"Water, Water, Every Where": Nuances for a Water Industry Critical Infrastructure Specification Exemplar

Shamal Faily[1], George Stergiopoulos[2], Vasilios Katos[1], and Dimitris Gritzalis[2]

[1] Bournemouth University, Poole, UK
{sfaily,vkatos}@bournemouth.ac.uk
[2] Athens University of Economics & Business, Athens, Greece
dgrit@aueb.gr

Abstract. The water infrastructure is critical to human life, but little attention has been paid to the nuances of the water industry. Without such attention, evaluating security innovation in this domain without compromising the productivity goals when delivering water services is difficult. This paper proposes four nuances that need to be incorporated into a representative specification exemplar for the water industry; these provided input to the exemplar based on a fictional water company.

1 Introduction

The water infrastructure is one infrastructure we cannot do without. Despite the citing of water industry vulnerabilities as a motivation for critical infrastructure protection [1], there has been little work considering the nuances of this sector. As such, it is implicitly assumed that addressing security issues in one form of critical infrastructure effectively addresses the issues in all others. There are, however, many reasons why this may not be the case.

Previous work like [2] proposed security innovation in the water industry, but is premised on scenarios associated with the distribution of clean water only. However, threats in the quality of water distribution have also been identified due to loss of pressurised water, aging infrastructure, as well as vulnerabilities in interdependent infrastructure [3,4,5]. While case studies provide a means of disseminating nuances to the broader research and practitioner communities,it would be useful to share such insights using a format suitable for evaluating new innovation by researchers, or products and services by practitioners.

Specification exemplars are self-contained, informal descriptions of a problem in some application domain, and are designed to capture the harshness of reality [6]. They are designed to advance a single research effort, promote research and understanding among multiple researchers, and contribute to the advancement of software development practice. They should exhibit the "messy" nature of the real-world, but such messiness is difficult to elicit without actual case study data; commercial confidentiality concerns often impede access to such data. Specification exemplars also focus on modelling functional concerns, but many nuances

related to human issues are not so easily modelled. For example, previous work has suggested that the tensions that exist between security and safety can be addressed by designing security that 'Homer Simpson' can use [7]. However, trivialising all critical infrastructure users in such a way fails to consider how their skills and expertise are brought to bear when solving difficult, but not unrealistic, operational challenges.

In this paper we propose four nuaunces that need to be incorporated into a representative specification exemplar for the water industry. We present these nuances in Section 2, and briefly summarise their implications in Section 3.

2 Water Industry Nuances

We examined the empirical data from two previous studies designing security for the water industry [8,9]; this data included 11 contextual interview transcripts, 4 facilitated workshop transcripts, and a variety of photographs taken during several site visits. Following this review of case study data, four types of nuances that need to be incorporated into a specification exemplar were identified.

2.1 Organisational Nuances

To many people, water companies are predominantly concerned with the supply of clean (drinking) water. However, in many cases, water companies are also concerned with the infrastructure associated with distributing and treating waste water as well. At first blush, waste water issues may not appear security critical, but there are obvious environmental implications if poorly treated water is inadvertently pumped into waterways. Similarly, accidental or deliberate harm to terminal pumping stations can pose a flooding risk to residential or commercial properties in the vicinity of waste water treatment plants, together with the health risks that this entails.

Like many other firms, water companies are also under pressure to save money and reduce energy consumption. As a result, water companies carry out internal projects to optimise equipment in order to reduce energy consumption. However, there can be tensions because the drive to save energy and money might lead to elaborate and unpredictable changes to process operations. If not carefully managed, such changes might lead to human error if changes made by technicians are complex, or violations in order to save time or achieve goals deemed more important than security. Such errors and violations can be source of latent failures which, over time, can contribute to catastrophic failures [10].

2.2 Operational Nuances

A water company depends on the skills and expertise of the people that run it. The operations and goals associated with plant operators and technicians can vary based on a variety of contextual conditions such as geographical locale, time of day, or even the season of the year; these conditions may truncate or

extend activities, and practices are shaped around these different conditions. For example, plant operators may be called away to fix problems around a site depending on the availability of other staff and, depending on the site, may be required to carry out remedial activities associated with other roles, such as taking water samples to check agreed water quality criteria are met.

The use of technology for what appears to be innocuous physical artifacts is also shaped to satisfy operational requirements in such a way that they become key assets. While not normally considered a critical device, TVs in control rooms are often used to check weather reports to determine whether it was necessary to pump water from reservoirs to treatment sites. Security practices are also shaped around operational needs as well with default account logout times sometimes timed to correspond with shift hours, and information – ranging from contact phone numbers to Chlorine levels – is often written on whiteboards in control rooms; these whiteboards act as the collective memory for plant staff. Consequently, such settings can be modified without it being obvious who might have made the changes, and how warranted they might be.

2.3 Environmental Nuances

Unlike electricity, water cannot simply be turned off. A water company's infrastructure might support a large geographical region, with water pumped over 40 miles to the plant that treats it; this necessitates a large estate of supporting infrastructure to control water flow, and satisfy agreed water quality standards. After a prolonged period of hot weather, settlement can build up in the waste water distribution system; if the weather suddenly changes, this settlement can hit the treatment works at once and, if flow is obstructed, can lead to downstream flooding. The quality of water can also change in less than an hour due to weather conditions, and quality can be further exacerbated by accidents such as oil tanker spills. Automated monitoring plays an important role in monitoring clean or waste water quality, but so does human intervention and the ability to spot changes that appear unusual. As Section 2.1 illustrates, undertaking these processes can become error prone depending on the precise context in which any intervention takes place.

2.4 Physical Security and Safety Nuances

As important as cybersecurity is, the most pressing concern faced by many stakeholders are day-to-day physical security and safety issues. These include threats associated with the theft of metal parts for scrap. The form such attacks can take are myriad, and include theft of gates and fencing, and the damage of associated infrastructure – such as power lines – to get at copper earth connectors. Petty theft is also a concern due to externalities that might be introduced as a result. For example, the value of a stolen PC is insignificant compared to the overall impact on the infrastructure that is no longer being monitored or maintained as a result. These physical security issues also have a personal impact on stakeholders like technicians and plant operators. Plant operators working alone

at night might be apprehensive about confronting a team of scrap metal thieves, particularly if the plant is located in a remote, countryside location. This impacts how they might choose to respond to an alarm, and how they might carry out any remedial action.

3 Conclusion

This paper has presented four nuances that need to be incorporated into a representative specification exemplar for the water industry. In analysing pre-existing case study material, we have identified several classes of nuance with the potential to impact security in water companies. This impact might result from the direct loss of a physical asset, or from latent failures resulting from excessive physical and mental effort by plant operators or technicians. A limitation of this work is that these nuance classes may be specific to the water domain. We are, however, currently analysing case study data within the rail sector to see if such nuance classes are applicable there. We developed a specification exemplar for a fictional water company that encapsulates the nuances described. Further details and an evaluation of this exemplar will be described in future work.

References

1. Slay, J., Miller, M.: Lessons learned from the maroochy water breach. In: IFIP series in Critical Infrastructure Protection. Springer (2007) 73–82
2. Eliades, D.G., Polycarpou, M.M.: Security of water infrastructure systems. In Setola, R., Geretshuber, S., eds.: Critical Information Infrastructure Security. Volume 5508 of Lecture Notes in Computer Science. Springer (2009) 360–367
3. Van Leuven, L.J.: Water/Wastewater Infrastructure Security: Threats and Vulnerabilities. In Clark, R.M., Hakim, S., Ostfeld, A., eds.: Handbook of Water and Wastewater Systems Protection. Springer (2011)
4. Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., Cruz, E.: The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports. Public Administration **89**(2) (2011) 381–400
5. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Assessing n-order dependencies between critical infrastructures. IJCIS **9**(1/2) (2013) 93–110
6. Feather, M.S., Fickas, S., Finkelstein, A., van Lamsweerde, A.: Requirements and specification exemplars. Automated Software Engineering **4**(4) (1997) 419–438
7. Anderson, R., Fuloria, S.: Security economics and critical national infrastructure. In Moore, T., Pym, D.J., Ioannidis, C., eds.: Economics of Information Security and Privacy. Springer (2010) 55–66
8. Faily, S., Fléchais, I.: Towards tool-support for Usable Secure Requirements Engineering with CAIRIS. International Journal of Secure Software Engineering **1**(3) (July-September 2010) 56–70
9. Faily, S., Fléchais, I.: User-centered information security policy development in a post-stuxnet world. In: Proceedings of the 6th International Conference on Availability, Reliability and Security. (2011) 716–721
10. Reason, J.: Human Error. Cambridge University Press (1990)