process Monitoring and Security agents at a node, a simulation run was carried out with the Simulation Control and Attack agents disabled so the Interoperability Agent’s actions could be more objectively collected.
Figure 17.1 – Prototype Simulation Smart Grid Network and sample Live Results View
Figure 17.1 – Prototype Simulation Smart Grid Network and Sample Live Results View (Cont.)
Figures 17.2, 17.3, 17.4, 17.5 and 17.6 report on the number and volume of messages processed by the Interoperability Agent in a single simulation run used to evaluate its functionality.

Figure 17.2 – Messages Processed (distributed by source)
The results in Figure 17.2 show that most of the communication that occurs within the simulated smart grid environment is between internal components found at each node. All external messages were processed by a web service. External communication in the simulated smart grid occurred when individual nodes gathered status information from surrounding nodes.

Figure 17.3 – Messages Processed (distributed by sender Agent)
Figure 17.3 shows that the Interoperability Agent is the most interactive when compared to the other agents in the MA-SGS model. This observation comes as no surprise as the main task of the Interoperability Agent is to liaise the communication for all operations of the MA-SGS model.

Figure 17.4 – Messages Processed (by type)

Figure 17.4 shows that request messages are the most frequent in the simulated smart grid. Status request messages and data check messages are constantly exchanged in the simulation in order to compute either the status of the smart grid as a whole, or to determine whether data required for analysis is available.

Figure 17.5 – Messages Processed based on Completion
Given the high activity of the Interoperability Agent observed in Figure 17.3; Figure 17.5 further shows that the agent was capable of processing the bulk of the messages exchanged during the simulation run. Unprocessed messages are those that were still pending for processing by the time the simulation run was stopped. The more messages the Interoperability Agent is able to process, the better the model will work as other agents will be able to continue their operations after having received requested information.

![Number of Messages Processed during Simulation Run](image)

**Figure 17.6 – Number of Messages Processed over simulation time**

As demonstrated in Figure 17.6, the number of messages exchanged in the MA-SGS model can be seen as being very high. The high number of messages though is not processed by a single Interoperability Agent as the MA-SGS model uses a multi agent approach where each type of agent (i.e. – Interoperability Agent, Process Monitoring Agent and Security Response Agent) is deployed on every node in the simulated Smart Grid.

The results reported on in the current section reflected on data retrieved from a single simulation in which the Simulation Control and Attack Agents were disabled. The results reported on in the next session onwards are based on a series of three simulation runs where all agents in the simulation were fully functional.
17.2.2 – Agent Activity

Agent activity refers to the actions monitored from each of the agents found in the simulation of the smart grid and MA-SGS model. Each agent has a set number of actions that must be executed in order to meet its intended purpose. The purpose of the agent is dependent on its type. Table 17.2 lists all types of agents that may be found in the prototype system.

<table>
<thead>
<tr>
<th>Smart Grid Simulation Agents</th>
<th>MA-SGS Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Energy Agent (CEA)</td>
<td>Interoperability Agent (IA)</td>
</tr>
<tr>
<td>Power Generation Consumer Agent (PGEA)</td>
<td>Process Monitoring Agent (PMA)</td>
</tr>
<tr>
<td>Microgrid Energy Agent (MEA)</td>
<td>Security Response Agent (SRA)</td>
</tr>
<tr>
<td>Transformer Energy Agent (TEA)</td>
<td>Simulation Control Agent (SCA)</td>
</tr>
<tr>
<td>Power Station Energy Agent (PSEA)</td>
<td>Attack Agent (AA)</td>
</tr>
</tbody>
</table>

Figure 17.7 reports on the level of activity from each agent, found across three simulation runs carried out under the same circumstances to evaluate on how consistent operations were.

When examining the logged activity levels of the agents running the simulated smart grid, the Consumer Energy Agent was consistently across all three simulation runs the most active agent. This observation highlighted that in the simulation of the smart grid, the consumer nodes were essentially the drivers of activity. This activity in the consumer nodes came from the consumption and generation of electric power; which are actions all other subsequent smart grid nodes (i.e. – microgrid, transformer and power station nodes) had to respond to.

Amongst the MA-SGS model's agents, the Interoperability Agents deployed on the simulated grid showed to be the most active. This observation emphasises the relevance of the results examined in section 17.2.1 where the Interoperability Agent processed most of the data, thus meaning it was required to act on data much more often than the Process Monitoring and Security Response Agents.
The following section reports on the detection of possible threats by the MA-SGS model agents.
17.2.3 – Threat Detection

Threat detection refers to the MA-SGS agents’ ability to correctly flag and block potentially harmful events and commands. The responsibility of detecting possible threats is on the Process Monitoring Agent working at each node. Threats posed on to the system are created by the Attack Agent that tests the MA-SGS model. Figure 17.8 shows the results obtained from the Process Monitoring Agent after analysis of all occurrences to decide whether the commands or events should be flagged as possible threats.

**Simulation Run 1**

- **Flagged**: 5%
- **Authorised**: 95%

**Simulation Run 2**

- **Authorised**: 75%
- **Flagged**: 25%

**Simulation Run 3**

- **Authorised**: 89%
- **Flagged**: 11%

*Figure 17.8 – Process Monitoring Agent Detection*
When monitoring each command or event occurring at each node, the Process Monitoring Agent uses the knowledge that has been gathered by the system which indicates the likelihood of a possible threat. If an occurrence at the node resembles a previously identified threat, the occurrence is flagged for further analysis by the Security Response Agent.

Keeping the learning method in mind, it can be observed in Figure 17.8 that the Process Monitoring Agent was able to identify a larger percentage of flagged occurrences as it learned more from previous simulation runs. As more simulation runs were made, the Process Monitoring Agent managed to flag occurrences that were more similar to previously confirmed threats from the Security Response Agent.

The following section looks at how the data processed by the Process Monitoring Agent was then processed by the Security Response Agent to make the final deliberation on whether an event or command should be allowed to occur or be blocked. The section evaluates reports on the decisions made by the Security Response Agent.

### 17.2.4 – Defence Strategy Selection

Defence strategy selection refers to the MA-SGS model's Security Response Agent's ability to analyse occurrences that were flagged to be potentially harmful events or commands by the Process Monitoring Agent. To analyse the flagged occurrences, the Security Response Agent at the node uses the information from the data sources suggested in Figure 16.10.

Based on the type of flagged command or event, the agent analyses the current situational data of the node, previously identified threats on the type of node, property data of the node, previously created knowledge of the node and forecasted data that is expected to prevail on the node. The agent receives information on the validity of the occurrence based on the analysis and stores the analysis data for use in later analysis runs.
After analysing each occurrence, the SRA is then responsible to make the final decision to either block the event and collect knowledge on it, or authorise the occurrence to run on the smart grid. Figures 17.8 and 17.9, respectively, report on the SRA’s decision on flagged occurrences which were analysed by the agent and the decisions on the occurrences which originated from attack disruption attempts of the Attack Agent.

![Pie charts showing decision results for different simulation runs](image)

**Figure 17.9 – Security Response Agent Detection**

The results obtained from the decisions reported on in Figure 17.9 are recorded to form part of the knowledge gathered for each node of the simulated smart grid. The knowledge is then re-used over time when analysing future events. The constant recording of new information aids the SRA agent to improve its decisions as it analyses...
more occurrences. The SRA makes constant use of the extra data sources when making a final decision on whether to authorise or block an occurrence.

From Figure 17.9, as more simulation runs were carried out, the Security Response Agent managed to block a larger percentage of the flagged events which the agent examined. The increase in the percentage of blocked occurrences comes as the accuracy of flagging potentially disruptive occurrences increase.

Figure 17.10 – Processed Attack Agent Disruption Attempts

The Security Response Agent augments on the knowledge discovered by the model by confirming whether flagged events are indeed disruptive. Such knowledge
augmentation explains how the accuracy is increased in identifying disruptive occurrences.

With the increase in accuracy seen in Figure 17.9, it can also be observed on Figure 17.10 the percentage of blocked disruption attempts from the Attack Agent has been increasing as more simulation runs are done.

The following section reports on the statistics pertaining to the simulated smart grid’s operational stability. The goal of the MA-SGS model is to attempt to promote the most desirable operational status of the smart grid.

17.2.5 – Smart Grid Simulation Operational Stability

For the purpose of the dissertation, operational stability is evaluated by examining the simulated smart grid’s observed operational levels during the simulation. The range of possible statuses and their indication of the smart grid’s capacity was indicated in Tables 16.2 and 16.3 (page 184). Figure 17.11 shows the chart reporting the operational levels observed across the three simulation runs being used for comparison purposes.

![Smart Grid Operational Level during simulation](image)

Figure 17.11 – Smart Grid Operational Level Observed

232
In Figure 17.11, Simulation Run 2 and 3 demonstrate improvements in operational stability when compared to Simulation Run 1. The improved operational stability comes from the model’s improved ability to detect disruptions that put the grid into states that are not desirable.

The following section reports on the operational states observed across each of the three simulation runs. The intention of the MA-SGS model is to keep the simulated smart grid in the most desired state where all nodes connected to the grid are operational.

17.2.6 – Smart Grid Simulation Restoration and Recovery

Tables 16.2 and 16.3 indicated the states that can be observed in the operation of the simulated smart grid. Table 16.1 was used as a reference to indicate the desirability of the simulated smart grid’s status at each point in time.

The restoration and recovery ability of the MA-SGS model was evaluated by looking at the status data observed during a simulation and showing the time expended between operation states that were desired and not desired.
Figure 17.12 shows an increase in the recording of ‘Acceptable’ states on the smart grid as more simulation runs were executed. From Simulation Run 1 through to 3, the MA-SGS model agents were able to better respond to occurrences which promoted ‘Caution’ and ‘Emergency’ states. Thus keeping the smart grid operational for the most part of the simulation runs.

Taking the results of the smart grid simulation into consideration; the operation of the MA-SGS model’s agents demonstrated improvements over time as more simulations were carried out. The model’s ability to learn from previous experiences aided the model to improve its performance over time.

17.3 – Conclusion

The current chapter reported on the results obtained from the implementation of the MA-SGS model and its simulated Smart Grid environment. In order to allow for a more objective report, three simulation runs with the same characteristics were used to show the model’s performance.

The simulation characteristics were used to generate the same environment to demonstrate how the model would behave as it learned more from its previous experiences. The results were examined using four criteria that indicated the model’s ability to meet its intended goals. The following chapter concludes the addressed research topic and provides a review to the research questions set out in the dissertation.
Chapter 18
Conclusion
18.1 – Introduction

The dissertation aimed at creating a multi-agent model used to enhance security in Critical Information Infrastructure protection. Given the wide array of Critical Infrastructure domains available, the selection of the smart grid as its test-bed was selected due to its high connectivity environment described in Chapters 4 and 5 of the dissertation. Being a relatively new paradigm shift in how electric power systems are designed and operated, it was seen as an appropriate research topic for the dissertation.

The current chapter is the culmination of the researched material outlined in the entire dissertation, which sets out to answer the research questions defined in Chapter 1. The chapter begins by evaluating the MA-SGS model designed to enhance security in the smart grid. The model’s evaluation is followed by a re-visit of the dissertation’s research questions which set the research objectives thereof. A brief look into the future possibilities that could come from this research is discussed before the work conducted is drawn to a conclusion in the last section.

18.2 – Model Evaluation

Section 1.3 of the dissertation listed the objectives set out to be fulfilled by the research study. Each chapter of the dissertation aimed at meeting each of the objectives. Amongst all of the set objectives, the design and evaluation of the MA-SGS model can be seen as the main objective. Such an assertion is due to the fact that the creation of the model facilitates the finding of answers to the research questions set in section 1.4.

According to Habicht, Victora & Vaughan (1999), the main purpose of an evaluation study is to determine the plausibility, probability or adequacy of the subject in question. The current subsection is devoted to evaluating the characteristics and results obtained from the MA-SGS model.
To achieve an objective evaluation of the model, three criteria were used. Discussion on each criterion is expanded in subsection 18.2. Evaluation was based on each of the following criteria:

- Resilience and robustness;
- Model component modularity;
- Consistency and integrity.

### 18.2.1 – Resilience and Robustness

According to Fiksel (2003), the resilience of a system is determined by its ability to withstand disruptions to its operations while maintaining its regular functions and services. In the dissertation, maintaining the stability of the simulated smart grid under disruptive conditions brought upon the attack agent is a factor that demonstrates the MA-SGS model's ability to enhance resilience to the Critical Information Infrastructure in question.

The results in chapter 17 demonstrate that, at times of disruptions by the attack agent, the operational state of the simulated smart grid was, on average, maintained. This essentially means that in times of disturbances, the MA-SGS model agents managed to maintain operational stability, thus maintaining the grid's ability to continue providing services to the different nodes of the network.

Meyer (1997) defined robust systems as those with the ability to 'react appropriately to abnormal conditions'. This means that these systems have the capacity to analyse abnormal data and still act in the manner that best suits their operations. Therefore, a system that, although faced with different disruptions, is still capable of making decisions that allows it to generate the desired output.

The different types of disruption strategies acted on by the attack agent created abnormal data that disrupted the functioning of the simulated smart grid environment.
These different strategies created abnormal situations that prompted the MA-SGS model to establish acceptable operational states in the simulation environment.

Sussman (2007) stated that evolving systems tend to become more robust over time as every new knowledge-producing situation enhances the ability of the system to adapt. The MA-SGS agent’s ability to learn from its experiences enabled the model to evolve over time and make better decisions as more simulation runs were conducted.

Resilience and robustness were simultaneously considered in the functioning of the MA-SGS model as resilience allowed the model to demonstrate its robustness in maintaining the operations of the simulated smart grid environment.

18.2.2 – Model Component Modularity

Component modularity can be described as the degree of autonomy exhibited by each individual component in a system (Sosa, Eppinger & Rowles, 2007). The more independent a component is in a system, the more modular the system can be classified to be. Modularity allows flexibility in a system as its different components can be removed, replaced or re-arranged while the system still meets its purpose.

The design of the MA-SGS model allowed the compartmentalisation of functionality in different components. These components were then integrated to work together. At each node, the MA-SGS model used three different agents. Each had its responsibilities to meet and was combined to use its individual functionalities to monitor the stability of the grid’s node.

At the agent level, each agent had an internal structure where each of the agent’s components also had independent functions that, when combined, allowed the agent to meet its purpose. This compartmentalisation allowed more flexibility in the design of the agent.
18.2.3 – Consistency and Integrity

In terms of the operation of the simulation environment of the prototype, the model can also be evaluated by its ability to consistently maintain the integrity of the simulated smart grid. In other words, this refers to the model’s ability, over time, to prevent the degradation of the simulated smart grid.

Maintaining integrity in the environment referred to the maintaining of desired levels of operation in the simulation environment. The desired levels of operation were indicated in Chapter 16. Consistency of the model referred to how it responded to disruptive situations in the environment.

In any given network node, the MA-SGS agents learned from the data patterns they analysed and the results of the response actions they took. The agents also learned from the information made available by other nodes within the same network. Such mechanisms allowed the agents to collaborate into using the solutions that worked best for the disruption types that were classified.

This convergence allowed the model agents in different nodes to become more consistent in response strategies selected to deal with known disruptions. The response strategies that were united provided the most effective solution to maintaining the integrity of the simulation environment.

The evaluation of the MA-SGS model focused on three criteria and discussed how the model performed in each one. The discussion of how the model performed was based on the results obtained from the simulation runs and reported in Chapter 17. The results obtained only reflect on the characteristics taken into account in the creation of the simulated smart grid environment as well as the MA-SGS model. The following section presents a critical assessment of some of the considerations taken into account in the development of the simulation environment and the MA-SGS model.
18.3 – Critique

As previously explained in Chapter 16, in order to test the MA-SGS model, a simulation environment was needed. The reason for the development of a custom simulation tool was the lack of open source smart grid simulation environments that are readily built to enable integration with other custom-built subsystems and flexible enough to include considerations that are not included in the tool.

The simulation environment had to show some of the properties and concepts found in the real world smart grid. The properties of the environment were included to show the kind of data used and the interaction dynamics witnessed in the real environment.

The development of the smart grid simulation environment was an attempt to create a high level representation of the operations of the real world grid. The simulation environment used abstractions of the different systems and infrastructure found in the smart grid.

The real smart grid’s ICT infrastructure is composed of a myriad of different information and cyber-physical systems. Each system that works in the smart grid is complex in its own right, therefore creating multiple points of vulnerabilities to the grid. The simulation environment did not simulate all systems involved in the real environment. For example, the simulation environment did not simulate the network technologies used, the protocols used for communication, the smart efficient energy management systems used by different consumers and the infrastructure used in the integration of smart electric vehicles in the grid. Though development of the MA-SGS model would have potentially benefitted from a more holistic simulation environment, it was deemed to have met its overall intended purposes to help achieve the research objectives of the dissertation.

Although limited to the high level abstraction of the systems used in the smart grid and the interaction dynamics between them, the simulation environment still provided
functions that could be monitored by the MA-SGS model. Through its monitoring, analysis and response abilities; the MA-SGS attempted to protect the integrity and availability concerns that could be compromised through the IT aspects of the smart grid represented by the simulation environment.

With the simulated environment, the MA-SGS model managed to demonstrate an overall approach in which smart grid network nodes can be kept operationally stable. Such stability referred to the model’s ability to allow the simulation environment to be resilient and exhibit more robust behaviour in the generation and consumption of electric power in the grid.

The MA-SGS model demonstrated the proposed multi-agent approach to collect and analyse data generated at each point of the abstracted smart grid. From the processing of such data, the MA-SGS model showed how such analysis processes can be used to determine actions that maintain stability in the smart grid’s simulation environment.

The simulation environment therefore helped to evaluate the suitability of the multi-agent model so the dissertation’s questions could be answered. The following subsections re-visit the dissertation’s research objectives and questions.

18.4 – Research Objectives and Questions

At this stage of the dissertation, the research objectives and questions are re-visited. Chapters 1 to 17 defined the research objectives and the problem statement addressed by the dissertation; discussed background information about the different research domains the problem statement encompassed; proposed a potential model as a solution of the defined problem statement; and, lastly, evaluated the suitability of the model.

The content discussed in each chapter was selected to best meet the research objectives and to provide a clearer understanding of the purpose of the dissertation. Table 18.1 shows the chapters where each research objective was addressed.
Table 18.1 – Research Objectives Addressed

<table>
<thead>
<tr>
<th>Research Objectives</th>
<th>Chapter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification and analysis of aspects relevant to Critical Information Infrastructure protection</td>
<td>2 and 3</td>
</tr>
<tr>
<td>Description and understanding of the security requirements for a resilient and robust Critical Information Infrastructure</td>
<td>3</td>
</tr>
<tr>
<td>Identification and analysis of current developments in the smart grid and the security aspects discovered to date</td>
<td>4 and 5</td>
</tr>
<tr>
<td>Define and discuss concepts to do with intelligent agents and the use of multi-agent systems</td>
<td>6, 7, 8 and 9</td>
</tr>
<tr>
<td>Define and discuss common machine learning techniques</td>
<td>7</td>
</tr>
<tr>
<td>Design and implement a multi-agent system to monitor and enhance security in a simulated smart grid environment</td>
<td>9, 10, 11, 12, 13, 14 and 15</td>
</tr>
<tr>
<td>Examine results obtained from the simulated smart grid environment in order to evaluate the multi-agent approach to enhance security, resilience and robustness in the smart grid Critical Information Infrastructure.</td>
<td>16 and 17</td>
</tr>
</tbody>
</table>

Each chapter was added to the dissertation on the basis that it would help meet the research objectives identified in Chapter 1 and/or provide additional background knowledge that would aid in the considerations taken into account to address the problem statement and research questions. The current chapter now continues on from Chapter 10 to address the research questions of the dissertation. Before the primary research question of the dissertation is addressed, the three sub-questions are first elaborated on.

**Question 1** *Can intelligent agents in multi-agent systems be used in Critical Information Infrastructure protection?*

The background review and literature study section of the dissertation investigated aspects related to Critical Information Infrastructure protection and the purpose of multi-agent subsystems. Considerations as to what makes software agents intelligent, and how such agents can be deployed into complex systems such as Critical
Infrastructures were also investigated.

Research on the applicability of agent-based frameworks in Critical Information Infrastructure demonstrated that there have been multi-agent solutions developed to work with Critical Information Infrastructure. Such frameworks are still used to develop agent-based systems to work on many aspects of Critical Information Infrastructure, with security being one of the focus points.

To empirically answer Question 1, a multi-agent model (MA-SGS) was proposed and developed to test the possibility of using intelligent agents in Critical Information Infrastructure protection. Intelligence enabling methods discussed in the dissertation were used to make the model’s agents emulate intelligence during their execution.

An agent-based simulation environment was developed to simulate the complex environment of Critical Information Infrastructure. The simulation environment was then combined with the proposed model to enhance its security and resilience characteristics.

The research presented in the dissertation leads to the answer that intelligent agents can indeed be used in Critical Information Infrastructure protection. The literature work researched demonstrated that agent-based solutions are capable of thriving on multiple problem domains, including information security.

**Question 2   How can a multi-agent system theory be applied to the Smart Grid?**

Chapter 10 already elaborated on Question 2 that multi-agent systems can be developed to work on the smart grid. The dissertation set out to strengthen this argument by developing an agent-based simulation of a smart grid environment. This simulation environment then served as a test-bed for the proposed MA-SGS model.

To achieve the simulation of the smart grid, the major components of the grid’s
environment were identified from the study presented in Chapters 4 and 5. Software agents were then used to simulate each one of the major components and made to work together as a multi-agent system to simulate, to some degree, the communication interactions seen in the smart grid.

The smart grid, being a complex adaptive system as discussed in the dissertation, was determined to be an appropriate candidate on which to apply multi-agent theory. In order to apply such theory, what was crucial was the identification of the components found in the grid, the interactions between them, and, lastly, the design of software agents that could work with the different components.

Chapter 17 described this multi-agent simulation of the smart grid and discussed each of the agents involved in the simulation and how the agents interact with each other. Furthermore, the dissertation discussed how software agents could be integrated with the components of the smart grid.

**Question 3**  
*As follow up of Question 2: How would the security, resilience and robustness properties of the Smart Grid’s Critical Information Infrastructure be improved with the use of a multi-agent system?*

As explained, a simulated smart grid was developed and used to investigate the suitability of using a multi-agent system to enhance security, resilience and robustness in the Smart Grid's Critical Information Infrastructure. The MA-SGS model was developed and integrated to work how such properties of the smart grid could be enhanced.

Implementation and simulation runs of the smart grid and the MA-SGS model were reported on in Chapters 16 and 17. Results shown in Chapter 17 showed that the MA-SGS model learned more and more, over multiple simulation runs, as more data was made available. The increase in data allowed the agents to learn more about patterns of threatening situations and how to recover from them. The increased learning across simulations allowed the MA-SGS model agents to
better detect events that could potentially compromise the operational state of the smart grid simulation. This enhanced the availability and integrity of the environment, meaning that the system operated more securely if threatened by disruptions.

As more simulations were carried out, the MA-SGS model also learned from the use of response strategies during moments of disruption, which helped restore optimal operational states of the simulated environment. This enhanced the resilience and robustness of the grid as more information on the effectiveness of response strategies was made available.

By giving the agents of the MA-SGS model the ability to learn from previous experiences, the agents were then able to enhance the security, resilience and robustness aspects of the simulated smart grid environment. Using the sources of data identified in Chapter 16 allowed the MA-SGS model to protect the simulated Smart Grid’s Critical Information Infrastructure.

For the purposes of the dissertation, and taking into account the limitations of the simulation environment, the MA-SGS model managed to achieve results that showed its ability to secure the grid.

With the three research sub-questions of the dissertation addressed, the primary research question of the dissertation provides an overall elaboration of the main aim of the study.

*Primary Question:* Can Critical Information Infrastructure protection in a Smart Grid environment be achieved through the use of software agents using a multi-agent approach?

If all environment aspects are used and clearly defined, then the main point to be discovered and confirmed in the dissertation is that a multi-agent system can be used to enhance Critical Information Infrastructure protection in the smart grid. However, some enhancements to the MA-SGS model could be used to better assist in Critical
Information Infrastructure protection of the smart grid. The following section briefly discusses the contribution made by the research presented in the dissertation, as well as how the model could be improved in future work.

18.5 – Research Contribution and Future Work

The research presented in the dissertation concluded that multi-agent systems can be used to model and simulate complex adaptive systems. They can furthermore be used in Critical Information Infrastructure protection. Most implementations of prototype systems using multi-agent systems to simulate complex adaptive systems used single agents to represent each complex component in the environment in question.

The MA-SGS model took a different approach in the use of multi-agent systems. Each component of the environment in question was composed of a multiple set of agents that interacted with each other. Essentially, apart from the overall use of multiple agents in the simulation environment, examination of each node in the network found multiple agents working together. Therefore this could be seen as a ‘complex environment of multi agent systems working together’. Figure 10.1 (page 132) illustrated the MA-SGS model demonstrating a multi-agent environment at each node of the smart grid network.

The MA-SGS model agents benefited from the use of data generated across simulation runs to improve on its consistency. The smart grid simulation environment could be used to generate large event data sets. These can be used to train new multi-agent models developed to classify disruptive events out of large data sets.

The dissertation also contributed by the addition of a proof-of-concept tool used to test the functioning of the security model. The attack agent could be used as a testing tool that is loaded with new disruption models that can test the ability of the security algorithm to adapt to new forms of disruption.
As with all security focused models, there is always space for improvement. The MA-SGS model is no exception. The following is a brief list of techniques and considerations that can be used to improve the MA-SGS model:

- Using a trust-based mechanism to constantly evaluate the contribution of each smart grid node to the network as a whole;
- Integration of network protocol considerations to allow communication between each node;
- Using multiple data forecasting algorithms concurrently to enhance the accuracy of forecasts;
- Using a measure of risk analysis that takes into account the possible vulnerability of each node and the likelihood of the impact the smart grid would suffer if the node or a component were to be compromised by a threat;
- Using a multi-variate approach to determine situational awareness at each point of the smart grid environment.

The items listed above certainly are not exhaustive as the model could be further modified to take into account structural details of the smart grid that show the cyber-to-physical link between the information systems and the physical infrastructure of the grid. A change of this kind would also require further development in the smart grid simulation environment to include components that were not included. The following section concludes the research study.

18.6 – Conclusion

The current chapter provided an overview of all that was discussed in the dissertation. The dissertation mainly focused on the enhancing of Critical Information Infrastructure protection through the use of multi-agent systems. To meet this main research objective, aspects of the problem domain were discussed. The MA-SGS security model, and supporting components such as a simulation environment and a disruption attack agent, were developed and evaluated to demonstrate a proof-of-concept prototype.
Appendix A: Simulation Environment SQL Server Database Diagram
Appendix B: Implementation Statistics & Simulation Environment Hardware Details

B1 – Implementation Statistics

Development environment:  
- Microsoft Visual Studio 2010  
- Microsoft Expressions Blend 2010

Development languages:  
C#, XAML & XML

Number of classes:  
45

Number of lines of code:  
+/- 13000

Database management system:  
Microsoft SQL Server 2012 Express Edition

Number of database tables:  
23 (excluding auxiliary data logging tables)

Additional Libraries/Components:  
- Extreme Optimisation Library  
- AForge.NET Framework  
- Accord.NET Library  
- GraphSharp Network Visualisation Library  
- Visifire Charts (Community Edition)  
- ConsoleWidget Control

B2 – Simulation Hardware Details

Processor:  
Intel® Core ™ i5-337U CPU @ 1.80Hz (2 cores)

RAM:  
6.00 GB

System Type:  
64-bit Operating System, x64-based processor

Operating System:  
Microsoft Windows 8 Single Language (x64)

Version:  
6.2.9200 Build 9200

System Manufacturer:  
Acer

System Model:  
Aspire V5-571PG
Appendix C: Resulting Research Output

Abstracts

C1 – Abstract 1


Abstract:

Critical Infrastructure (CI) is the term used to describe assets that are of utmost importance, or in other words, essential in the functioning of an environment. Societies depend on their critical infrastructure in order to maintain and continuously improve on their standards of living. As these systems increasingly depend on cyber-technology, their security on networked environments become crucial.

The modern smart grid has become part of CI through the enhancement it provides to regular electricity grid infrastructure. The application of biologically inspired systems to ensure security in aspects such as intrusion detection, access control, anomaly detection and others has become a widely researched field in when dealing with networked computing systems.

This paper discusses the importance of CI, the application of artificial immune systems in the protection of CI information systems and proposes a new model for smart grid protection using biologically inspired concepts.
C2 – Abstract 2


Abstract:

Critical Infrastructure is the term used to describe assets that are of utmost importance, or in other words, essential in the functioning of an environment. Societies depend on their critical infrastructure in order to maintain and continuously improve on their standards of living.

The creation of more self-sustainable methods of energy consumption and generation drives towards the creation of a better and more efficient evolution of the power grid, named the smart grid. This paper aims at creating a multi-agent model that can be applied at the individual node level of the smart grid critical infrastructure in order to help improve the reliability of the information transferred between each node on the network.

The model is composed of six agents that take the tasks of: monitoring the processes at a node, analyzing the different sensory inputs at the node level to determine security threats, notifying other nodes on the system of security threats at a node, responding to security threats through determining the best course of action to take, sharing knowledge across the entire system, and enabling communication between all different agents on the system. .
Appendix D: Accompanying DVD

D1 – Contents of Accompanying DVD

The following can be found in the accompanying DVD of the dissertation:

- A digital copy of the dissertation in PDF format;
- Foxit Reader installer file. Foxit Reader is available for free download and usage here: http://goo.gl/BJxZxE;
- Prototype source code;
- Sample screenshots of the prototype system;
- A video demonstrating the prototype system;
- VLC Media Player installer file; and
- Digital copies of the two resulting research outputs of the dissertation.

D2 – Running the Prototype Implementation

The prototype developed for the dissertation is comprised of multiple projects where each is responsible for a specific task. The implementation is divided into three projects where each is responsible for the following tasks:

- Execute the simulation of the smart grid environment and the MA-SGS model agents;
- Provide the web service interface used for exchange of information between different nodes in the simulated smart grid; and
- Provide an interactive user interface where the simulated smart grid and MA-SGS model can be viewed.

Due to the interdependencies of the projects and their operating environment, a remote server has been configured with all necessary tools and the installed version of the implemented prototype. To access the remote server, a remote desktop connection application will need to be used. The details necessary to access the remote server can be found in the accompanying DVD.


Council of European Energy Regulators/European Regulators Group for Electricity & Gas (CEER/ERGEG), (2011). *The Drive towards Smart Grids*.

Coupelon, O. (2007). Neural network modeling for stock movement prediction, a state of the art.


258


Cybernetics.


He, H. (2010). Toward a Smart Grid: Integration of computational intelligence into Power Grid. *The 2010 International Joint Conference on Neural Networks (IJCNN).*


International Conference and Exhibition, pp.1--5.


National Infrastructure Advisory Council (NIAC), (2004). Prioritizing cyber vulnerabilities. NIAC.


Southeastcon.


Sieminski, A. (2013). *Fuels Used in Electricity Generation (for the U.S. Nuclear Infrastructure Council)*.


271


