Application of Work Domain Analysis for Cybersecurity

Hao Wang[1], Nathan Lau[1(✉)], and Ryan Gerdes[2]

[1] Grado Department of Industrial and Systems Engineering, Virginia Tech, Blacksburg, VA, USA
{drkwh05, nathan.lau}@vt.edu
[2] Bradley Department of Electrical and Computer Engineering, Blacksburg, USA
rgerdes@vt.edu

Abstract. Cyber Physical Systems (CPSs) are pervasive in businesses and critical infrastructures that are becoming targets of cyber attack by our adversaries. The presence of advanced persistent threats or zero-day attacks suggests that cyber defense must include recovery response from cyber intrusions. Recovery response must rely on adaptive ability of the CPS as the impact of zero-day attacks cannot be anticipated. In unanticipated situations, human adaptive ability can contribute greatly to the recovery from cyber intrusions. This paper presents Work Domain Analysis (WDA) as a human factors engineering tool for evaluating system and identifying solutions supporting operators in their response to cyber threats. The cyber attack on Australian Maroochy Water Services is used as illustrative case study to demonstrate the potential of WDA in enhancing cyber security of CPS.

Keywords: Cyber-physical systems · Cyber security · Work domain analysis · Abstraction hierarchy · Maroochy water breach

1 Introduction

Cyber physical systems (CPSs) are becoming pervasive in our society. CPSs are "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical component" [1], in which embedded computer and network systems monitor and control physical processes [2, 3]. Computer or automated control of physical equipment and process through communication networks is going to be a fundamental aspect for all future systems [4, 5]. Even very small systems such as a family home are becoming "smart" with internet of things.

For today, many of the most significant CPSs still reside in critical infrastructures and heavy industries, such as electric power generation, sewage treatment, petrochemical refineries and steel mills. The systems for these industries and infrastructures are pioneers in computer control of equipment or physical process out of necessity for safety and productivity (e.g., extreme temperature in a steel mill). Further, virtually all of these CPSs critical to our society have a cyber or operational technology (OT) design around the Supervisory Control and Data Acquisition (SCADA) control system

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 384–395, 2017.
DOI: 10.1007/978-3-319-58460-7_27

architecture [6]. A SCADA system typically consists of supervisory computers, remote terminal units (RTUs) and programmable logic controllers (PLCs), human-machine interface, and a communication infrastructure [7]. The RTUs, preferred for wireless controls, and PLCs, preferred for wired controls, connect to sensors for collecting process information and actuators for controlling the equipment according to the instructions from the supervisory computers. The supervisory computers run software applications that process the sensor data, issue control commands and host the human-machine interface. Finally, the communication infrastructure connects the supervisory computers, PLCs and RTUs while providing an interface for human operators to oversee the physical process and exercise manual controls. Figure 1 depicts a simplified network for a typical SCADA system [8]. In essence, the functions of the SCADA system are essential for the operations of major industries and critical infrastructures.

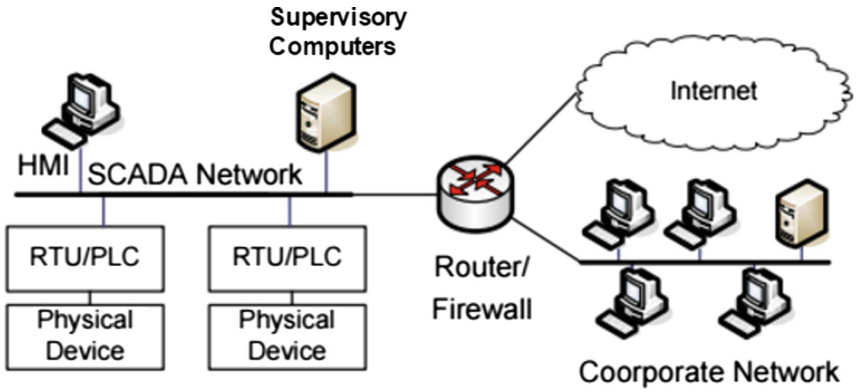

Fig. 1. A simplified SCADA network depicting PLCs, RTUs, supervisory computers, and human-machine interface.

While providing autonomous and complex functions in CPS, SCADA systems have also become the target of cyber attacks for effecting the physical systems. For example, Stuxnet is a malicious worm employing multiple zero-day exploits to penetrate traditional single detection mechanism [9, 10] and to infect PLCs for controlling industrial equipment. As discovered after being deployed to damage about 1,000 centrifuges in the Iran's nuclear program [11], Stuxnet was designed to access the SCADA components for physical sabotage rather than the traditional data theft or denial of service [12, 13]. Other infamous attacks on CPSs have resulted in severe social, economic, and political impacts, such as the 2015 Ukrainian Power Grid cyber attack causing power outages for over 225,000 customers [11].

Cyber attacks, such as Stuxnet, are classified as "Advanced Persistent Threat" (APT), which cannot be mitigated with traditional cyber security tools such as virus scans [14]. APT targeting major industries and critical infrastructures are mostly carried out by well-prepared, well-funded and well-trained adversaries. Current cyber security

solutions are mostly perimeter-based such as firewalls and authentication although research has expand to network traffic monitoring, vulnerability modeling, and cyber deception (e.g., honeynet) [15, 16]. Though essential to improve overall security of SCADA, these research, by definition, do not directly address zero-day attacks when intrusion already occurred. To cope with APT, security research must also investigate effective and efficient recovery from cyber intrusions.

Recovery from APT or zero-day attacks must rely on adaptive behaviors built into the CPSs. Human intelligence remains superior to computers or machines in responding to unanticipated events or handling ill-defined tasks [17]; thus operators can play a central role in recovering from cyber intrusions, particularly in formulating and executing mitigation plans [18, 19]. Human factors research has begun investigating how to aid operators in cyber defense. There was an organized panel to identify the human role in cyber defense across professionals from diverse domains [20]. Research has found high demands and low vigilance for cyber defenders, and efforts have been made to find strategies in supporting cyber defense performance [21]. Cognitive task analysis has been applied to evaluate cognitive demands and situation awareness of cyber analyst and team cognitions. Human performance evaluation has indicated that moderate-to-low team situation awareness could compromise cyber defense performance [22]. Despite increasing research focus on cyber security, the literature does not contain any publications on supporting and evaluating human adaptability for responding to APT and zero-day attacks.

Work domain analysis [17, 23] is a human factors engineering method for modeling complex systems to generate design requirements that can support operators in problem solving during unanticipated events which can be caused by APT and zero day attacks. Hence, we are investigating the potential applications of WDA for informing cyber system design that would aid operators and security personnel in recovering from cyber intrusions. In this paper, we review the WDA literature and then present a case study of applying WDA to examine the cyber attack on the Maroochy sewage treatment plant. The paper concludes with a discussion on how the WDA can be useful for system design evaluation and coordinate incidence response in the case study.

2 Work Domain Analysis

Work Domain Analysis (WDA) [17, 23] models the functional structure of the system for identifying domain invariants or constraints that workers and automated controllers must respect in order to achieve system goals [24]. By depicting the boundary conditions and relationships with respect to goals of the system, WDA stands in contrast to many other human factors analysis methods that focus on eliciting requirements from the user or inferring human limitations from science [25]. That is, WDA studies how system works and thereby informs design requirements for tools that help operators conceive possible actions or trajectories within such operational constraints of the system, thereby supporting adaptive behaviors during unanticipated events.

Abstraction hierarchy [26] is one of the major modeling tools for WDA [24]. The abstraction hierarchy is a knowledge representation framework characterized by structural means-ends links between levels (see Fig. 2) as each level describes the work

domain from a different perspective. Between adjacent levels, middle levels represent the structure of the work domain (what), while levels above explain the purpose (why) and levels below describe the means (how). In other words, the lower level represents the system elements to achieve the higher level ends, or what can operators use to accomplish a system function. The upper level describes the goals or functions that can be supported by lower level means, or why operators are provided with various system elements.

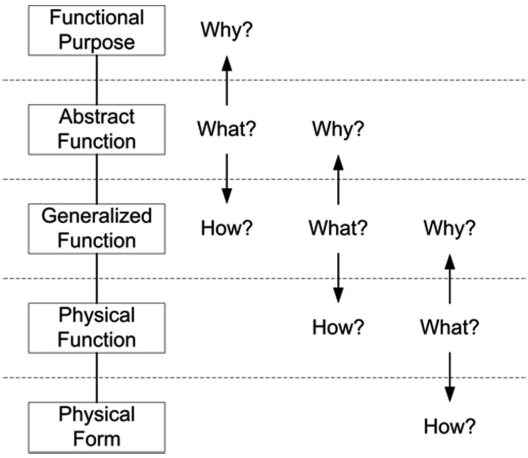

Fig. 2. Typical five-level abstraction hierarchy depicting why-what-how means-ends relationships

A typical abstraction hierarchy has five levels: Function purpose serves as the highest level which describes the primary purpose of the system. Abstract function is the second level which describes the scientific laws or disciplines applied to achieve the functional purpose. Generalized function is the third level which represents the engineering processes derived from applying the scientific laws. Physical functions is the forth level which depicts the physical equipment or components that realize the engineer processes. Physical forms is the lowest level which represents the physical appearance, condition, and location of the system equipment or components to indicate their operating states.

The abstraction hierarchy has demonstrated merits in modeling and supporting human problem solving in many safety critical domains, including algorithm development in computer science [27], automated trading system in finance [28], process control in nuclear power plants [29], flight control in civil aviation [30], and system acquisition in military [31]. Regarding nuclear power plants, WDA has been widely acknowledged as a valid and qualified technique in all stages of system design to accommodate human abilities and limitations [32]. However, the literature does not contain any applications of WDA for cyber security.

To investigate the application of WDA for cyber security, we completed two abstraction hierarchies for analyzing the cyber attack on a sewage treatment plant

(Maroochy Water Services) in Australia. This case study can illustrate whether WDA is a meaningful analysis tool for developing cyber security solutions.

3 Case Study: Australian Maroochy Water Services Cyber Attack

The cyber attack targeted the water sewerage system in Maroochy Shire Council which consists of 142 pumping stations that treats 35 million liters of wastewater per day [33]. All pumping stations are equipped with two-way radios systems to receive commands from and transmit information to the supervisory computers and the main control room. For safety, the Protective Distribution System (PDS) Compact 500 computer devices are installed at each pumping to issue alarms, communicate with main control room, as well as to start or terminate pump operations.

The Maroochy cyber attack occurred between February and April, 2000 during which pumps were not running when they should, alarms were not transmitted to industrial control system and main control room, and communication were lost between pumping stations and supervisory control computers. The initial troubleshooting involved monitoring and recording radio traffic as well as inspection of physical equipment. The troubleshooting indicated that a PDS Compact 500 computer of a particular identification was issuing corrupt electronic messages that led to erratic pump operations. The OT staff devised a workaround that all pumping stations would ignore commands from the PDS computer of that identification.

The workaround was short lived as a PDS computer with another identification began sending corrupted messages. In March, the attack involving remote access of a PDS computer altered the electronic signals and caused erratic pump operations. The OT staff was able to identify the bogus information but the intrusion was not stopped. The sewage facility resorted to mobilizing field workers to operate the pumps manually at a great cost. On one occasion, this costly workaround was deficient, resulting in 800,000 L of untreated sewage overflow, polluting over 500 m of open drain and creek and incurring significant financial losses for the cleanup [34].

Another intrusion occurred in late April resulting alarms being disabled on four pumping stations. At this time, a former contractor of an outsourcing company to the sewage company was under suspicion. This contractor was eventually arrested for the cyber attack with the possession of a PDS Compact 500 computer and a two-way radio set to frequencies of radio systems of the sewage facility. The attack was an act of revenge for failing to secure a job at the sewage facility [35]. Given his knowledge of the sewage facility as a former contractor, the attacker was considered an insider. He used the same radio equipment as the sewage facility to intervene the communication between pumping stations and supervisory computers in central control room. He stole the PDS Compact 500 computer to disable alarms and change pump configurations. Between February and late April, he intruded 46 times through the radio, disguising himself with different identifications.

3.1 Work Domain Model: The Abstraction Hierarchy

The Maroochy cyber attack highlights the physical damages that can incur as a result of deficient OT security. To study this cyber attack from a CPS perspective, we present and integrate two abstraction hierachies representing the physical and cyber/OT design of the sewage plant. Due to limited access to system documentations and restriction on publication lengths, the two work domain models are highly simplified representations of the plant's physical and cyber system. There can be many more elements for each levels of abstraction. However, the simplification should still be sufficient for the purpose of illustrating the application of WDA for system evaluation and coordinated incident response during cyber attacks.

Abstraction Hierarchy of Sewage Treatment Process. Modern sewage treatment plant is a CPS in which a series of complex physical processes to remove contaminants from water is controlled by a network of computers [36]. The abstraction hierarchy provides a multi-level representation of the sewage treatment process and thus can be applied to illustrate the physical impact of the Maroochy cyberattack. The top half of Fig. 3 (in yellow background) presents an abstraction hierarchy of a simplified sewage treatment plant that should be suffice to illustrate the general operations and impact of the cyber attack in Maroochy Shire. This abstraction hierarchy is based on the Australia and New Zealand 1997 guidelines for sewage systems that highlights six major processes – pre-treatment, primary treatment, secondary treatment, disinfection, sludge treatment, and advanced/tertiary wastewater treatment [37].

The abstraction hierarchy depicts that the functional purpose of sewage plant is to ensure sewage throughput and quality as well as environmental safety and public health. These purposes are achieved through the application of several abstract functions: mass transfer and fluid dynamics, conservation of energy, biochemistry balance, discharge and emission regulations. The means to achieve abstract functions are engineering processes at the generalized function level such as transport of liquid/gas and disinfection. For example, environment regulation and biochemistry balance can be fulfilled through disinfection of sewage materials. These engineering processes are realized through several major types of equipment in the physical functions level. Continuing on the means-end example, the disinfection process can be achieved through ultraviolet irradiator and chemicals. Finally, the states of these equipment are described in the physical form level to indicate how the equipment is functioning. For instance, the on/off state and radiation frequency would be indications of whether the UV irradiator is disinfecting wastewater.

Abstraction Hierarchy of OT for Sewage Treatment Plant. To represent the cyber design and impact of the Maroochy sewage plant, an abstraction hierarchy is developed for the OT as shown bottom of Fig. 3 (In reverse order of abstractions). The functional purpose of OT is to ensure efficient, effective, and secure equipment controls as well as personnel communication. Achieving security depends on fundamental principles of information integrity, confidentiality and availability in the abstract function level; whereas, effective and efficient equipment control depends on control theory as well as information availability. Adhering to these fundamental principles requires information transmission, computation and security process to be in place. For example, information

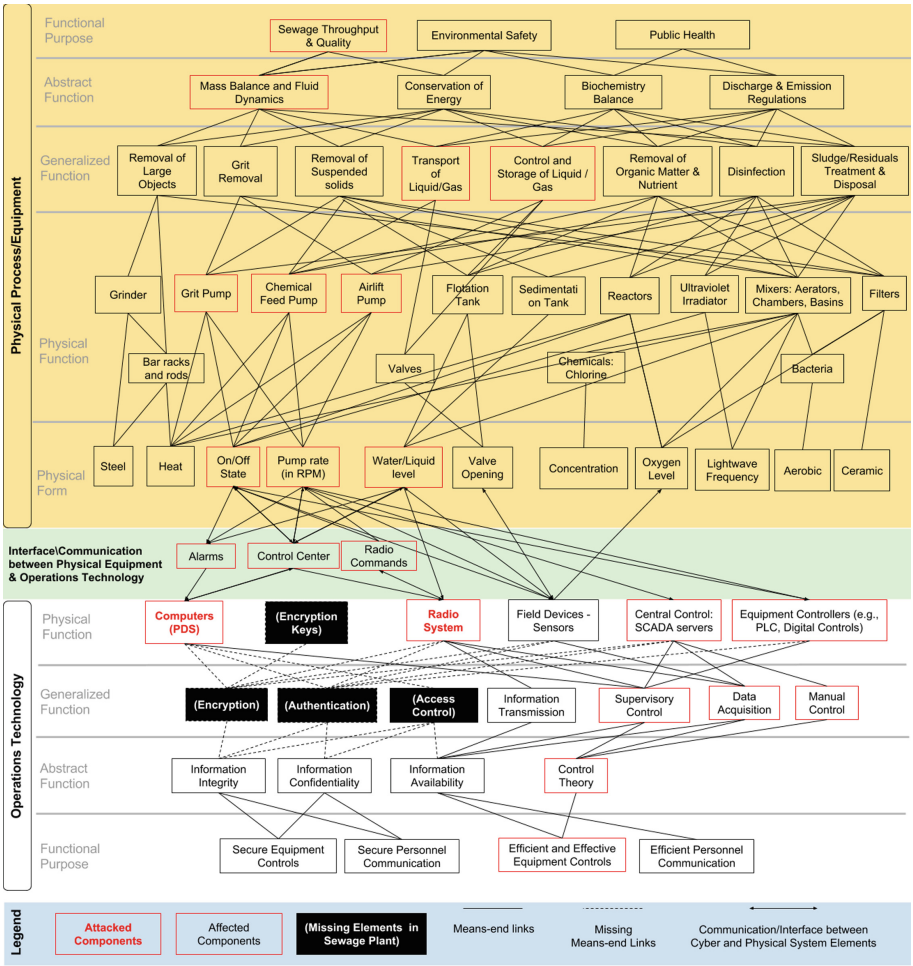

Fig. 3. Abstraction hierarchies representing physical process of a simplified sewage plant (top in yellow background), and corresponding operational technology (bottom in white background). (Color figure online)

integrity and confidentiality are commonly achieved through encryption, authentication and access control. However, the Maroochy sewage plant was lacking in these security processes/protocols. In other words, there are no means to information integrity and confidentiality. The abstraction hierarchy of Fig. 3 denotes missing elements in the Maroochy plant using white texts in parenthesis and black boxes, and missing means-end relationships using dashed lines. On the other hand, the Maroochy sewage plant was able to adhere to control theory through supervisory control, data acquisition and information transmission. These engineering processes are enabled by OT hardware and software. For example, encryption are enabled by computers generating encryption keys and performing decryption. Given the lack of encryption protocol, encryption keys

did not exist in the Maroochy OT system. Supervisor control and data acquisition of Maroochy plant was achieved through the SCADA server, equipment controllers and radio transmission system. The physical function level of the OT abstraction hierarchy is omitted because the additional level of details (e.g., packet size) are not necessary to illustrate the merits of WDA for cyber security.

Integrating the Abstraction Hierarchy and Mapping the Cyber Attack. The integration of the abstraction hierarchies for physical and cyber design of Maroochy sewage plant is represented by the interface of OT controllers and sensors with physical states of the equipment as highlighted with green background and arrowed lines in Fig. 3 That is, an OT component can communicate and thus impact the physical state of the process that in turns propagate upwards in the abstraction hierarchy to alter the equipment operations (physical function) which together in turns effect various engineering processes (generalized function). The engineering processes reflect whether scientific principles (abstraction function) are satisfied to achieve system goals (functional purpose). For example, the PDS computers can issue commands to stop pumps when water/liquid level becomes too low or high. Such commands may eventually impact other pumping operations with grit pump, chemical feed pump, airlift pump and thereby affect multiple generalized functions, namely transport of liquid/gas, removal of organic matter & nutrient, disinfection, and sludge/residual treatment and disposal in the generalized function level.

The integration of physical and cyber abstraction hierarchies provides a system map to study the Maroochy cyber attack. The attacker began the intrusion by using a system computer to access the plant control systems wirelessly using the same radio equipment and frequency as depicted with the red boxes with red texts in Fig. 3. Once intruded, the attacker issued radio commands to equipment controllers to cause erratic pump behaviors, affecting transport, control and storage of liquid/gas resulting in mass imbalance for the plant. At the same time, the attacker also used PDS computer and software to access the SCADA system, disabling alarms and overriding messages from or to the control center/room. This intrusion thus propagated upwards in the OT abstraction hierarchy to affect supervisory control, acquisition and manual control, thereby breaking process control fundamentals for the sewage treatment and thus the goal of effective equipment control.

3.2 Work Domain Model in System Evaluation and Design

The Maroochy cyber attack case study illustrates that the abstraction hierarchy can be useful to assess cyber security of CPS and thereby inform system design. Referring the abstraction hierarchy for OT or cyber system design, encryption and authentication are important processes to ensure information integrity and confidentiality. However, none appeared to be implemented for computer devices or wireless system at Maroochy sewage treatment plant, permitting attacker to intrude through the radios and access the SCADA system easily. As shown by the dashed lines in Fig. 3, there are no means or

processes to achieve information integrity and confidentiality pointing to cyber design deficiencies that must be mitigate in order to prevent access to OT components by adversaries. In essence, the abstraction hierarchy helps identify potential physical impact from missing security processes.

The abstraction hierarchy also highlights specific engineering process or equipment that should be "hardened" or further defended for cyber security. In this case study, attacker's access in PDS computer led to erratic of pump operations. The OT abstraction hierarchy shows that PDS computers serve as the only interface between the pumps and OT. Given physical pumping stations are essential to so many processes, OT components connected to pumping stations may deserve additional security solutions such as frequency hopping for the radio communication system. The protection provided by frequency hopping itself is limited, so diverse and redundant techniques may also be employed depending on budgets.

3.3 Work Domain Model for Coordinated Incidence Response

Coordination between operations and OT staff is essential in troubleshooting, specifically in deciphering cyber attacks from system malfunctions. The equipment connected to OT components without security features can be the primary target of cyber attacks. In this case study, control room operators were first to experience erratic pumping operation as a symptom of the cyber attack, and field operators were first to rule out physical problems with equipment inspection. Their investigation into erratic pump operations informed OT staff to look for false data, commands, and network address. In addition, the operations staff conceived the workarounds of manual controls at the pumping station to maintain throughputs while the OT personnel identified the compromises in the radio communication and alarm configurations. In essence, the final diagnosis and mitigation response to the cyber attack mandated coordination between operations and OT staff [33].

As cyber attacks are detected, coordination between operations and OT staff plays a critical role in responding to cyber intrusions. The abstraction hierarchies can help to illustrate the interaction between OT components and plant equipment during cyber events. In the Maroochy case study, the unexplained pump operations and pump lock ups were highly observable to operations personnel but the root cause of cyber attack could only be diagnosed by OT personnel.

The joint abstraction hierarchies therefore illustrates that effective incidence response to cyber intrusion must be coordinated between operations and OT staff. For example, when OT personnel detected suspicious network traffic between plant equipment, operations should be informed to monitor specific process area for unusual behaviors. Verification of control room indications with field operators may become temporarily necessary as OT personnel investigate the issue. Similarly, when unusual process behaviors occur, operations personnel may need to troubleshoot the root cause with OT personnel who would be aware of the security levels for different SCADA components.

4 Limitation

The WDA in this case study is solely based on publicly available information on the cyber attack and the Maroochy sewage treatment facility. For this reason, the WDA or the abstraction hierarchies likely contain some discrepancies to the physical and cyber design of the actual sewage facility. Discrepancies may also exist in the details of the actual cyber attack. Further, cyber security technology for SCADA equipment has improved drastically since the 2000 Maroochy cyber attack. Thus, the cyber security findings derived from the WDA specifically for Maroochy sewage facility are for illustration only rather than generating exact solutions.

5 Conclusion

This paper proposes WDA for evaluating and designing CPS through a case study of the Maroochy cyber attack on the sewage treatment plant. The case study illustrates that WDA can help identify system deficiencies and potential solutions to enhance cyber defense. Thus, WDA has demonstrated promise for improving cyber security that is increasingly relevant with advancing digital technology in CPS. As all of our critical infrastructures are becoming CPSs, cyber security is an essential design consideration that has serious economic, social, and financial implications. Given increasing number of insider threats and evolving APT, WDA can be one of many invaluable tools for system design and incidence response in cyber security.

References

1. NSF Program Guidelines: Cyber-Physical Systems (CPS) (2017). https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286
2. Lee, E.A.: Cyber physical systems: design challenges. In: 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC). IEEE (2008)
3. Alur, R.: Principles of Cyber-Physical Systems. MIT Press, Cambridge (2015)
4. Baheti, R., Gill, H.: Cyber-physical systems. Impact Control Technol. **12**, 161–166 (2011)
5. Helal, S., et al.: The gator tech smart house: a programmable pervasive space. Computer **38** (3), 50–60 (2005)
6. Kott, A., Aguayo Gonzalez, C., Colbert, E.J.M.: Introduction and preview. In: Colbert, E.J.M., Kott, A. (eds.) Cyber-security of SCADA and Other Industrial Control Systems. AIS, vol. 66, pp. 1–13. Springer, Cham (2016). doi:10.1007/978-3-319-32125-7_1
7. Sridhar, S., Manimaran, G.: Data integrity attacks and their impacts on SCADA control system. In: 2010 IEEE Power and Energy Society General Meeting. IEEE (2010)
8. Bagri, A., Netto, R., Jhaveri, D.: Supervisory control and data acquisition. Int. J. Comput. Appl. **102**(10) (2014)
9. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**(3), 49–51 (2011)
10. Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. In: 37th Annual Conference on IEEE Industrial Electronics Society, IECON 2011. IEEE (2011)
11. Denning, D.E.: Stuxnet: what has changed? Future Internet **4**(3), 672–687 (2012)

12. Chen, T.M., Abu-Nimeh, S.: Lessons from stuxnet. Computer **44**(4), 91–93 (2011)
13. Farwell, J.P., Rohozinski, R.: Stuxnet and the future of cyber war. Survival **53**(1), 23–40 (2011)
14. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: Leading Issues in Information Warfare and Security Research, vol. 1, p. 80 (2011)
15. Tang, K., Zhou, M.-T., Wang, W.-Y.: Insider cyber threat situational awareness framework using dynamic Bayesian networks. In: 4th International Conference on Computer Science and Education, ICCSE 2009. IEEE (2009)
16. Cai, N., Wang, J., Yu, X.: SCADA system security: complexity, history and new developments. In: 6th IEEE International Conference on Industrial Informatics, INDIN 2008. IEEE (2008)
17. Vicente, K.J.: Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work. CRC Press, Boca Raton (1999)
18. Mancuso, V.F., et al.: Human factors of cyber attacks a framework for human-centered research. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (2014)
19. Gutzwiller, R.S., et al.: The human factors of cyber network defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (2015)
20. Mancuso, V.F., et al.: Human factors in cyber warfare II emerging perspectives. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (2014)
21. Finomore, V., et al.: Effects of cyber disruption in a distributed team decision making task. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (2013)
22. Champion, M.A., et al.: Team-based cyber defense analysis. In: 2012 IEEE International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE (2012)
23. Rasmussen, J., Pejtersen, A.M., Goodstein, L.P.: Cognitive Systems Engineering. Wiley, Hoboken (1994)
24. Naikar, N.: Work Domain Analysis: Concepts, Guidelines, and Cases. CRC Press, Boca Raton (2013)
25. Burns, C.M., Hajdukiewicz, J.: Ecological Interface Design. CRC Press, Boca Raton (2004)
26. Rasmussen, J.: A framework for cognitive task analysis in systems design (1985)
27. Tokadli, G., Feigh, K.M.: Option and constraint generation using work domain analysis. In: 2014 IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE (2014)
28. Li, Y., Burns, C., Hu, R.: Understanding automated financial trading using work domain analysis. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (2015)
29. Lau, N., et al.: Ecological Interface Design in the nuclear domain: an empirical evaluation of ecological displays for the secondary subsystems of a boiling water reactor plant simulator. IEEE Trans. Nucl. Sci. **55**(6), 3597–3610 (2008)
30. Ahlstrom, U.: Work domain analysis for air traffic controller weather displays. J. Saf. Res. **36** (2), 159–169 (2005)
31. Jenkins, D.P., et al.: Using cognitive work analysis to explore activity allocation within military domains. Ergonomics **51**(6), 798–815 (2008)
32. Sanderson, P., et al.: Use of cognitive work analysis across the system life cycle: from requirements to decommissioning. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. SAGE Publications (1999)

33. Weiss, J.: Industrial control system (ICS) cyber security for water and wastewater systems. In: Clark, R.M., Hakim, S. (eds.) Securing Water and Wastewater Systems, pp. 87–105. Springer, Cham (2014)
34. Abrams, M., Weiss, J.: Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. The MITRE Corporation, McLean (2008)
35. Slay, J., Miller, M.: Lessons learned from the Maroochy water breach. In: Goetz, E., Shenoi, S. (eds.) ICCIP 2007. IIFIP, vol. 253, pp. 73–82. Springer, Boston, MA (2008). doi:10.1007/978-0-387-75462-8_6
36. Metcalf, E., et al.: Wastewater Engineering: Treatment and Reuse. McGraw Hill, New York City (2003)
37. Australian Guidelines for Sewerage Systems: Effluent Management. Australian Water and Wastewater Association, Editor (1997)