Security-based Safety Hazard Analysis using FMEA: A DAM Case Study

Irum Inayat[1], Muhammad Farooq[2], [3]Zubaria Inayat, and [4]Muhammad Abbas

[1,2] Department of Software Engineering, National University of Computer Emerging Sciences, Islamabad, Pakistan
[3]Department of Computer Science, Bahira University, Islamabad, Pakistan.
[3]Univeristy of Twente, Enchede, The Netherlands.
[4]Research Institutes of Sweden Västerås, Sweden
irum.inayat@nu.edu.pk, i191235@nu.edu.pk,
zubaria.buic@bahria.edu.pk, muhammad.abbas@ri.se

Abstract. Safety and security emerge to be the most significant features of a Cyber-Physical System (CPS). Safety and security of a system are interlaced concepts and have mutual impact on each other. In the last decade, there are many cases where security breach resulted in safety hazards. There have been very few studies in the literature that address the integrated safety security risk assessment. Since, the need of the time is to consider both safety and security concurrently not even consequently. To close this gap, we aim to: (i) perform hazard analysis using Failure Mode Effect Analysis (FMEA) of a cyber physical system case i.e., Dam case study, and (ii) perform risk identification, risk analysis and mitigation for the said case. As a result, we extracted the potential failure modes, failure causes, failure effects, and the risk priority number. In addition, we also identified the safety requirements for the modes of the subject.

Keywords: Safety-Security Hazard Analysis, Risk Assessment, Safety Requirements, FMEA, Cyber-Physical Systems.

1 Introduction

Cyber-physical systems (CPS) have changed the way humans and machines (computational resources) connect with each other. CPS have many open issues such as data query, latency, storage, real-time data processing, and security among many [1]. Security being the prime factor to let the consumer trust on technology, surfaces the most. Intricate systems like smart homes, industrial automation systems, and automotive rely on secure communication to prevent the risk of life and property. A total of 490 cyberattacks were reported on CPS in the last one decade (2010-2020) published by an American think tank (Center for Strategic & International Studies) [2], [3]. Some of the famous cyber-attacks of the decade are Stuxnet [4], Shamoon [5] etc. It is worth mentioning here, that the connection between security and safety is inevitable for CPS [6]. Safety is a non-functional requirement/trait of the system and is defined as specific,

mandatory and minimum amount of safety for system to remain in safe state. Safety has a specific metric assigned to it referred as functional safety of the system [7]. ISA 99/IEC62443 (a safety standard) states that risk management for Industrial Control Security (ICS) (which is a CPS) should cover three parts, functional safety (according to ISA 84/IEC61511 & IEC61508 functional safety focuses on protecting and monitoring the devices or equipment from accidental failures or maintaining a safe state during the operating process), physical safety (Physical safety issues cause hazards such as fire breakout, explosion, flood, chemical spills, biochemical spill and crash of a vehicle [8] [9]) , and cybersecurity (ISA 99) [8].
Studies and reports framed many safety incidents and security attacks that happened in industries. Recently, more cases have surfaced where the attackers compromised the safety of CPS by intruding the security of a certain CPS [4]. Some of the recent examples are explained here. For instance, Maroochy Shire Sewage Spill (MSSS) [10] where a SCADA based plant controls more than 142 sewage pumping stations, where each pumping station has their own computer system that receives the command from master station and sends it back to the center. It is one of the largely quoted case of cybercrime disrupting SCADA. Stuxnet virus attack on the SCADA control system of Iranian Nuclear enrichment plant [11]. The worm was particularly devised to target equipment of SCADA utilized by the targeted country in their nuclear power improvement processes. The attack maimed hardware and burnt centrifuges in the Natanz facility of Iran. The cyber-attack on the German Still mill [4] making its furnace go out of control causing physical damage. The ransomware attack on US natural gas pipeline made the supply halt for two days causing chaos and business loss [12]. The Aramco, which pumps 10% of global oil supply, experienced its largest cyber-attack to date in August 2012, when a Shamon virus attack damaged around 30,000 computers and was aimed at stopping oil and gas production at the biggest OPEC exporter [13].

The examples showed the cases where security vulnerabilities facilitated attackers to compromise the safety of the system [4] . Therefore, the interlaced concepts of security and safety of CPS have become highly relevant in the recent past. CPS utilizes both cyber and physical layers for the communication. It is also noteworthy that in recent years, most of the cyber-attacks commenced with security vulnerability that helped the intruder to inject the malfunction or virus into the system. Therefore, it ends up with compromising the functional safety of the system, that could be fatal to a user life that works in the surrounding. These issues highlight the importance of restructuring the process for development of CPS. If the failure and the vulnerabilities were addressed at design stage there will be less chances of system, failure. That is why, the study includes FMEA that is safety hazard analysis which help to mitigate the risk at design stage. Therefore, in this study we aim to: (i) to identify the hazards from FMEA hazards analysis method, (ii) derive the safety requirements by aligning the identified hazards with IEC-61508 standard and, (iii) identify, analyze and mitigate the risk from DAM case study.

The remaining part of the study is aligned as follows. Section 2 describes the background of different hazard analysis methods and other aspects of the paper. Section 3

provides the designing process of case study. Section 4 contains the results of the process. Section 5 holds the discussion on the results and Section 6 concludes/summarizes the paper and discusses the future work.

2 Background

Risks are the uncertain events that lead to hazard. The risk management process can help in eliminating or reducing the probability of occurrence of such events. However, the need of the hour is to consider safety and security risks together and not in succession [10]. Here we summarize the key features that lack in the existing risk management techniques for security-safety risks. Boolean logic driven Markov Process (BDMP) is a graphical modeling approach designed for four kinds of events (i.e., basic, security, safety, and instantaneous events) for CPS [12]. The technique facilitates to draw the security features like Confidentiality, Integrity and Availability (CIA) and addresses the security-safety interlink. However, risk assessment and analysis are not addressed in BDMP. STPA-SafeSec claims that security has an impact on safety and demonstrates its evaluation through a causal model [13]. Bayesian Relief Networks (BRN) is a process used in the industrial control and security over the last two decades that deals with decision making for the uncertain situations [14]. It estimates the likelihood of occurrence of a failure in achieving safety and security requirements. Six-Step Model (SSM) and Information Flow Diagram (IFD) integration approaches help in identifying safety-security requirements by providing significant communication channel vulnerabilities. The risk assessment method combines the attack tree and simulation of CPS resources [15]. The Failure Mode Effect Analysis (FMEA) is type of risk assessment method. The method was applied on autonomous braking system [14] and helps to find risk and assess them in quantitative manner.
Keeping the mentioned gaps in view, this study aims to identify, analyze, plan, control, and track the safety security risks for CPS demonstrated with a case study example of a hydroelectric plant.

3 Case Study Design

The Taum Sauk project [15] is located in the Mountain region of St. Francois in southwest of Missouri which is a region of United States. The plant was developed between 1960-1962. It consists of turbines, power station, tunnels and reservoirs. Basically, Taum Sauk has two dams referred as Upper and lower dam. The main purpose of its design (as shown in Fig.1) was to fulfill the electric demand in peak hours. It started its operation from 1963 and the water was flowing from the upper reservoir to lower reservoir. Because of the absence of natural flow, the law of thermodynamics enforces to consume more power to pump the water into the upper reservoir for electricity generation. Although, it was still running on economic cost because the upper reservoir got filled at night. It was referred as the biggest battery because of its vast capability of

storing energy. It is generally controlled with microwave signal system from Osage Plant. The minimum water level in lower reservoir of the dam is 736 feet and maximum water level 749.5 feet. The instrumentation of the dam is divided into two parts (as shown in fig 2) : Pressure sensors and conductivity sensors. Different kinds of PLC were installed to operate under dispatch controller and operation. The complete system depends upon the two kinds of PLC (Programmable logic controllers) known as Common PLC and Upper Reservoir PLC (UR PLC). In December 2005, the upper reservoir of the dam witnessed a catastrophic failure and stop its operation until it was redeveloped and commenced its operation in 2010. In 2005, the Northwest side of UR got overtopped during it refilling process. As a result, 38000000m^3 amount of water released in just around 12 minutes, which is equal to 1 billion US gallons. All the crew members survived the flood. According to the investigation and press notes, gauges that were used to monitor the water level in the upper reservoir were crashed/malfunction [15].

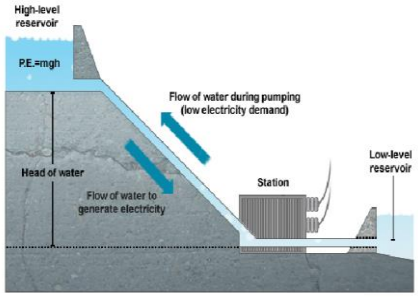

Fig.1. Taum Sauk Dam

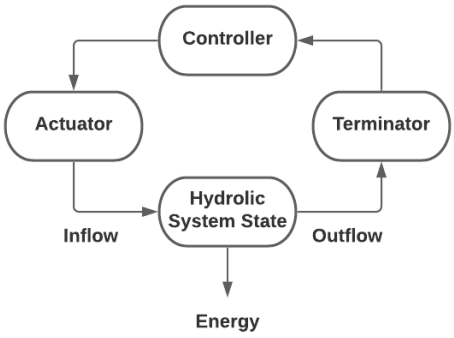

Fig..2 Control Diagram

4 Results

4.1 Security-based safety hazard analysis of DAM case study using FMEA

Failure mode effect analysis (FMEA) is a bottom-up risk analysis approach. It is used at the design stage to prevent the potential failures. It can be applied in the design phase of the system by following the five basic steps: (i) System partitioning, (ii) Assign function to every component, (iii) Determine failure modes for the system, (iv) Risk evaluation with RPN (Risk's priority number), (v) Risk mitigation mechanism.
After performing the FMEA on Taum Sauk project, we managed to identify 58 hazards for the five basic components of the system i.e., Operator, dispatcher, PLC, Sensors, gates. Once identified the hazards, RPN was calculated to analyze the severity level of the risks. The analysis led to the fact that by compromising the system authentication and launching the DDoS attack the data may be altered to make the system components perform in an anomalous way. This abnormal behavior can result into sudden release

of water causing disaster (flooding). Another major cause of accident is the failure of the physical components i.e., turbines, PLC, spillways, or sensors etc. All the components must be fully functional in order to generate electricity. The power station is controlled by the microwave signal, so the jamming attack can disturb the whole system. This will end up in shutting down the hydroelectric power station. Most of the data sent from the HMI (Human Machine Interface) controller and the operator sends that information to other integrated components, if such data is compromised with MITM (Man in the Middle) attack. The end situation will create safety hazards that can demolish the whole structure. The detailed FMEA analysis done on the Dam case is explained in the table 1, below. For the dispatch control software which is a part of dispatch control system has the application function "send megawatt instruction" which could fail due to security breach causing "no electricity generation" as the effect. This shows the interconnection of safety and security risks in a CPS. Likewise, for the Operator control center which is responsible for activation/deactivation of generators and water pump has a risk of jamming attach due to weak or no message encryption. As a result, there will be no electricity generation during the scheduled hours. The deactivation of generators could cause the UR empty causing the water level reaching minimum.

Table 1. FMEA

System	**Component**	**Application Function**	**Potential Failure Mode**	**Potential Cause of failure**	**Potential Failure Effect**	**Risk Assessment**			
S	C	AF	FM	CF	FE	B	A	E	RPN
Conductivity Sensors	Sensor	HI sensor	Pump stop at HI_HI sensor level	structural instability	Faulty HI Sensor	3	2	2	12
					Delay in Stop signals to pump	3	3	3	27
Conductivity Sensors	Sensor	HI_HI Sensor	The pump does not stop at HI_HI sensor	UR Toppled	Faulty HI_HI Sensor	4	2	2	16
				Upper Reservoir Toppled	Delay in Stop signals	4	2	3	24
Upper-Reservoir PLC	PLC	UR PLC	The pump does not stop till S_HI_HI level	Upper Reservoir Toppled	Incorrect data to the operator control center	4	3	2	24
Common PLC	PLC	Common PLC	The pump does not stop till S_HI level	Structural instability due to over water capacity	Fault in PLC	3	2	3	18
				Structural instability due to over water capacity	S_HI Faulty data	3	3	2	18
Logical Gates	Conditions	AND | OR	Data interruption	Gate Failure	Delay	2	3	1	6
Operator	Operator Controller	Operator Control Center	Feedback not reported	Provide wrong signal	Display Irrelevant message	3	3	2	18

Taum Sock unit	Operator Control-ler	Operator Control Center	Operator Con-troller failure	Primary sensor sending wrong infor-mation	unable to access remotely	3	2	2	12
Firewall	Operator Control-ler	Authenti-cation	Intrusion into System	IDS not working	Loss of data	2	4	1	8
Pump Turbine	PLC	Pump	(Pump Tur-bine)	System spilled	Pump not started	3	5	3	45
Dispatch Control Center	dispatch Control software	Send Megawatt generation instruction	Attacker modifies the sent Megawatt instruction.	No encryption.	False or No Megawatt generation	5	2	1	10
			Megawatt generation instruction sent too late or lost.	Jamming attack	No electricity generation	2	2	1	4
				Network Issue	electricity generation in low de-mand hours	2	2	1	4
		Reception of generation data from operator	Generation Feedback not received / Lost Feedback / Feedback received late.	Jamming attack	No feedback regarding dam operation	1	2	1	2
Operator Control Center	Common PLC	Water Level	Erroneous cal-culation	SW Defect	Overtopping	2	4	3	24
			Obsolete Data	Network Congestion	Pumps are not stopped	2	4	3	24
		Activation of generators	Activate gen-erator com-mand sent lost.	Jamming attack or Network issue.	No electricity generation.	5	2	2	20
			Activate gen-erator com-mand altered by the at-tacker.	No encryption	No electricity generation during the required hours.	5	3	3	60
			Activate gen-erator com-mand not sent.	HW-failure	No electricity generation.	5	1	3	15
		Deactiva-tion of generators	Deactivate generator command lost.	Jamming attack or Network issue	UR empty	1	2	5	10
			Deactivate generator command altered by the attacker.	No encryption		1	2	3	6
			Deactivate generator command not sent.	HW-failure		1	2	3	6
			Deactivate generator command sent late.	erroneous implemen-tation of event	water level reaches below mini-mum level.	1	2	3	6
		Deactiva-tion of pump	Stop pump command delay to the plc pump	erroneous implemen-tation of	Potential overtopping of upper reservoir	5	2	4	40

				events and queues					

4.2 Safety Requirements

Table 2 presents the complete description safety requirements and constraints derived from the FMEA hazard analysis.

Table 2. Safety requirements

Modes	**Safety Requirement**
Pressure sensor failure	The pressure sensor shall trigger the shutting down of pump if level of water in reservoir reaches above its desired level.
Conductivity sensor failure	The conductivity sensors shall activate if the water level rises above the safe level.
Incorrect monitoring	The sensors LO and LO-LO shall be activated as soon as the water level becomes too low.
Malfunctioning	HI sensor shall activate the automatic shutdown of the pumps if pressure sensors start operating incorrectly
	The HI and the HI-HI sensors shall be used for emergency shut-down when extremely high-water levels occur.
	HI-HI sensor shall activate a hard emergency stop of the pumps if pumping mode is not terminated
	The reversible pumps shall be deactivated when the water level in the upper reservoir becomes high
	The system shall be able to notify the operator when an operation is about to occur between the safe and unsafe states of the pressure sensors (p1, p2, and p3).
	The system shall be able to notify the operator when an operation is about to occur between the safe and unsafe states of the conductivity sensors that are placed in pairs above and below the water levels.
	Problem- free circuity shall design for the elements that have failure results probabilities greater than 0.00001 for any explosion or damaged
	The system shall be able to notify the operator when an operation is about to occur between the safe and unsafe states of the conductivity sensors that are placed in pairs above and below the water levels.
Incorrect reading of k-n-gates measure normally it is (2/3) voter	The system shall be able to be written in the specified probability of the fault detections, probability of the fault isolations that has been taken as input from the pressure sensors. The system components shall return the hardware to an assigned safe state when unsafe hardware states are identified

Software components associated with the high level and low-level water has failures.	All elements shall provide a permissible error rate to ensure that the HMI components software is operating properly. System shall be able to alarmed when HMI software components cannot work properly.
HCI producing apparently correct but infect wrong result	System shall display a message in HMI in case of the software elements are failures. The system shall identify leading severity failures in an outer safety-critical appliance, I/O device devices, operator control center, modules, and interfaces. The system shall revert to a safe state upon all the high severity occurrence.
After water level touches the high, H1 sensors does not alarmed and did not sent signals to common PLC which sends instruction to PLC pump to shut down the pump.	The H1 sensors conditions shall be detected by Common PLC. System shall be able to be alarmed when the water touches the highest water level. System shall send instructions to pump to shut down the operation aft
Feedback from common-PLC and UR-PLC that are not reported in the operator-control-center.	System shall be able to report the feedback from common-PLC and UR-PLC. Feedback circuit shall reserve 10s after operator control center switch is actuated. System shall display a message in HMI for users about the feedback every 1 hour.
Operator-soft gets incorrect feedback showing the highest water level value; it would send an instruction to common-PLC to shut down the pumping-unit.	System hardware devices shall be able to send feedback from hardware components to UR- water level. The common operation shall not create system injury while compiling a particular function at a specific period under certain conditions. System shall get the hardware components UpToDate and valid. System shall be able to measure the water highest level and send feedback to common-PLC.
PUMP PLC	water Pump shall not be stopped when water in upper reservoir is bellow low level. water level reported by low sensor shall be validated using water level value of pressure sensors.
	SCADA shall ON alarm on failure of high-level sensor. Operator control center shall shutdown water pump when high level sensor fails
	SCADA shall ON alarm on HI-HI sensor failure. Notification of high sensor failure shall be sent to operator control center. Water Pump shall shutdown after HI-HI sensor failure notification received at operator control center.
	System shall calculate water level using pressure sensor after failure of LO-LO sensor and start water pump.
Water shortage in upper reservoir	Water Pump shall not be stopped when water in upper reservoir is below low level.

Pressure Sensor	The pressure sensor shall trigger the shutting down of pump if level of water in reservoir reaches above its desired level
Conductivity Sensors	The conductivity sensors shall activate if the water level rises above the safe level.
HI_HI Sensor	The HI and the HI-HI sensors shall be used for emergency shut-down when extremely high-water levels occur
L0-L0 Sensor	The sensors LO and LO-LO shall be activated as soon as the water level becomes too low.
HI Sensor	HI sensor shall activate the automatic shutdown of the pumps if pressure sensors start operating incorrectly

5 Conclusion and future work

Secure CPS are the safe ones. Vulnerabilities in CPS can be exploited to cause destruction and damage to property and life. With increasing connectedness, the vulnerabilities and backdoors are also escalating. However, for CPS security breach can be detrimental to physical assets along with data and can have serious consequences. It is predicted to have a ransomware attacks on businesses every 11 seconds in 2021 as compared to 40 seconds in 2016 causing loss of billions of dollars. Therefore, it is the need of the time to consider security and safety as one. In this work, we have performed risk analysis of a CPS i.e., Dam case study using FMEA to identify the potential safety and security risks, modes, effects and the risk priority numbers. The failure modes and their underlying effects helped us to identify the relevant safety requirements. We have identified safety requirements for all the identified modes of the case under discussion. This shows that safety requirements may be identified while identifying security breaches of a system. Our results show that the dispatch control system and operator control center have security risks that can cause damages like “no electricity generation” and “emptying the UR to let the water touch minimum level”.

Close at hand, we plan to align our safety requirements with the safety standards and comparing our results by evaluating the case using other hazard analysis methods. We also aim to replicate the analysis on another CPS to discuss on the differences system dynamics might have on risk identification.

References

[1] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, “Cybersecurity of Industrial Cyber-Physical Systems: A Review,” *Cryptogr. Secur.*, p. 32, 2021.

[2] J. A. Lewis, “Significant Cyber Incidents since 2006, Center for Strategic and International Studies.” p. 57, 2021.

[3] M. N. Al-Mhiqani *et al.*, “Cyber-security incidents: A review cases in cyber-physical systems,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 1, pp. 499–508, 2018.

[4] R. M. Lee, M. J. Assante, and T. Conway, “German Steel Mill Cyber Attack,” *ICS Def. Use Case*, p. 15, 2014.

[5] Z. Dehlawi and N. Abokhodair, “Saudi Arabia’s response to cyber conflict: A case study of the Shamoon malware incident,” *IEEE ISI 2013 - 2013 IEEE Int. Conf. Intell. Secur. Informatics Big Data, Emergent Threat. Decis. Secur. Informatics*, pp. 73–75, 2013.

[6] T. Alladi, V. Chamola, and S. Zeadally, “Industrial Control Systems: Cyberattack trends and countermeasures,” *Comput. Commun.*, vol. 155, no. March, pp. 1–8, 2020.

[7] R. Fu, X. Bao, and T. Zhao, “Generic safety requirements description templates for the embedded software,” *2017 9th IEEE Int. Conf. Commun. Softw. Networks, ICCSN 2017*, p. 5, 2017.

[8] M. T. De Azevedo, A. B. Martins, and S. T. Kofuji, “ISA99 - Security Standards in water treatment plants,” *Water/Wastewater Autom. Control. Symp.*, pp. 1–15, 2013.

[9] H. Gall, “Functional Safety IEC 61508 / IEC 61511 the impact to certification and the user,” *AICCSA 08 - 6th IEEE/ACS Int. Conf. Comput. Syst. Appl.*, pp. 1027–1031, 2008.

[10] N. Sayfayn and S. Madnick, “Cybersafety Analysis of the Maroochy Shire Sewage Spill Cybersafety Analysis of the Maroochy Shire Sewage Spill,” *Cybersecurity Interdiscip. Syst. Lab.*, no. May, pp. 1–29, 2017.

[11] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, “Towards a framework for assuring cyber physical system security,” *Int. J. Secur. its Appl.*, vol. 9, no. 3, pp. 25–40, 2015.

[12] N. Scaife, P. Traynor, and K. Butler, “Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward),” *IEEE Potentials*, vol. 36, no. 6, pp. 28–31, 2017.

[13] S. Alelyani and H. Kumar G R, “Overview of Cyberattack on Saudi Organizations,” *J. Inf. Secur. Cybercrimes Res.*, 2018.

[14] S. M. Sulaman, A. Beer, M. Felderer, and M. Host, “Comparison of the FMEA and STPA safety analysis methods-a case study,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-292, pp. 175–176, 2019.

[15] S. Kriaa, M. Bouissou, and Y. Laarouchi, “SCADA Safety and Security joint modeling (S-cube): case study of a dam,” 2016.