2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation

Simulating Critical Infrastructure Cascading Failure

Áine MacDermott, William Hurst, Qi Shi and Madjid Merabti
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool, L3 3AF
a.mac-dermott@2008.ljmu.ac.uk and {w.hurst,q.shi,m.merabti}@ljmu.ac.uk

***Abstract*— The reliance on critical infrastructures, which are heavily interconnected, is one of society's greatest weaknesses. An individual failure has the potential to have a huge impact on society and affect other infrastructures. Predicting the effects of a cascading failure is a challenge. In this paper, a simulation of a virtual city is presented in order to visualise the effects of a cascading failure. The simulation is used to assess the resulting effect of a telecommunications failure. Data extracted from the simulation is used to evaluate the impact of the failure on the emergency services provision. Behaviour analysis techniques are used to demonstrate how a failure in one infrastructure can impact another and present a way for organisations to plan for its effects.**

Keywords- Critical Infrastructure, Cascading Failure, Simulation, Behaviour Analysis

I. INTRODUCTION

Critical infrastructures are controlled by networked computers and can be defined as sectors that would have a debilitating impact on national security if incapacitated [1]. Failures result in devastating impact on national defence, the economy, communication, e-government systems, and society as a whole. Often heavily interconnected and mutually reliant on each other, their service provision tends to cross boarders and multiple countries, which can consider the same infrastructure as critical.

Natural phenomenon, system errors, or cyber-attacks have the ability to produce failures, which cascade as a result of the high level in interconnectivity between the infrastructures [2]. The resulting impact would cover large sectors causing devastating consequences. Critical infrastructure protection has now become a multi-disciplinary area, which requires interdisciplinary involvement.

The US Department of Homeland Security defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the government that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" [3]. Many of the nation's critical infrastructures have historically been physically and logically separated systems that had little interdependence [2]. However, because of advances in information technology, and efforts to improve efficiencies in these systems, infrastructures have become increasingly automated and interlinked. These improvements have created new vulnerabilities relating to equipment failure, human error, as well as physical and cyber- related attacks.

Within the US alone, critical infrastructures include approximately 28,600 networked Federal Deposit Insurance Corporation (FDIC) institutions, two million miles of pipeline, 2,800 power plants (with 300,000 production sites), 104 nuclear power plants, 80,000 dams, 60,000 chemical plants, 87,000 food-processing plants, and 1,600 water treatment plants [4]. There has been a growing recognition that control systems are vulnerable to cyber-attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders. Smart attacks and coordinated attacks could have severe impacts to the stability, performance, and economics of the infrastructure.

Therefore, in this paper, the focus is on an evaluation of the provision of emergency services when a cascading fault occurs, as a result of a telecommunications failure. The problem being addressed is that, as critical infrastructures become increasingly interconnected, the risk of a cascading failure occurring is becoming a realistic danger. Simulation can provide an effective role in evaluating the effects of a failure occurring and help plan for resilience. The benefits of using simulation can offer effective ways to visualise the effects of a failure in a safe environment.

A simulated city depicting the interconnectivity of eight critical infrastructures is presented in this paper. The aim of the research presented is to highlight an innovative approach for organisations and government institutions to visualise cascading failure through simulation and plan for its effects. By extracting simulation data, our research presents a method for the identification of subtle behaviour changes across multiple infrastructures, as a result a failure occurring in a single infrastructure. The system behaviour is evaluated using nine machine-learning algorithms to classify changes in behavioural patterns.

Studying the interconnections and dependencies of multiple infrastructures can lead to the development of a more holistic security approach. The aim is to present a method for infrastructure operators to view how fault(s) in a connected infrastructure has direct impact on their service provision.

The remainder of the paper is as follows. Section 2 presents a background on critical infrastructure cascading failure, and how simulation has a key role in security enhancements. In Section 3, a simulation of a virtual city is depicted. Section 4 presents a cascading failure taking place in the simulation. In Section 5 we detail the data analysis process and present a discussion of the results. Section 6 details our conclusion and future work.

978-1-4799-4923-6/14 $31.00 © 2014 IEEE
DOI 10.1109/UKSim.2014.85

II. BACKGROUND

Cascading failure occurs inside individual infrastructures, in addition to between infrastructures. Protecting the interconnected and interdependent infrastructure requires a robust partnership that provides the private sector with information on incidents, threats and vulnerabilities [5]. An appropriate, integrated, and reliable network of critical infrastructures is an essential requirement not only for infrastructure policy objectives, but also for a national economic strategy [5].

Current research focuses on risk identification and assessment, where the universality of methodologies that involve hazard maps, and risk matrices sets them apart [6]. Paradigms of system simulation are widely used as a support for decision making for prioritisation, implementation and monitoring of actions, in order to estimate risk mitigation strategies and policies.

Infrastructure protection modelling is a relatively new area of research and analysis, but terrorist attacks and natural disasters have shown that the impact of threats on infrastructures should be thoroughly evaluated, and simulation is an ideal tool to accomplish this [6].

A. *Critical Infrastructure*

Critical infrastructures, such as the power grid and water distribution facilities, include a high number of devices over a large geographical area. These infrastructures face significant threats as the growth in the use of industrial control systems such as SCADA systems and their integration to networks in order to coordinate and manage the actions of these devices [7]. The evolution of SCADA systems has also raised concerns about cyber-related vulnerabilities. The SCADA industry is transitioning from a legacy environment, in which systems were isolated from the Internet and focused on reliability instead of security, to a modern environment where networks are being leveraged to help improve efficiency [8].

Critical infrastructures are the supporting mechanisms of modern society, and cyber-attacks are increasing at an alarming rate. Security experts around the globe are now recognising the importance of effective simulation in planning the fight against the growing cyber-threat [9]. The need to remain one-step ahead of the attacker is becoming more and more important.

The consequences of failure can produce unexpected results and must be planned for in order to prevent disasters escalating through a cascading effect [9]. The close interconnectivity of these vital service providers means that failures impact the provision of other services, affecting multiple systems through a single fault.

Disruptions in one part of the infrastructure may spread out through the system and have cascading effects on other sectors [8]. An example of this is displayed in Figure 1, which shows the direct impact a power plant fault would have on other infrastructures.

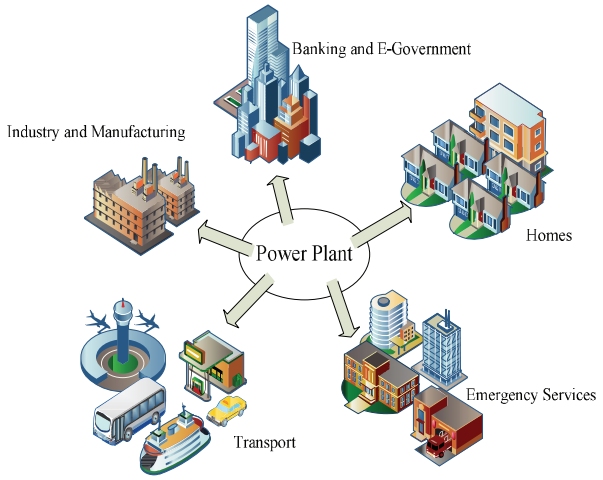

Fig. 1 Power Reliance

It is visible from the figure that a failure, such as the one presented, can easily propagate across all other dependent infrastructures. As a result, they cannot function properly. For example, loss of service from the power plant would directly affect the industry and manufacturing infrastructure. They rely heavily on the power plant for power in order to run pumping stations, control systems and for telecommunications.

A real-life example of such a failure was the Fukushima Daiichi nuclear disaster in Japan. Following a major earthquake, a 15-metre tsunami disabled the power supply and cooling of three Fukushima Daiichi reactors, causing a nuclear accident on 11 March 2011 [10]. All three cores largely melted in the first three days. Apart from cooling, the basic ongoing task was to prevent the release of radioactive materials, particularly in contaminated water leaked from the three units [11].

Three years after a triple meltdown, the Fukushima Daiichi nuclear power plant is faced with a flood of highly radioactive wastewater they are struggling to contain. Groundwater is pouring into the plant's reactor at a rate of almost 75 gallons a minute. This highly contaminated water is being pumped out to prevent it from swamping a critical cooling system.

This disaster highlights an example of a cascading failure. Although there were procedures in place for dealing with natural disaster, the scope of the interdependencies was not considered. There were local independencies in the form of reliant systems that could not provide service and affected the local economy, security, and environment. On a global scale, three years later the cascading problems have still not been resolved, and this has impacted industry and global trade, causing huge financial losses.

B. *Simulation*

As previously mentioned, it is clear that there are many benefits of using simulation. Notably, experimentation can be done on a realistic representation of a system without the worry that any damage done would have a real impact [12]. In particular, when testing against cyber-attack resilience and

developing new approaches to security, critical infrastructure simulation is of great benefit.

Modelling and simulation are components of ensuring the safe, reliable, and continuous operations of critical infrastructures. There are many factors to consider when evaluating the cascading effects caused by a failure. Many organisations and infrastructures have policies and procedures in place for dealing with random 'worst case' scenarios, but how do we determine if these are implemented in a time-efficient manner?

Currently, there are no satisfactory metrics today that would enable:

- Comparisons of mitigation, response, recovery, reconstitution, and restoration strategies.
- Comparisons of the criticality of nodes and links.
- Determination of appropriate investment strategies to increase security.
- Evaluation of the relative effectiveness of security measures and policies [13].

Development of a comprehensive and widely accepted set of metrics should be a component of the national critical infrastructure protection program. Simulation presents an ideal tool to evaluate and experiment with procedures to counter cascading failure. In the following section, a simulated virtual city is presented in order to evaluate the effects on emergency service provision in the case of a failure occurring in a connected infrastructure.

III. Simulation

The simulated city presented consists of eight infrastructures all interconnected by a network of cables and pipes, which are used for electricity, communication and water distribution. The infrastructures comprised in the construction include: a power plant, an industrial infrastructure, a telecommunications infrastructure, a water distribution plant, housing, a petrol station, an airport, and the emergency services. A road network links the emergency response with each of the other infrastructures.

A. Simulation Specification

Errors or anomalous behaviour in one infrastructure has direct impact on another. A component failure in our simulation allows the city to keep functioning, but the effects of the fault are visible in the dataset. The construction of the simulation is accomplished using the Siemens Technomatix Plant Simulation Tool [14]. The software is based on object-oriented modelling, where each component inserted is an individual object, which can be adjusted and used to construct data.

In this paper, the focus is on an evaluation of the emergency service response provision when a fault is introduced in one of the eight infrastructures. An analysis is presented of how the emergency services is affected as a result of a cascading fault occurring.

B. Simulation Overview

Figure 2 displays an overview of the whole system. Each infrastructure has a graphical icon to represent its function more clearly. The icons can also be expanded to detail their interconnectivity and the various components each uses to allow the system to operate.

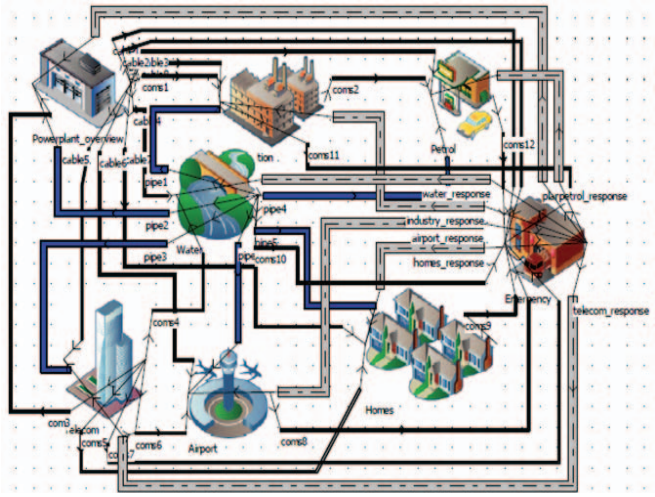

Fig 2. Simulation Overview

When linked together, the system functions, as shown in Figure 3. The individual blue blocks represent a visualisation of water flow. The yellow blocks represent units of energy generated by the power plant. The green blocks represent a communication between infrastructures. The communication may include a call for help to the emergency services. The vehicle icon represents emergency service vehicles.

The system functions smoothly and consistently. However, the output and behaviour differs slightly every time the system operates resulting in variance in the datasets.

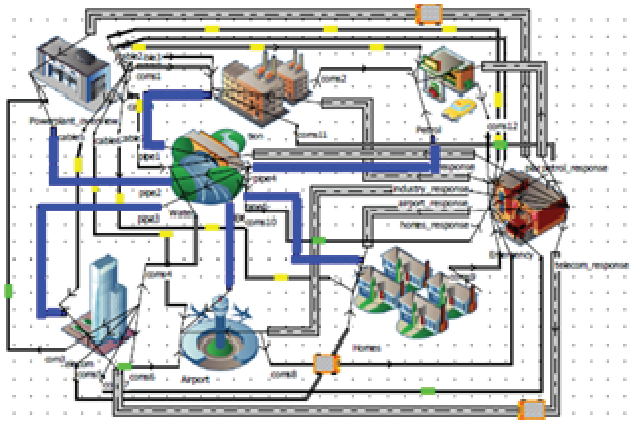

Fig. 3. Simulation Functioning

In the following section, an evaluation of a cascading fault is presented.

IV. Cascading Failure

A cascading failure is created in the simulation by causing targeted and random disruptions to a target infrastructure. In this paper, the employment of a failure to a server in the telecommunication infrastructure allows the

introduction of a fault, which has a cascading effect. The failure results in random communication blackouts during a 24-hour period. A knock-on effect is caused throughout the rest of the city as a result.

A. *Data Collection*

The effects of the failure are visualised and reflected in the dataset produced by each of the infrastructures. Two data sets are extracted from the emulation. One when the system is functioning normally, and one when the failure is implemented. The change in data is displayed in Table 1, which displays subtle changes in data as a result of the failure taking place. The data we extract is based on an evaluation of the emergency response.

TABLE I. DATA SAMPLE

Normal	Abnormal
0.8122	0.6606
4.0353	3.7116
0.8225	0.4773
5.1003	3.3735
0.8122	0.6606
4.0353	3.7116
0.8225	0.4773
5.1003	3.3735

The data displayed in Table 1 shows one feature extracted from the dataset generated by the petrol station. The extracted from the dataset include aspects, such as, mean unit response time and number of calls for assistance recorded. In total, the behaviour analysis process is implemented using eighteen features extracted from seven infrastructures for both normal and abnormal data. The dataset used is constructed over a 48-hour simulation time. Two days of normal and abnormal behaviour data are collected.

B. *Data Behaviour*

The difference between normal behaviour and cascading behaviour, displayed in Table 1 is demonstrated in Figure 4. The blue circles represent normal data, and the red blocks represent abnormal.

Changes in behaviour, as a result of a system failure, can often be subtle and hard to identify. For that reason, data classification is essential. Identifying these variations in behaviour and subtle changes in patterns of activity to evaluate the effects of a cascading failure is presented in the following section.

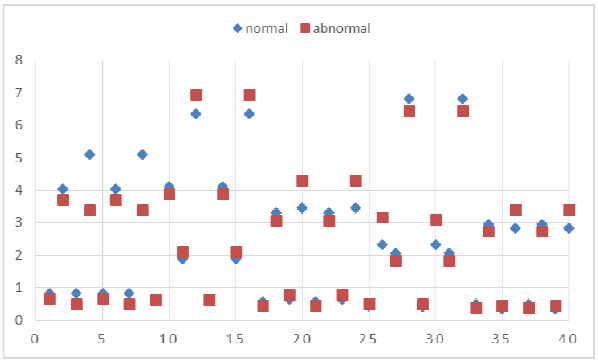

Fig. 4 Behaviour Analysis

As Figure 4 displays, changes in behaviour as a result of cascading failures can be subtle but signification. A change in the timing of the emergency unit response, as a result of an inability to communicate, may mean the difference between life and death.

V. RESULTS AND DISCUSSION

In order to demonstrate the significance of the cascading effects, a classification process displays the extent of the subtle changes in behaviour. In the case of emergency service response, the effects of a cascading fault may be apparent. However, having the ability to identify more subtle results of a cascading effect may allow for the planning and mitigation for responding to cascading effects in a real city.

Having the ability to evaluate subtle changes in behaviour allows for evaluating how a fault in one infrastructure may affect critical aspects of another.

A. *Data Classification Approach*

The evaluation process discussed in this paper uses supervised learning. Supervised learning involves giving the classification algorithms the 'right answer' to enable them to operate self-sufficiently. By using this method, we are able to train the classifiers using features, extracted from the dataset to identify when anomalous behaviour has occurred.

The approach involves specific data classification techniques, including: Uncorrelated Normal Density based Classifier (UDC), Quadratic Discriminant Classifier (QDC), Linear Discriminant Classifier (LDC), Polynomial Classifier (PLOYC), k-Nearest Neighbour (KNNC), Decision Tree (TREEC), Parzen Classifier (PARZENC), Support Vector Classifier (SVC) and Naïve Bayes Classifier (NAIVEBC) [15–17].

Each of these classifiers were chosen because they have the ability to learn how to recognise abnormal values in a dataset. They also employ a supervised learning approach, which is a key part of the approach. In the following subsection, the classification evaluation techniques are presented. Each of the techniques provides an assessment of the classifiers' success or failure when classifying the data.

B. *Classification Results*

The overall classification process is implemented using eighteen features with two classes. Two classes both for

normal and abnormal behaviour. The data collection period is conducted data over a four day period. Two days running the system as normal and two days where a fault is taking place.

Classifying the feature sets allowed for the identification how subtle failures in one infrastructure rippled and resulted in a change in behaviour in another in the simulated city. The results from the nine classifiers are presented in Table 2.

TABLE II. CLASSIFICATION RESULTS

Classifier	Error
LDC	0.5
UDC	0.5714
QDC	0.4286
PolyC	0.5
ParzenC	0.5714
TreeC	0.1429
SVC	0.3571
Naivebc	0.2857
KNNC	0.5714

The table displays the error level in the data classification. The lower the value the more successful the classifier was able to identify changes in behaviour. For example, LDC analysis can identify 50% (0.5) of the data accurate. Whereas, QDC can classify 58.14% (0.4286) accurately.

The three most success classifiers include TreeC, which is able to accurately classify 85.61% (0.1429) of the data, SVC which is able to classify 64.29% (0.3571) of the data and Naivebc, which is able to identify 71.43% (0.2857) of the data accurately.

The results show that, whilst some of the changes in behaviour are subtle, they can be detected.

C. *Results Visualisation*

A visualisation of the results is presented in this section. Each diagram represents a sample of the outcomes and provides a visual demonstration of how the classifiers function. In each figure, the division of data into two groups for normal and abnormal behaviour is displayed.

Figure 5 displays a graph of the Naivebc classification for two of the eighteen features. The ellipses, displayed, refer to likelihood contours, where the points inside the ellipse are most likely to belong to that grouping. The blue ellipses consist of data that comes from the normal behaviour dataset and the red referring to threat behaviour data. Threat behaviour can be identified as a result of one grouping clearly standing out from the other.

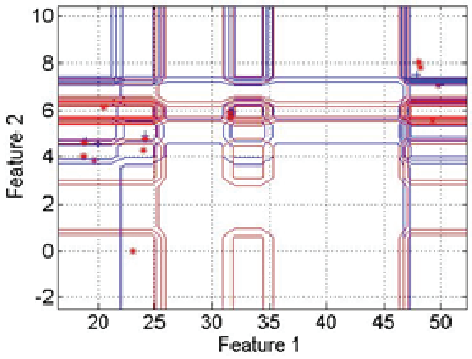

Fig. 5 Naivebc Visualisation

Feature 1, on the x-axis, refers to one of the dominant features and Feature 2, on the y-axis, refers to one of the lesser dominant features from the dataset. Two features were used in each visual representation to demonstrate how the classifiers function. The graph displays that some changes in behaviour can be identified but often some are subtle and difficult to identify. Similarly, to Figure 5, Figure 5 displays a graph of the Parzenc classification process.

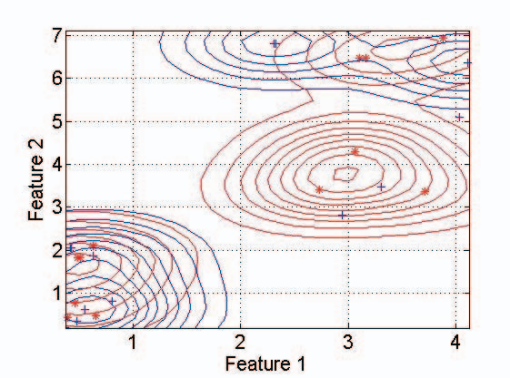

Fig. 6 Parzenc Visualisation

As before, the blue ellipses represent normal behaviour groupings. The effects of a cascading effect on the emergency service provision, are again represented by the red ellipses.

D. *Results Discussion*

The results demonstrate how behavioural patterns can be analysed to identify system changes in one infrastructure as a result of fault in another. The outcomes of the classification process act as a demonstration of how a cascading effect can be identified on an infrastructure which is not directly connected to the infrastructure where the fault originated. Using behaviour classification techniques, the effect on the emergency service provision is highlighted.

This evaluation process is intended to present how infrastructures, which are seemingly separate, heavily rely on each other for an effective service provision. The results also

display how the visualisation of the cascading failure visible in our simulated city can be mathematically demonstrated.

VI. Conclusion and Future Work

A simulated city depicting the interconnectivity of eight critical infrastructures is presented in this paper. The aim of this research is to highlight an innovative approach for organisations and government institutions to visualise cascading failure through simulation and plan for resilience.

Our behavioural analysis of this simulation allows for the identification of subtle changes in other infrastructures as a result of a failure cascading. This approach will be built upon in our future work through a real case study and visualisation of Liverpool (UK). We will demonstrate how behavioural analysis techniques can be used to evaluate the effects of cascading failure in a real city environment.

Satisfying such a criterion requires a sampling algorithm to be capable of controlling its sampling rate to provide sufficient accuracy at a minimal overhead. However, detecting low and high-volume threats and attacks requires the development of different algorithms. Adaptive threshold algorithms are suitable for this approach; however, in particular, the use of cumulative sum (CUSUM) has a better detection rate.

In particular, an alarm is signalled when the accumulated volume of measurements gn up to some time n that are above some traffic threshold exceeds an aggregate volume threshold h. As with the adaptive threshold algorithm, the traffic threshold is given by $(\alpha + 1)\ \mu$, where μ is the measured mean rate. Unlike the adaptive threshold algorithm, which considers only violations of the threshold, the CUSUM algorithm considers the excess volume sent above the normal volume, hence accounts for the intensity of the violations.

References

[1] M. Chander, "Protection of National Critical Infrastructure," Defence and Security Alert, pp. 54–58, 2013.

[2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control Sysem Magazine, vol. 21, no. 6, pp. 11–25, 2001.

[3] Department of Homeland Security, "CIPR Month 2012," Homeland Security, 2012. [Online]. Available: http://www.dhs.gov/cipr-month-2012. [Accessed: 03-Jan-2013].

[4] A. Miller, "Trends in Process Control Systems Security," IEEE Security & Privacy., vol. 3, no. 5, pp. 57–60, Sep. 2005.

[5] Department of Homeland Security, "National Infrastructure Protection Plan," 2006.

[6] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," Energy Policy, vol. 39, no. 10, pp. 6100–6119, Oct. 2011.

[7] Á. MacDermott, Q. Shi, M. Merabti, and K. Kifiyat, "Considering an elastic scaling model for cloud security," in The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), 2013.

[8] Á. MacDermott, Q. Shi, M. Merabti, and K. Kifayat, "Intrusion Detection for Critical Infrastructure Protection," in 13th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PGNet 2012), 2012.

[9] W. Hurst, M. Merabti, and P. Fergus, "Behavioural analysis for critical infrastructure security support," in The 7th European Modelling Symposium (EMS 2013), 2013.

[10] M. Fackler, "Flow of Tainted Water Is Latest Crisis at Japan Nuclear Plant," New York Times, 2013. [Online]. Available: http://www.nytimes.com/2013/04/30/world/asia/radioactive-water-imperils-fukushima-plant.html?pagewanted=1&_r=1.

[11] World Nuclear Association, "Fukushima Accident," World Nuclear Association, 2014. [Online]. Available: http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident/.

[12] C. Davis and J. Tate, "SCADA cyber security testbed development," Proceedings of the 38th North American power symposium (NAPS 2006), pp. 483-488., 2006.

[13] S. M. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies," in Proceedings of the 37th Hawaii International Conference on System Sciences, 2004, vol. 00, no. C, pp. 1–8.

[14] Siemens, "Tecnomatix Plant Simulation," Siemens Industry Software Limited., 2013. [Online]. Available: http://www.plm.automation.siemens.com/en_gb/products/tecnomatix/plant_design/plant_simulation.shtml.

[15] P. Fergus, P. Cheung, A. Hussain, D. Al-Jumeily, C. Dobbins, and S. Iram, "Prediction of Preterm Deliveries from EHG Signals Using Machine Learning," PLoS One, vol. 8, no. 10, p. e77154, 2013.

[16] Addinsoft, "Running a Principal Component Analysis (PCA) with XLSTAT," Statistics package for Excel - XLSTAT, 2013. [Online]. Available: http://www.xlstat.com/en/learning-center/tutorials/running-a-principal-component-analysis-pca-with-xlstat.html.

[17] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques," Informatica, vol. 31, no. 249–268, 2007.