CYBER PHYSICAL SECURITY OF A CHEMICAL PLANT

Mr. Gyanesh Kumar[1]
[1]Academic Counselor, IGNOU
Mr. Nandan Kumar[2]
[2]Resource Person, B.M.D. College, Dayalpur, Vaishali, Bihar
Dr. Prakash Vardhan[3]

Abstract- Providing more secure procedures to protect industries and reduce risks requires immediate attention given the rise in cyber attacks on industries. Industrial Control Systems (ICS) refer to cyber physical systems (CPS) utilised in industries like oil and gas, chemical process plants, and similar ones (ICS). Control system security aims to stop purposeful or unintentional interference with industrial automation and control systems' normal operation (ICS). In order to identify when a sensor signal is being maliciously altered, this study suggests a process-aware strategy using invariant equations based on the physical and chemical features of the process and multiple Security Domain Non deducibility (MSDND) framework. We used a benzene production facility as a case study to demonstrate our methodology and its efficacy in ascertaining the system's status.

Keywords: Cyber, Physical Security, Chemical Plant, Industrial Control Systems (ICS), Cyber Physical Systems (CPS).

1 INTRODUCTION

An industrial process plant that manufactures or processes chemicals on a big scale is often referred to as a chemical plant. Such a plant receives a certain set of raw materials as input and processes (reacts) those elements to create the intended chemical output. The manufacturing process is carried out in these facilities using specialised machinery, units, and technology. Information confidentiality, integrity, and availability are all given adequate consideration, as well as operational safety. The National Institute of Standards and Technology (NIST) lists the following as important security risks of a chemical plant in its Public Working Group in CPS: 1) Process Safety 2) Equipment Safety These can be maintained by high reliability and security and only cyber security can provide the necessary protection against attacks on the control processes. While the NIST document discounts privacy as a concern due to a lack of personally identifiable information, one can envision confidentiality of the actual processes as desirable. In this document, we examine the general security concerns of a benzene production plant using Multiple Security Domains No deducibility (MSDND) [1] [2] models and Belief, Information transfer and Trust (BIT) logic [4] [5].

2 RELATED WORK

This paper mainly focuses on information flow disruption rather than theft of information.

(i) Non Deducibility (ND)- Non deducibility was introduced by Sutherland in an attempt to model information flow in a partitioned model. The partitions are divided into two sets, these sets are usually labeled as high and low with information restricted to one side of the partition or the other. Information that cannot be deduced from the other side of the partition is said to be non deducibilty secure. However, the partitions must be absolute and the partition is necessarily simplistic. Overlapping security domains present difficulties for ND as do information flows which cannot be evaluated because the model lacks the required valuation functions. However the restrictions of Sutherland's ND model made it difficult to model critical infrastructures like industrial control systems, transportation systems etc. The motivation to model security for these critical infrastructures and to have much more refined control over the information being transferred and to deal with multiple physical and cyber components at a time led to the development of Multiple Security Domain Non deducibility model.

(ii) Valuation Function- $V_x{}^y(\varphi)$ represents valuation function of boolean x in domain y. A valuation function is a function which assigns a truth value to question φ in place based on x with respect to the security domain y.

(iii) Security Domain (SDⁱ)- The event system divides the system into multiple security domains SDⁱ as viewed by each entity i in the model. These security domains may or may not overlap with each other. An entity i is any part of the system that is capable of independent observation or action.

(iv) Multiple Security Domain Non Deducibility- There exists some world with a pair of states where one must be true and the other false (exclusive OR), but an entity I has no valuation function for those states. In security domain SDⁱ, i simply cannot know which state is true and which is false.

$$\mathrm{MSDND(ES)} = \exists \mathrm{w} \in \mathrm{W} \vdash [(s_x \vee s_y)] \wedge \sim(s_x \wedge s_y) \wedge [\mathrm{w} \models (\nexists V_x^i(\mathrm{w}) \wedge \nexists V_y^i(\mathrm{w}))]$$

An equivalent formula is

$$\mathrm{MSDND(ES)} = \exists\ \mathrm{w} \in \mathrm{W} \vdash [(s_x \oplus s_y)] \wedge [\mathrm{w} \models (\nexists V_x^i(\mathrm{w}) \wedge \nexists V_y^i(\mathrm{w}))]$$

MSDND is not a high/low hierarchy model, but is instead a partitioning model. MSDND does not depend upon examining two domains on any relationship between those domains such as low and high or left and right. The domains in question might be wholly contained in the other, they might overlap, or they might be disjoint. Sutherland's Non deducibility can be reduced in polynomial time to MSDND [2].

(v) BIT logic- BIT logic was introduced by Liau [4] [5] to formally reason about belief, information transfer and trust when dealing with cyber entities. While it was developed primarily for handling trust in database and distributed systems, BIT logic is useful for describing CPS, especially when humans are involved. Before BIT logic, social engineering attacks could only be described by a narrative in imprecise language. With BIT logic, spoofing and other unwanted behavior is described with simple, formal proofs. BIT logic is designed to reason about the belief and trust an entity i has in information from an entity j, e.g. the belief and trust an operator has in the reading from a monitoring station.

(vi) Invariants- Invariant is a function, quantity, or property that remains unchanged when a specified transformation is applied. An invariant is a logical predicate on a system state that should not change its truth value if satisfied by the system execution. An axiomatic basis for the truth of invariants on cyber systems was first proposed by [10]. Most recently invariants are also known to be used in physical power systems [11] and water treatment systems [12]. Invariants are well-understood for cyber processes, but extending them into the physical domains requires some insight. We can arrive at invariant equations based on the physical or chemical properties of the system which can be used as an alternative source of information for the parameter under question.

(vii) Execution Monitors- Some research has been done in implementing execution monitors like the Shadow Security Unit (SSU) [7] in industrial control systems. The SSU is attached in parallel to Remote terminal units (RTUs) or Programmable logic controllers (PLCs), being able to capture and decode the Supervisory control and data acquisition (SCADA) protocol information flow, correlating this information with the status of the physical I/O modules that interface with sensors and actuators on the field. This enables the possibility of implementing a redundant security-checking mechanism that follows a "black box" approach regarding the analysis of the monitored device behavior. Coupling MSDND and a few techniques from SSU along with the ground truths i.e. the invariant equations we can further reduce the bounds on parameters measured in a chemical plant and also more accurately determine the corrupt information path. A ground truth refers to information provided by direct observation as opposed to information provided by inference. The invariant equations are the rules or laws that govern the operation of the plant and are always true.

(viii) Application: Chemical Plant Model- Consider a chemical plant which produces benzene through hydrodealkylation (HDA) of toluene [3]. The below reaction is exothermic and irreversible and takes place in presence of a catalyst. Figure 1 shows the basic process flow diagram of a benzene plant.

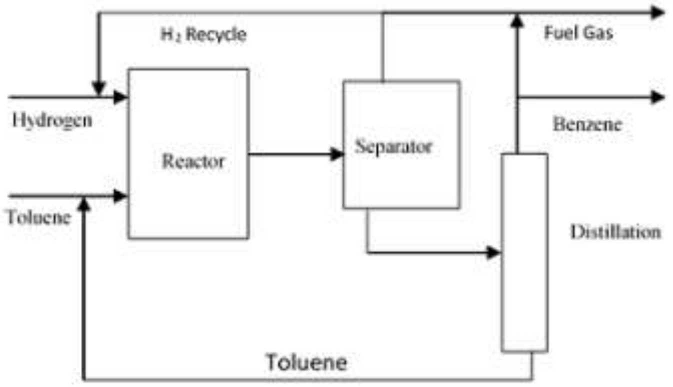


Figure 1 Process flow diagram

$$\text{Toluene} + \text{Hydrogen} \rightarrow \text{Benzene} + \text{Methane} + \text{energy}$$

$$C_7H_8 + H_2 \rightarrow C_6H_6 + CH_4 + \text{energy}$$

Examples of critical information:

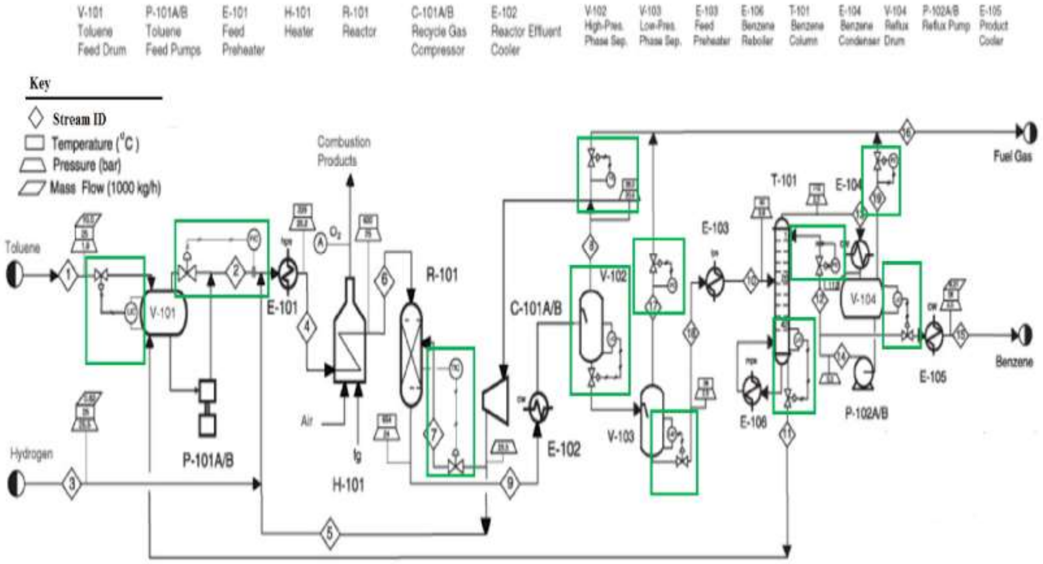


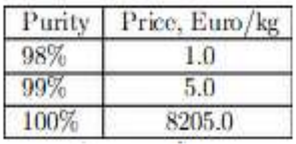
Figure 2 P & ID diagram

3 TYPES OF CYBER PHYSICAL ASSESSMENT

The delivery of products at consistent quality and possibly low cost, the management of plant dynamics affected by material recycling and energy integration, the fulfilment of environmental and safety regulations, and some degree of flexibility to handle fluctuations such as production rate changes (in response to changing market demand) and feed quality are all challenges faced by modern industrial plants. A trustworthy and effective control system must be able to handle all of these tasks. The complexity of modern plants is growing beyond the simple union of a number of unit processes. In terms of information security, an attacker's objective can be to steal data or obstruct software from operating normally. The attacker's objective in the cyber-physical arena is to obstruct the regular operation of control systems. A shell code is created to tell a system to carry out the attacker's intended activities when a buffer overflow is weaponized. Similar to physical exploits, cyber-physical exploits include sending a set of instructions to the target process in the attacker's payload. The instructions chosen depend on the effect the attacker wishes to have on the target process. So what can be done to a process in reality? Cyber-physical attack effects can be divided into three categories. The classes listed are connected, it is true, as harm of one sort might result in damage of another kind. For instance, equipment damage can stop production from happening. Runaway reactions can result in catastrophic safety mishaps and equipment damage. To avoid "over-engineering," however, and to maximise attack impact and reduce attack implementation costs, a clear knowledge of the attack goal is required.

(i) Equipment damage- This category of assaults tries to physically harm infrastructure or equipment (e.g. pipes, valves). Larsen examines various categories of bodily harm. There are two ways to cause equipment damage. overworked machinery. By the conclusion of its anticipated life cycle, every piece of equipment ages or malfunctions. Equipment under prolonged overstress may speed up this process. Wear-off assaults on valves as a result of unsteady process control are an example. The Stuxnet worm's second iteration included this attack method. breach of security perimeters. The second choice is to breach safety regulations, hopefully in a responsible manner. In this manner, Idaho National Laboratory researchers remotely destroyed a power generator. The initial iteration of Stuxnet also included this kind of assault. You can find the piping infrastructure safety limits in.

(ii) Production damage- Rather of damaging the equipment, an attacker could target the manufacturing process to taint the product or increase the cost of production. Three categories can be used to attacks on production. Production volume and product quality. Attacks may be made on the product, its quality, or its rate of production. Every product has its own requirements and market costs for a particular quality. The attacker may render the item useless or lower its value. With increased product purity, a product's price may increase dramatically. The relative pricing for paracetamol are shown in Table 1. As is evident, it can be quite costly to produce a product that falls short of expectations.



Purity	Price, Euro/kg
98%	1.0
99%	5.0
100%	8205.0

Table 1 Paracetamol prices. Source

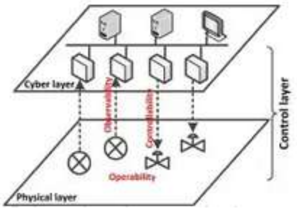


Figure 3 Shows the connections between a cyber-physical system's levels

Operational costs: Once the process has been tuned, the operator's main goal is to maintain the process as close as possible to the conditions that are economically optimal for operation. Every plant has an objective cost function, which influences the operating expenses and is composed of many components. It could result in the purge losing raw materials, the catalyst deactivating too soon, or more energy being used.

Maintenance efforts- By adding to the workload for maintenance, an attacker might affect a production process. Troubleshooting equipment problems and process disturbances is referred to as maintenance. For instance, the rapid opening and closing of a flow valve can result in the harmful cavitation process, which creates vapour cavities in a liquid. Cavitation gradually wears out the valve and causes leaks, necessitating valve replacement. Furthermore, bubbling of a liquid makes process management far more difficult.

(iii) Compliance Breach- To maintain safety and to safeguard the environment, industrial sectors typically undergo stringent regulation. In contrast to attacks, whose impact can be contained within a corporation, non-compliance can result in fines and negative publicity.

Safety- Attacks on environmental and occupational safety would be the most harmful since they might lead to fatal accidents and significant environmental harm. In most circumstances, this kind of attack will result in collateral damage.

Environmental damage- Attacks that result in legal emission limitations being exceeded would be less dramatic.

This may have to do with the quantity and concentration of gaseous emissions, contaminated water, or anything similar. As an illustration, if the effluent from an industrial facility does not adhere to local regulatory norms, the plant may be fined, and persistent violations may result in plant closure. A additional effect could be a bad impact on reputation.

Agreements under contract- Usually, production timetables are meant. Consider the manufacture of vaccines as an illustration. Pressure from the public and politics is frequently generated in response to disease outbreaks. Deliveries that are late may result in contractual penalties and negative publicity.

4 STAGESOFCYBER PHYSICALATTACKS

The ability to fully understand and control a remote process may not be immediately available to an attacker who targets it. Before an attack to succeed, it may need to pass through a number of stages (Fig. 4).

(i) Access – This level most closely resembles classic IT hacking. In order to influence the process, the attacker typically needs code running somewhere in the victim's network, thus they must gain access. Typically, a process network is linked to a business network, a field network, and different regulatory links pertinent to any used hazardous compounds. Process control systems have many of the same requirements as IT systems, in addition to all the data streaming off the control network that feeds corporate and third-party systems. Updates for anti-virus software and patches must enter the network. Moreover, control commands must leave the network and reach field devices. Sending regulatory data to multiple agencies is required. The data must occasionally be sent in real time. These data flows may offer access points to the process network.

(ii) Discovery- Finding information about a plant through documentation is referred to as discovery. It is doubtful that an attacker can accomplish more than annoyance without detailed understanding. The emergency shutdown logic and the pressure relief valves will likely only be used if a process is purposefully overheated, as in the example above. Plants have a great degree of propriety. To develop a talcum powder plant, ten chemical engineers can come up with ten entirely different procedures. Even if they were limited to using the same chemical process, they could still construct the facility differently. They might select various suppliers for the pumps and valves. That would then affect the positioning and size of different pipes and holding tanks. The design of the control loops and how the plant is regulated would change as a result.

(iii) Control- The values of process variables in dynamic systems, such as cyber-physical systems, vary over time in accordance with the principles of physics. Yet, transitioning of a process from one state to another is in most situations not instantaneous and ad-heres to the well-known reality that "things take time".

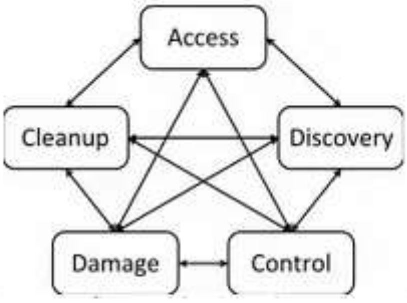


Figure 4 Stages of cyber-physical attacks

The attacker is currently attempting to ascertain the process' dynamic behaviour, which may be expressed in terms of basic differential equations, such as $dy/dt = f(y, u)$, where y and u are coupled through cause-and-effect linkages.

(iv) Damage- Since the attacker has a clear understanding of the process and how to manipulate it, she must choose the best way to accomplish her objectives. There might be a number of conflicting hypotheses. To pick between them, the attacker will need to create some form of metric. It might be a good idea to knock some pumps off the floor until they break, but the economic damage to the target plant might be far less than, for example, poisoning the catalyst in the reactor.

5 CONCLUSION

When the objective of an assault is to conceal crucial information from an operator rather than to steal information, MSDND is a valuable modelling tool. The information can be hidden by making it hard to assess the desired question or by falsifying the actual valuation function to create an invalid valuation, making it MSDND secure and undetectable. This is bad for the system and good for the attacker. A system has fewer vulnerabilities if there are fewer MSDND secure information pathways between the CPS and monitors/observers. Attacks in the CPS that resemble Stuxnet adapt to the system and replay accurate readings despite causing disruptions. By carefully placing physical alarms on the information routes and having a monitoring entity, attacks like this can be partially detected. The invariants, acting as a secondary source of information for the specified parameter, play a crucial role when these attacks interrupt functionality without setting off the alarms. By demonstrating that a system with an MSDND secure path can be converted to a not MSDND secure system utilising the right invariant, we have significantly increased the security and dependability of the system.

6 FUTURE WORK

The primary focus of this study was an attack on a single entity throughout the entire plant. A chemical plant, however, contains a number of processes and associated processing units that can also harm the environment. With the aid of other invariants discussed in the paper, we will therefore examine the following in the future:

- The impact of this attack on other connected processing units, specifically on the distillation column;
- Attacks like the limit switch failure at the BP plant, where information from a sensor was MSDND secure because it lacked valuation functions for the switch's normal and abnormal functioning.

REFERENCES

1. G. Howser and B. McMillin, ”A Modal Model of Stuxnet Attacks on Cyber-physical Systems: A Matter of Trust,” Software Security and Reliability (SERE), 2014 Eighth International Conference on, San Francisco, CA, 2014, pp. 225-234. doi: 10.1109/SERE.2014.36
2. G. Howser and B. McMillin, “A Multiple Security Domain Model of a Drive-by-Wire System,” in Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual. Computer Software and Applications Conference, 2013
3. Turton, Richard, et al. Analysis, synthesis and design of chemical processes. Pearson Education, 2008.
4. C.-J. Liau, “Belief, information acquisition, and trust in multi-agent systems - A modal logic formulation,” Artificial Intelligence, vol. 149, no. 1, pp. 31 – 60, 2003
5. C.-J. Liau, “A modal logic framework for multi-agent belief fusion,” ACM Trans. Comput. Logic, vol. 6, no. 1, pp. 124–174, January 2005.
6. T. M. Chen, “Stuxnet, the real start of cyber warfare?” Network, IEEE, vol. 24, no. 6, pp. 2–3, 2010.
7. T. Cruz et al., “Improving network security monitoring for industrial control systems,” 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015, pp. 878-881.
8. D. Sutherland, “A model of information,” in Proceedings of the 9th National Computer Security Conference. DTIC Document, 1986, pp. 175–183.
9. Framework for Cyber-Physical Systems Release 1.0 May 2016
10. S. Owicki and D. Gries, “An axiomatic proof technique for parallel programs,” Acta Informatica, vol. 6, pp. 319–340, 1976.
11. T. Paul, J. W. Kimball, M. Zawodniok, T. P. Roth, B. McMillin and S. Chellappan, ”Unified Invariants for Cyber-Physical Switched System Stability,” in IEEE Transactions on Smart Grid, vol. 5, no. 1, pp. 112-120,Jan. 2014.
12. S. Adepu and A. Mathur. Using process invariants to detect cyber attacks on a water treatment system. In Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2016 (IFIP AICT series). Springer, 2016.
13. Chemical Facility Anti-Terrorism Standards (CFATS), September 7, 2016.
14. H. W. Thomas, and J. Day, Integrating Cyber Security Risk Assessments into the Process Safety Management Work Process, Poster Session, AiChe 2015 Spring Meeting & 11th Global Congress on Process Safety (ISBN: 978-0-8169-1089-2).
15. Marina Krotofil, Jason Larsen, and Dieter Gollmann. The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS ’15). ACM, New York, NY, USA, 2015, 133-144.
16. US Chemical Safety Board Report, 03/20/2007, america-refinery-explosion, accessed September 7, 2016.