Risk and Impact Assessment Using Causal Graphs in Critical Infrastructure

Shengbo Wang
Supervised by: Sridhar Adepu

July 3, 2023

Abstract

Cyber physical systems (CPS) are intelligent systems controlled by computer-based algorithms, including sensors and actuators. They play an essential role to the functioning of human society for they provide fundamental resources, like water plants, power plants, etc. However, due to the complex architecture involving sensors, networks and communications, CPSs face vulnerabilities when the system gets larger in scale and attacked. Attacks towards CPSs can cause damages and huge financial losses. Therefore, assessing CPSs and the impacts under attacks becomes a paramount issue. In this thesis a risk and impact assessment method that captures both cyber-physical and physical-cyber dependencies between components is proposed. Causal dependencies and causal graphs are applied to represent the dependencies between nodes. Then attacks are designed and applied to a small scale water testbed. The impact of attacks are recorded. The results show that causal dependencies efficiently reveal the propagating impact of cyber attacks, and the method shows an ideal effect in assessing the riska and impacts.

Ethics statement: This project does not require ethics approval, as reviewed by my supervisor Sridhar Adepu.

I have completed the ethics test on Blackboard. My score is 12/12.

1 Project Plan

1.1 CPS concepts and attacks

A CPS integrates computational, networking, and physical components. Common examples are water plants, power plants and chemical factories. It usually includes Supervisory Control and Data Acquisition (SCADA) system composed of Programmable Logic Controllers (PLC), sensors, actuators (e.g., pumps, valves), and Human Machine Interface (HMI) [1].

A PLC is typically composed of CPU, I/O modules and communication modules [2]. They receive data from sensors and send corresponding commands to actuators. An HMI enables operators to interact with the system. A SCADA gathers and forwards data to other system that process and presents then to HMI [3]. It also records all the events of CPS and warns when conditions become hazardous.

Nowadays, due to the complex architecture of CPS and remote control through network, CPS are vulnerable to cyber attacks. For example, a power plant in Ukraine was compromised by illegally entering the SCADA and power was cut off for three hours [4] in 2015. Stuxnet worm virus targeting at PLCs invaded Iran's nuclear program and almost 1/5 of Iran's nuclear centrifuges were damaged [5].

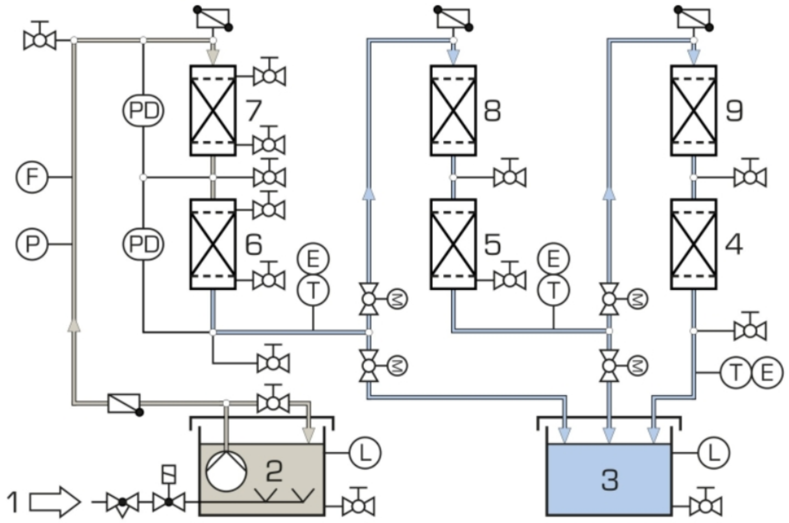
Attacks towards CPS can be divided into cyber attacks and physical attacks. Cyber attacks means disturbing the state of CPS through computer systems and communication network, while physical ones attempt tampering actuators directly [6].

1.2 Testbed architecture

University of Bristol cyber security group has a water testbed working as a small scale water plant. Figure 1 shows the architecture.

Raw water can become treated water through 6 tanks and there are several sensors and valves in control of the system. Raw water is pumped to the first tank, then passes solid filters, absorbers, ion exchangers, and finally ends up as treated water in a large tank. Conductivity, flow rate, water level, pressure, differential pressure and temperature are monitored by sensors. The maximum flow rate is 21 m^3/h.

The system can be controlled with a touching screen and a PLC is integrated to it. PCs can control the testbed as well through connecting to it in multiple ways. Data are stored in the internal memory and can be accessed through the IP address. The whole device is manufactured by German company GUNT (product code: CE 581) [7]. The system network architecture can be found in [8], where the same testbed is used.



1 external compressed air supply, 2 raw water, 3 treated water, 4 mixed bed ion exchanger, 5 adsorber (activated carbon), 6 sand filter, 7 gravel filter, 8 adsorber (aluminium oxide), 9 cation exchanger, E conductivity, F flow rate, L level, P system pressure, PD differential pressure, T temperature

Figure 1: Testbed architecture. Source: GUNT[7]

2 Literature Review

2.1 The testbed

Rashid et al.[8] who used the same water testbed for research give ways for cyber attacks. Kepware is a data historian with direct access to the control hardware. It performs data aggregation for the testbed. Thingworx is used as the primary cloud service. When connected to Kepware, applications can be developed to process the data from control devices. To attack the PLC, Thingworx is compromised through security vulnerabilities in Tomcat first, then HTTP listener is set up. After several steps, attackers can interfere with the physical processes directly and force HMI show false data. This is realised through writing false data into specific memory locations where overwritten data are stored.

2.2 Attacks

Some kinds of attacks are mainly mentioned in works about CPS: denial of service (DoS) attack, deception attack, and replay attack.
DoS attack refers to flooding the machines or computers with traffic to deprive legitimate users of the service they want [9]. In [10] Dos is used to impede a PLC to receive values from sensors.
Deception attacks affect the data integrity of packets by modifying their pay-

loads [11].
In replay attacks, attackers try to invade sensors, record values and then replay the data [12].

2.3 Causal graphs and Bayesian network

Bayesian networks (BN) are directed acyclic graphs (DAG) with a set of discrete random variables and directed edges representing the dependent relations between nodes [13]. The directed edge indicates that the two nodes are correlated. BN includes 2 kinds of nodes, i.e., parent node and child node.
BN can be used to simulate a causal relationship. Given a set of discrete variables $\mathcal{X} = \{X_1, X_2, \cdots, X_n\}$, the joint probability distribution (JPD) can be calculated as 1.

$$\begin{aligned} P(\mathcal{X}) &= P(X_1, X_2, \cdots, X_n) \\ &= P(X_1)P(X_2|X_1)\cdots P(X_n|X_1, X_2, \cdots, X_{n-1}) \\ &= \prod_{i=1}^{n} P(X_i|Parent(X_i)) \end{aligned} \tag{1}$$

Causality is a familiar thing to human. It means one event causes another. Causal graphs are represented as DAGs and show causation between variables. Two variables of interest can be distinguished, the exposure and outcome [14]. In the thesis, CPS can be presented as causal graphs, where nodes represent sensors and actuators, and edges represent control and information flows.

2.4 Impact and risk assessment

There are a lot of work regarding risk and impact assessment of CPS. To divide the task, risk assessment tests the vulnerability of CPS, while impact assessment shows the effects of CPS after attacks.

Lyu et al.[15] proposed a risk assessment method based on Bayesian network then applied to a dual tank system. The method is designed towards cyber-physical attacks whose cyber threats impact physical processes. The risk value is defined as the sum of multiplication of value for each part and the probability that this part is compromised. The Bayesian network topology of the system is derived first, where listed vulnerabilities point to digital layer, physical layer then to the tanks. The vulnerabilities are identified on Common Vulnerability Scoring System (CVSS) and the probability that each is exploited is calculated through multiplying several numbers. After knowing the probabilities of parent nodes, the probability that the tank is compromised can be derived.
However, this method may not fit our system because the value for each separate part is not given. In addition, it is hard to identify the vulnerabilities for our system.

Adepu et al.[6] point out a good direction, where experiments are conducted

on a water testbed. They define an attacker model, attack model and attacks in mathematical language, which solves the problem that no model is specifically designed for CPS. Then two series of attacks with different aims are designed and implemented on the testbed. Through experiments, researchers found the attack that causes the largest number of affected actuators and the greatest cost of recovery. In addition, researchers studied the impact on the flow rate and pH of the testbed.
Of course the experiments above may not suit other CPS due to different structures. For our testbed, there is no sensor measuring pH, but conductivity of water can be a good choice to study the impact of attacks on water quality.

Tantawy et al.[16] developed an integrated model-based CPS security risk assessment approach. The CPS in the research is a simulated exothermic Continuous Stirred Tank Reactor (CSTR). Researchers derived an automaton model fro the architecture and enumerated hazardous states. Then attack scenarios are developed and tested on the testbed, so that researchers could find ways to mitigate the attacks.
The automaton model is introduced specifically. In the CPS there are 3 actuators and each has 2 states, so there are 8 states in total. Then a state diagram is derived where a state can transfer to another through one or two operations. Hazardous states are identified and a hazard execution tree is generated with the initial state as the root node and hazardous states the leaf nodes. Attacks are developed after deriving attack trees with AND and OR gates judging relevant vulnerabilities.
Automaton models may not be suitable when the CPS is quite complex, i.e., there are too many states in the diagram.

Wu et al.[17] proposed a risk assessment method where the total risk score is the sum of risk scores of all hosts in a CPS, and concrete calculating formulae are given. However, the sources of formulae are quite confusing.

Pelissero et al.[10] studied the anomaly propagation in a naval water distribution CPS. A methodology of value is that researchers use a 3-layer model [18] to describe the water system, where layers represent digital subsystems, physical subsystems and system variables. Researchers designed 4 kinds of attacks and simulated to find the propagation of attacks.

Huang et al.[19] apply BN to model CPS and probabilities are inferred. Then the probabilities are fed into a stochastic hybrid system (SHS) model to predict the evolution of the physical processes. SHS is s defined on a hybrid state space involving both continuous and discrete states.

References

[1] M. Balaji, S. Shrivastava, S. Adepu, and A. Mathur, "Super detector: An ensemble approach for anomaly detection in industrial control systems," in *Critical Information Infrastructures Security*, D. Percia David, A. Mermoud, and T. Maillart, Eds. Cham: Springer International Publishing, 2021, pp. 24–43.

[2] Y. Chang, T. Kim, and W. Kim, "Impact analysis of plc performance when applying cyber security solutions using active information gathering," in *Critical Information Infrastructures Security*, D. Percia David, A. Mermoud, and T. Maillart, Eds. Cham: Springer International Publishing, 2021, pp. 133–151.

[3] "SCADA (supervisory control and data acquisition)," 2021. [Online]. Available: https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition

[4] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[5] M. B. Kelley, "The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought," 2013. [Online]. Available: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?r=US&IR=T

[6] S. Adepu and A. Mathur, "An investigation into the response of a water treatment system to cyber attacks," in *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, 2016, pp. 141–148.

[7] "G.U.N.T. Gerätebau GmbH Germany," 2023. [Online]. Available: https://www.gunt.de/en/products/2e-environment/water/multistage-water-treatment/water-treatment-plant-1/083.58100/ce581/glct-1:pa-148:ca-693:pr-57

[8] A. Rashid, J. Gardiner, B. Green, and B. Craggs, "Everything is awesome! or is it? Cyber security risks in critical infrastructure," in *International Conference on Critical Information Infrastructures Security.* Springer, 2019, pp. 3–17.

[9] "What is a denial of service attack (DoS) ?" [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[10] N. Pelissero, P. M. Laso, and J. Puentes, "Impact assessment of anomaly propagation in a naval water distribution cyber-physical system," in *2021*

IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2021, pp. 518–523.

[11] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th annual Allerton conference on communication, control, and computing (Allerton).* IEEE, 2009, pp. 911–918.

[12] L. Faramondi, G. Oliva, and R. Setola, "Optimal man-in-the-middle stealth attack," in *Critical Information Infrastructures Security: 16th International Conference, CRITIS 2021, Lausanne, Switzerland, September 27–29, 2021, Revised Selected Papers 16.* Springer, 2021, pp. 44–59.

[13] D. Kuipers, "Common cyber security vulnerabilities observed in control system assessments by the inl nstb program," *Idaho National Lab.(INL), Idaho Falls, ID (United States), Tech. Rep*, 2008.

[14] A. Földvári and A. Pataricza, "Support of system identification by knowledge graph-based information fusion," in *27th PhD Minisymposium of the Department of Measurement and Information Systems.* Budapest University of Technology and Economics, 2020, pp. 12–16.

[15] X. Lyu, Y. Ding, and S.-H. Yang, "Bayesian network based c2p risk assessment for cyber-physical systems," *IEEE Access*, vol. 8, pp. 88 506–88 517, 2020.

[16] A. Tantawy, S. Abdelwahed, A. Erradi, and K. Shaban, "Model-based risk assessment for cyber physical systems security," *Computers & Security*, vol. 96, p. 101864, 2020.

[17] W. Wu, R. Kang, and Z. Li, "Risk assessment method for cyber security of cyber physical systems," in *2015 first international conference on reliability systems engineering (ICRSE).* IEEE, 2015, pp. 1–5.

[18] N. Pelissero, P. M. Laso, and J. Puentes, "Naval cyber-physical anomaly propagation analysis based on a quality assessed graph," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).* IEEE, 2020, pp. 1–8.

[19] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 8153–8162, 2018.

A Project Timeline

Table 1: Timeline (3 July - 31 Aug)

Week	1	2	3	4	5	6	7	8	9
Literature review	X	X							
Risk and impact assessment method study	X	X	X						
Attack design		X	X						
Attack related methodology study		X	X						
Experiments				X	X				
Experiment assessment and optimisation						X	X		
Thesis							X	X	X

B Risk Assessment

Table 2: Risks and Mitigations

Risk	Likelihood	Severity	Mitigation
Computer problem (stolen or broken)	Medium	High	Backup all work using the cloud. Keep cups and bottles far from the computer.
The testbed gets broken	Medium	High	Design attacks carefully. Stop experiments when noticing the test bed goes wrong.
The supervisor goes for holidays and no time to meet	Low	Medium	Ask the supervisor about his summer plans in advance.
Miss the supervisor's feedback	Low	Low	Check the email and Teams regularly.
Time conflict with others working on the testbed	Medium	Medium	Maintain a schedule for all people working on the testbed.