A case study in Critical Infrastructure Interdependency[1]

Authors
Bernhard Schneidhofer, MSc (ISG, Royal Holloway, 2015)
Stephen Wolthusen, ISG, Royal Holloway

Overview

Critical Infrastructures such as electricity grids and water distribution systems provide services that are vital for the correct functioning of countries and modern societies. Their protection from cyber-attacks requires extensive efforts from governments, security practitioners, and security researchers.

In this article we provide a short introduction into the topic of Critical Infrastructure Protection and an overview of a case study that examines regional Critical Infrastructures. We also detail the findings of the case study and the security vulnerabilities discovered during the investigation.

Case Study – Introduction

The majority of research publications in the area of Critical Infrastructure Protection are focused on abstract modelling and simulation efforts. One notable side effect is the large number of proposed models and methodologies contrasted with a comparably small number of publications dedicated to validating or even applying these in the field. Most research papers on the subject limit themselves to only including small case studies with academic test cases. For this project we tried to take a different approach and subject a real-world environment to detailed analysis in order to identify security vulnerabilities and possible attack targets.

A region in Austria with an area of 1850 square kilometres has been chosen as the target area and will serve as the case. The case study at hand aimed to examine the selected target area, analysing the various critical infrastructure sectors and facilities in the target area, and based on this to identify security vulnerabilities as well as cyber-attack scenarios. In order to take a realistic approach from an attacker's point of view, the investigation and modelling was limited to open source information. The underlying research hypothesis was that it is possible for an outside attacker with limited resources to choose suitable critical infrastructure targets in the target area for an attack and, with the help of a simulation model, to develop viable attack strategies with the goal of severely degrading the operation of those targets.

[1] This article is to be published online by Computer Weekly as part of the 2016 Royal Holloway information security thesis series. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full MSc thesis is published on the ISG's website.

The importance of Critical Infrastructure Protection

Critical Infrastructure Protection is concerned with the security of all services and infrastructure systems vital for the smooth functioning of entire nations. Modern industrialised societies have a nearly absolute dependence on the permanent and reliable availability of services such as electricity and telecommunications. Every disruption or unavailability of any of these services for a long time can lead to high financial losses or damage public safety. The providers for these services are called (national) critical infrastructures. There exists no simple textbook definition to clearly identify a system as a critical infrastructure, and each country makes its own choice as to which systems are sufficiently important to be seen as critical infrastructures. All such classifications, however, include power grids, water supply systems, and telecommunication infrastructures.

UK - Critical Infrastructure sectors

- Energy
- Water
- Communications
- Government
- Emergency services
- Transport
- Financial services
- Healthcare
- Food

Critical infrastructures are rarely able to operate as a stand-alone system; their effective function frequently depends on services provided by other critical infrastructures. A helpful mental image is that of a city with electricity, water, and telecommunications infrastructure. Power plants in the electricity sector require a steady supply of water and reliable information infrastructure to work properly for regulating grid frequency. The water supply system requires electricity and a working telecommunications infrastructure to distribute and process water, and the telecommunication sector in turn requires electricity to function. In a similar fashion, critical infrastructures form complex webs of services and dependencies within and across countries. As a direct consequence, an attack or service interruption on a single critical infrastructure sector may result in cascading faults across multiple sectors.

Underlying Information Infrastructures

Most modern critical infrastructures have come to rely on extensive computer and communications network systems for their effective operation and are automated in such a way that manual operation is difficult. The main task of these computer systems is the supervision and control of industrial and physical processes, ranging from feed stock temperature control in the manufacturing of pharmaceutical products to operating generator sets in power stations. These specialised systems and networks are commonly summarised under the designation of Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS).

The traditional approach to security in SCADA and industrial network environments focused on physical security and strong separation from external networks. This concept is known as “Air Gap Security”, and it aims to physically separate the control system from any other system to ensure secure operation. However, the appearance of modern business operations has made this a largely theoretical concept as it is frequently necessary to bypass these gaps with firewalls and communication bridges. As a result, the security posture of ICS is frequently somewhat dire. Figure 1 shows an exemplary SCADA network with originally isolated control networks that had to be connected to a supervisory network in order to gather business information.

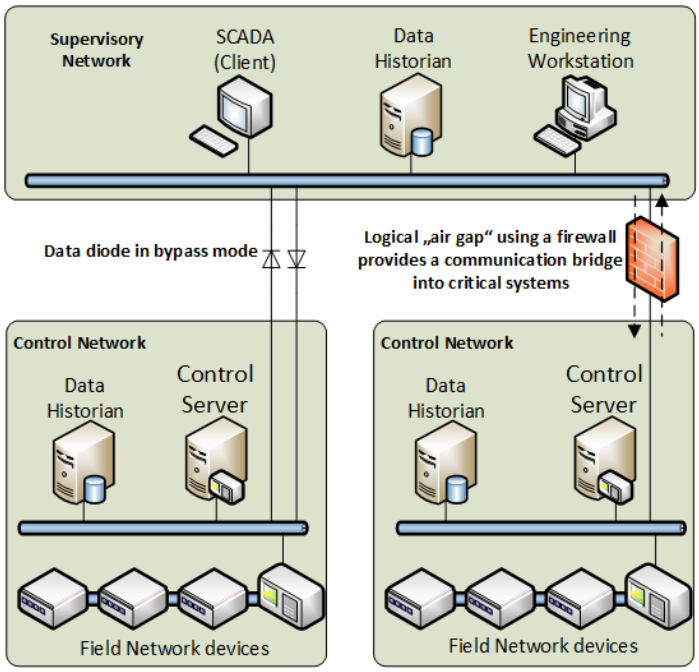

Figure 1 - Example of an actual "air-gapped" security environment

Modern industrial networks consist of standardized components but are still purpose-built and highly adapted to their individual industry and environment. Compared to conventional IT systems, the main goals in such industrial network and control system environments are real-time communication and reliability. Other aspects of Information Security such as message authentication (for both authentication and integrity protection) or encryption (for confidentiality) are considered not to be of critical importance, and are mostly overlooked.

Industrial network protocol flaws

- Lack of authentication
- Lack of encryption
- All connected devices receive all messages
- Protocols are designed to program end-devices

Consequently, from an attacker's point of view the main obstacle is to get access to the control network portion of an industrial network environment. As soon as a way to the ICS networks and field bus systems can be secured, it is generally trivial to disturb regular operations or damage vital systems.

Analysis of Critical Infrastructures

The sensitive nature of critical infrastructures makes it very difficult and rather unethical to perform any actual experiments on live systems. Any interference with live systems would potentially result in damages or dangers to life and limb. As a consequence, the analysis of critical infrastructures makes extensive use of computer simulation and models based on expert knowledge instead.

For the case study at hand, the modelling task required extensive data gathering from a wide variety of openly available sources. The main data sources are a geographical information system of the target area, a field study conducted on the power grid and power plants in the area, and system data published by the local power and water distributors. The resulting graph model includes the electricity, water, and telecommunications sectors in the target area. It consists of 1241 nodes, each representing distinct electricity or water sector facilities, and 1800 dependency relations between these nodes. The electricity model nodes mainly represent substations and wind turbines, whereas the water model nodes represent wells, water pressure stations, and water purification facilities. Figure 2 shows a portion of the graph model for the electricity grid and water supply system with their dependency connections.

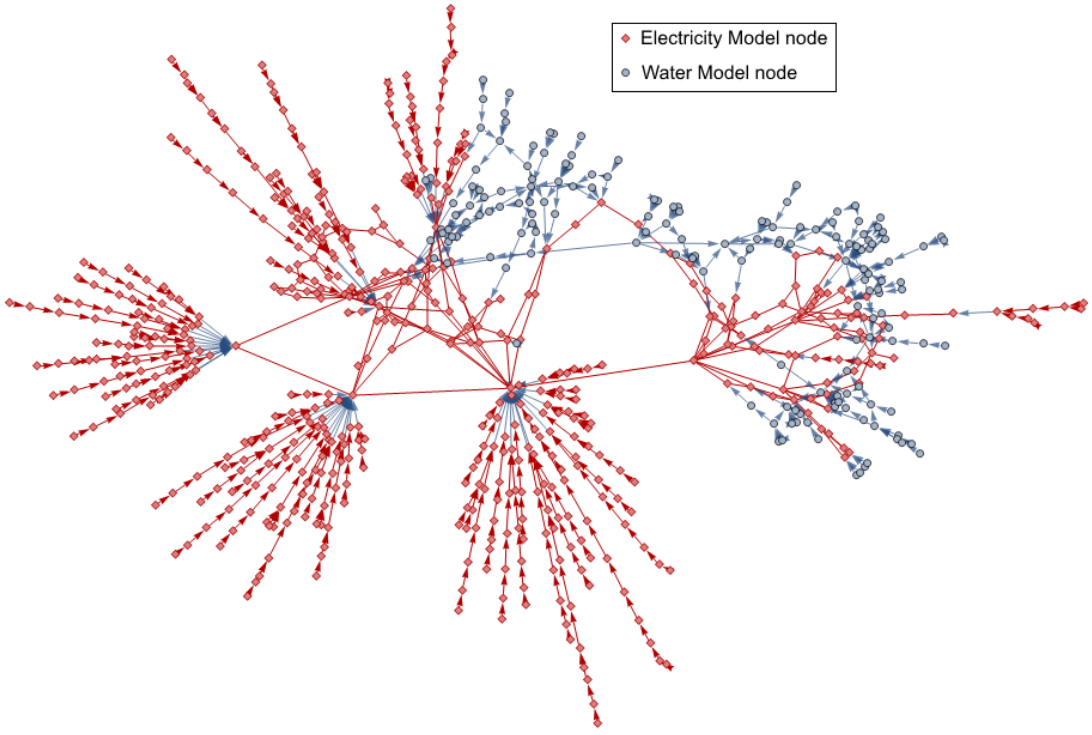

Figure 2 - Graph model of power sector and water sector

The static graph model has been augmented with dynamic code in order to simulate electricity supply and demand, water supply and demand, and telecommunication capabilities and dynamic changes to their behaviour and availability.

Case Study – Results

We note that all security issues identified as part of this case study have been reported to the corresponding operator companies by the authors and have already been corrected; consent was also sought from operators and authorities prior to publication.

Global Vulnerability Analysis

In order to get an impression of the vulnerabilities and overall robustness of the model, random node removal has been simulated. When 20% of the components of the water sector model have been removed, approximately 33% of the consumers have lost water supply. When 20% of the nodes of the electricity sector model have been removed, approximately 24% of the consumers have lost power supply. From a vulnerability point of view, it can therefore be argued that the electricity system is more robust against failures than the water system, but that to obtain a significant impact requires large parts of the network to fail randomly; this matches earlier results on robustness to random failures in complex networks.

Figure 3 illustrates the dependency relation between the electricity sector and the water sector. The consequence metric is again the number of households losing water or power supply, respectively. It can be seen that random node removal in the electricity sector also results in consequences in the water sector, thus the water sector clearly depends on electricity for its operation while the power sector is not directly dependent on the water supply. An attacker should therefore be able to cause more potential damage by targeting the electricity sector than targeting the water sector.

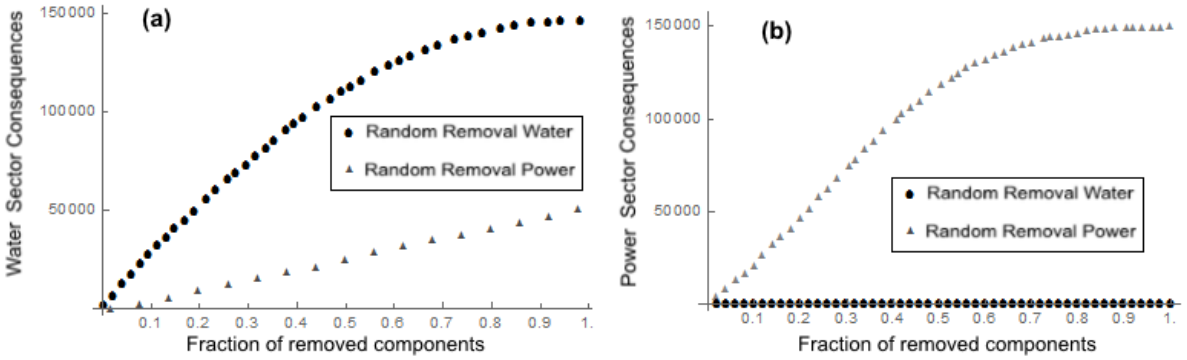

Figure 3 - Random node removal consequences in water sector and power sector

Critical Node Analysis

From an attacker's point of view, after learning about the general characteristics of the overall system it will be useful to identify the weakest links in the system and possible effects that enable efficient and effective attack scenarios. The Critical Node Analysis provides some insight in this area. The full computation of all possible failure scenario permutations in the model was not a viable option for computational complexity reasons. As an alternative, about 700,000 simulations for dual simultaneous node failure on all node subsets with length two have been carried out.

Table 1 lists the top ten calculated scenarios involving two simultaneous failures in the electricity sector and/or water sector. The figures in the "Consequences" columns denote the number of people without power or water supply. The dual failure scenarios are dominated by the failure of the substation 2721, which supplies electricity to a number of nearby cities and enables a number of possible further scenarios with greater resulting consequences, in combination with other single node failure scenario nodes. Only a single scenario at rank 4 is limited to a single sector; all of the other scenarios take advantage of dependencies between the electricity and water sectors. Around 75% of all computed dual failure scenarios have only consequences in a single sector and roughly 12% of all scenarios end without any consequences for water or electricity supply.

Rank	System {Component}	Consequences Power + Water	Total Consequences
1	Power {2721} ; Power {2742}	18512 + 7269	25781
2	Power {2721} ; Power {2738}	17623 + 6293	23916
3	Power {2721} ; Water {3735}	14787 + 8964	23751
4	Power {2721} ; Power {2744}	23610 + 0	23610
5	Power {2721} ; Power {2835}	14787 + 8759	23546
6	Power {2721} ; Water {3743}	14787 + 8759	23546
7	Power {2721} ; Water {3824}	14787 + 8759	23546
8	Power {2738} ; Water {3825}	2836 + 19885	22721
9	Power {2738} ; Water {3736}	2836 + 17623	20459
10	Power {2738} ; Water {3907}	2836 + 17623	20459

Table 1: Top Ten subsets of critical components for two simultaneous failures - Water/Power Supply

Identified Security Vulnerabilities

Based on the analytical findings outlined above, it was possible to develop a number of attack scenarios on the critical infrastructures in the target area. Investigation into these scenarios identified several security vulnerabilities that would provide an attacker with easy access to the control networks of wind turbine power plants and subsequently the SCADA centres and systems of the electricity distributors.

- **VPN and Remote-Dial-In**
  Several wind turbine systems operate with backup telecommunication access via vulnerable VPN solutions over ISDN and leased lines.

- **Maintenance and Control Panels**
  In some instances the standard set-up for a wind turbine facility has been altered with external control boards. The employed display cases were easily accessible at ground level and would make it simple to provide backdoor access.

- **Webcams and Video Surveillance**
  Several wind turbines in the target area have been equipped with network cameras on top of their towers and entrance area video surveillance cameras. In a few limited cases the cameras were connected to control networks and the cameras' administrative web interfaces were directly available on the Internet via public IP addresses. Access to the administration interfaces was secured by simple password authentication vulnerable to brute-force attacks.

- **SCADA Centre**
  If access to the control network can be gained, it is also feasible to target systems on a higher level and attack targets from the supervisory network portion, which may influence a much larger number of facilities in the electricity distributors network.

- **Safety Policies**
  A regulatory requirement was identified, which has a profound impact on operating requirements for wind turbines. For protection against ice shedding, it is insufficient to shut down a single affected wind turbine as adjacent turbines may also suffer from icing. As a result, safety regulations require a forced shutdown command enabling control systems to broadcast an emergency shutdown command to turbines in the surrounding area. Restarting affected turbines requires manual intervention by a technician and consequently a considerable amount of time. If physical access to the control network can be gained, a shutdown message could be forged and sent by an adversary with minimal effort. The security measures in place to prevent such an attack were limited to a specific message format and a basic message checksum.

Conclusion

In this article we provided a compact introduction to the topic of Critical Infrastructure Protection and presented a short overview of the findings of our case study investigating the security situation of regional critical infrastructures.

For our case study we were able to gather enough openly available information to construct a model for analysis and simulation purposes. The resulting model has been subjected to global vulnerability analysis in order to assess the overall robustness of the infrastructures and to critical node analysis with the goal of identifying the best attack targets. Apart from the identification of the more vulnerable critical infrastructure parts in the target area, the findings of the case study include a number of interesting vulnerabilities in various infrastructure sectors. Among those are a few notable vulnerabilities that would have enabled access to the control networks of wind farms and substations.

All steps in the development and analysis of the model and attack scenarios were solely based on information that is available to the general public (although in some cases not over the Internet), strongly suggesting that an attacker even with very modest resources would be able to achieve large-scale effects.

Biographies

Bernhard Schneidhofer completed his Dipl.-Ing. degree in Information Management at FH-Joanneum Graz in 2008. He worked as an independent IT consultant in Austria from 2008-2011 and as a Technical Manager for Hesticare B.V. in the Netherlands from 2011-2013. He graduated in 2015 from Royal Holloway, University of London with an MSc in Information Security and received the David Lindsay prize from the British Computing Society for his thesis.

Dr Stephen Wolthusen received his Dipl.-Inform. degree in computer science in 1999 and completed his Ph.D. in theoretical computer science in 2003, both at TU Darmstadt. He was with the Security Technology Department at Fraunhofer-IGD from 1999-2005, serving as deputy division chief from 2003 onwards and as senior visiting scientist from 2005 onwards. He is currently a Reader in Mathematics with the ISG, and also Full Professor of Information Security (part-time) at the Norwegian University of Science and Technology, Norway. His research focuses on models of adversaries and resilient networks, with applications in defence networks and particularly in critical infrastructure networks and control systems security. He has led a number of national and European projects, including the Internet of Energy project. He is author and editor of several books, as well as over 130 peer-reviewed publications. He has served as editor-in-chief of *Computers and Security* and as vice-chair of the IEEE Task Force on Information Assurance, and is currently vice-chair of the IEEE Task Force on Network Science.