Spring 2017

Cyber-physical security of a chemical plant

Prakash Rao Dunaka

CYBER-PHYSICAL SECURITY OF A CHEMICAL PLANT

by

PRAKASH RAO DUNAKA

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN COMPUTER SCIENCE

2017

Approved by

Dr. Bruce McMillin, Advisor
Dr. Daniel Tauritz
Dr. Alireza Hurson

ABSTRACT

The increasing number of cyber attacks on industries demands immediate attention for providing more secure mechanisms to safeguard industries and minimize risks. A supervisory control and data acquisition (SCADA) system employing the distributed networks of sensors and actuators that interact with the physical environment is vulnerable to attacks that target the interface between the cyber and physical subsystems. These cyber attacks are typically malicious actions that cause undesired results in the cyber physical world, for example, the Stuxnet attack that targeted Iran's nuclear centrifuges. An attack that hijacks the sensors in an attempt to provide false readings to the controller can be used to feign normal system operation for the control system, while the attacker can hijack the actuators to send the system beyond its safety range. Cyber physical systems (CPS) being used in industries such as oil and gas, chemical process plants and the like are termed Industrial Control Systems (ICS). Control system security is aimed at preventing intentional or unintentional interference with the proper operation of ICS. This thesis proposes a process-aware approach with the use of invariant equations based on the physical and chemical properties of the process and a Multiple Security Domain Nondeducibility (MSDND) framework to detect when a sensor signal is being maliciously manipulated. We have taken a benzene production plant as case study to illustrate our approach and its effectiveness in determining the state of the system. A system without any MSDND secure information flows between the CPS and cyber monitors has fewer weaknesses that can be exploited.

ACKNOWLEDGMENTS

First of all, I would like to express sincere gratitude to my academic father Dr. Bruce McMillin for his continuous support for my research, for his guidance, patience, inspiration and immense knowledge. Dr. Bruce has been an amazing advisor. I could not have imagined to have a better advisor and a mentor. Working with him on research has been enjoyable and fruitful.

I would also like to thank my thesis committee: Dr. Daniel Tauritz and Dr. Alireza Hurson for their support and valuable suggestions. My sincere thanks also goes to Dr. Jonathan Kimball and Dr. Joseph Smith for their insightful comments and encouragement. I also want to thank all the people of the Computer Science Department at S&T that have helped me directly or indirectly in so many different ways. I would also like to thank my fellow graduate students in our research group: Uday Kanteti and Anusha Thudimilla for the stimulating discussions and valuable suggestions.

I would like to thank my family: my parents, my brother and my wife for putting immense trust in me and supporting me in every way possible. Thank you is a very small gesture.

Finally, This work was sponsored by a grant from the National Institute of Standards and Technology, Grant Number 60NANB15D236 and with support from the Missouri S&T Intelligent Systems Center and by a grant from the US National Science Foundation under award number CNS-1505610.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Figure Page

LIST OF TABLES

Table Page

NOMENCLATURE

SYMBOL	DESCRIPTION
s_x	A boolean state variable, x is true or false
W	The set of all possible worlds of the system
w	A world of interest
ϕ	A boolean statement that can be evaluated
$\oplus$	Exclusive OR (xor)
SD^i	Represents the security domain with respect to i
$V_x^i\ (\phi)$	A valuation function of boolean x in domain i
$B_i\ \phi$	Modal BELIEF operator
$T_{i,j}\ \phi$	Modal TRUST operator
$I_{i,j}\ \phi$	Modal INFORMATION TRANSFER operator
p	Pressure reading
f	Flow rate reading
t	Temperature reading
l	Level indicator reading
β	β represents the parameter in consideration $\beta \in \{p,t,f,l\}$
F	Feed to the distillation column
B	Bottom output of the distillation column
D	Distillate of the distillation column

1. INTRODUCTION

Our increasing dependence on technology and web-based communication has opened the door for cyber security threats, and the chemical and manufacturing sectors are prime targets. Successful attacks on chemical and other manufacturing facilities and systems can disrupt services and operations and endanger entire populations. With the growing number and sophistication of cyber attacks, securing access to sensitive information and hazardous substances has never been more important or necessary. A chemical plant is typically an industrial process plant that manufactures or processes chemicals on a large scale. Such a plant has an input of a given set of raw materials and performs operations (reactions) on them to produce a desired chemical output along with some residual outputs. These plants use specialized equipment, units and technology in the manufacturing process. Ample amount of attention is focused on safety and operational reliability along with information confidentiality, integrity and availability. Due to a vast and widely spread infrastructure, there is a possibility of security breach either by an intruder or an insider. Physical security is an equally important as cyber security for these infrastructures. Imagine an intruder hacking into the system and changing critical parameters like temperature or pressure in the operational units or even changing the raw material ratios etc. The damage could be catastrophic. The major consequences of a security breach are the following:

- Plant Sabotage/Shutdown
- Intellectual Property Theft
- Physical Hazard/Material Spill
- Overpressure/Expansion/Explosion
- Exposures/Health Issues from Releases beyond Plant Limits

The National Institute of Standards and Technology in its Public Working Group in CPS (NIST) [4] cites major security concerns of a chemical plant as Process Safety and Equipment Safety. These can be maintained by high reliability and security and only cyber-physical 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. The biggest threat to CPS is from the targeted attacks where the attackers have a deep knowledge of the targeted controller and various processes controlled by it. Attackers can take advantage of vulnerabilities in CPS to take control of the system. With physical manifestations in the real world, attacks on CPSs can cause disruption to physical services or create a national disaster. A first generation of research on securing CPSs focused on the IT infrastructure deployed around industrial processes; it was observed that in many cases appropriate network security measures were lacking putting the processes at risk. The dominant suggestion was to adapt state-of-the-art network security solutions such as cryptographic protocols, intrusion detection systems, and firewalls to the industrial application domain. These defenses primarily deal with attacks on the IT infrastructure. This research assumes an attacker like stuxnet that can manipulate actuators to cause impact on the process and hides real process measurements from the control room and/or the process operator. We investigate methods for identifying those readings that have been manipulated. Specifically, we consider attacks generating believable artificial values, that is the values may reside in the lower and upper threshold of the process and presenting that data to the operator to deceive her about the true state of a process. However, these can have an impact on the system in the long term compromising the efficiency of the product or the process. As a cyber physical system requires a tight coupling between the physical and cyber controlling components, it is crucial to ensure that the system is secure for all the cyber and physical processes. Therefore, protecting the CPSs' against cyber attacks is of paramount importance.

Traditional security methods can be applied to protect a CPS against cyber threats or threats imposed by malicious insiders. However, due to the unique characteristics and complexity of a CPS, traditional security models and approaches are not sufficient enough to address the security challenges of a CPS. In order to identify the loopholes in the system, a complementary approach was proposed more than thirty years ago to track and regulate the information flows of the system to prevent secret data from leaking to unauthorized parties. This work was the origin of the theory used in this paper [5].

Information flow security in CPS can lead to particularly complex security partitions. Tools that work well with securing the cyber part of the system rarely work well to keep the physically observable parts of the system from leaking information. Physically locking the fence around the physical parts of the CPS does not protect from a purely cyber attack. Typical electronic or cryptographic solutions do not match specific cases closely enough to handle the cyber-physical interfaces. A persistent attacker with enough time and backing will get in [1].

This thesis examines the current security models in practice for information-flow technology and tries to identify some of the main obstacles of putting them into practice. It also introduces a new information flow security model to minimize the shortcomings of the traditional models. The effectiveness of this model is demonstrated by modeling security aspects of chemical plant.

1.1. MOTIVATION

Critical infrastructure systems, such as electricity, gas and water distribution systems have been subject to changes in the last decades. The need for distributed monitoring and control to support their operations has fuelled the practice of integrating information and communication technology to physical systems. Supervisory Control and Data Acquisition (SCADA) systems have been the first approach to distributed monitoring and control by means of information technology. From a larger perspective, this integration has led to the term “Cyber-Physical System” (CPS), where physical processes, computation and information exchange are coupled together to provide improved efficiency, functionality and reliability. The inherently distributed nature of production and distribution and the incorporation of mass scale sensors and faster management dynamics, and fine-grained adaptability to local failures and overloads are the means to achieve this.

Security in critical systems has historically been an important matter of concern, even when the cyber domain was not present. Attacks in the physical domain can have severe impacts on society and can have disastrous consequences. In the past, most of the security mechanisms were implemented using physical protection. Critical assets were typically located in controlled environments, and this often prevented the occurrence of undesired manipulations. In some cases, however, physical protection is not always fully applicable. Chemical plants, for example, deserve special attention in critical infrastructure protection. The process used in a chemical plant is known, so in thesis more attention has to be focused on integrity attacks rather than confidentiality. In contrast to some other infrastructures where the physical access to the critical assets may be possible to restrict, in chemical plants there are a large number of remote access points difficult to control and protect from accidental or intentional attack.

1.2. THESIS OUTLINE

This thesis is organized as follows, Section II describes related work and some of the key definitions which are used for analysing and modeling the security of a chemical plant, Section III describes the system model that has been taken into consideration i.e., a benzene production plant. A brief overview of the hydrodeaklylation process through which benzene is produced has also been described. Section IV describes the problem statement and the attack model. Section V looks at related efforts. Section VI shows the mathematical analysis of the threats/attacks stated and mitigations for phase-I of the chemical plant and Section VII shows the analysis of the attack on phase-II of the plant. Section VIII presents concluding remarks and results.

2. RELATED WORK

2.1. NONDEDUCIBILITY

2.1.1. Nondeducibility. Nondeducibility (ND) was introduced by Sutherland [5] 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 Nondeducibility secure. However, the partitions must be absolute and the partition is necessarily simplistic. Absolute divisions are conceptually clean, but they do not reflect the real world, i.e. they cannot be extended or combined with other security domains (mostly fixed). 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 the Multiple Security Domain Nondeducibility model.

2.1.2. Valuation Function $V_x^y(\phi)$. $V_x^y(\phi)$ represents a 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.

2.1.3. Security Domain (SD^i) [1]. The event system divides the system into multiple security domains SD^i 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.

2.2. MULTIPLE SECURITY DOMAIN NONDEDUCIBILTIY

A modal technique to model complex security domains, Multiple Security Domain Model Nondeducibility(MSDND)[1][6] was introduced. MSDND can model any system where Sutherland Nondeducibility holds and complex systems where Nondeducibility cannot be determined.

2.2.1. Multiple Security Domain Nondeducibility [1]. There exists some world with a pair of states where one must be true and the other false; i.e., both states must be mutually exclusive (exclusive OR), but an entity i has no valuation function for those states. In security domain SD^i, i simply cannot know which state is true and which is false.

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

it can also be written as,

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

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 Nondeducibility can be reduced in polynomial time to MSDND[1].

Computer security tools work best when secure domains are cleanly nested inside less secure domains like a Medieval castle with its outer walls and interior keep. This model serves us well for most uses, but breaks down when applied to CPS. Because CPS typically need to secure both data and information flow, the security domain picture gets complicated. We need tools that can model the cyber and physical components of CPS.

MSDND is also being used in modelling security for air traffic control systems, vehicle platoon systems and few other critical infrastructures. MSDND security model when coupled with invariants shows a promising way improving the resiliency of CPS.

2.3. BELIEF, INFORMATION TRANSFER AND TRUST (BIT) LOGIC

BIT logic was introduced by Liau [7] [8] 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.

- $T_{i,j}\ \phi$ defines the trust i has in a report from j that ϕ is true
- $B_i\ \phi$ defines the belief by i that ϕ is true; it does not matter if ϕ is true or not, i believes it to be true
- $I_{i,j}\ \phi$ defines the transfer of information directly from one agent to another, that is j reported to i that ϕ is true

2.4. 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 [9]. Most recently invariants are also known to be used in physical power systems [10] and water treatment systems [11]. 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. More on invariants is discussed in the further sections.

2.5. EXECUTION MONITORS

Some research has been done in implementing execution monitors like the Shadow Security Unit (SSU)[12] 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 information flow attributed to the Supervisory control and data acquisition (SCADA) protocol, 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.

3. SYSTEM MODEL

A distinction has been made between embedded systems that use electronic and physical components developed separately by experts in their respective domains, and true cyber-physical systems where expertise in both domains must be combined to advance the state of the art. The chemical industry spends a huge amount of resources to ensure the safety of its personnel, customers, and surrounding community. The increase in cyber attacks on chemical plants demands to device new cyber-physical security measures and frameworks. For example, during summer 2011, a cyber attack named 'Nitro' caused several casualties among targeted companies. Some of them are part of the defense sector and majority of them belong to the chemical industry. These companies are spread around the world, from the United States to the United Kingdom and through Asia. The malware which was used, labeled with the name 'PoisonIvy', had the clear intention to steal information. Another attack was the stuxnet attack that targeted Iran's nuclear centrifuges. In this section a detailed mathematical security analysis of a benzene production plant is shown.

3.1. BENZENE PRODUCTION PLANT

A benzene production plant produces benzene through hydrodealkylation (HDA) of toluene [2]. The below reaction is exothermic and irreversible and takes place in presence of a catalyst. Figure 3.1 shows the basic process flow diagram of a benzene plant.

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

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

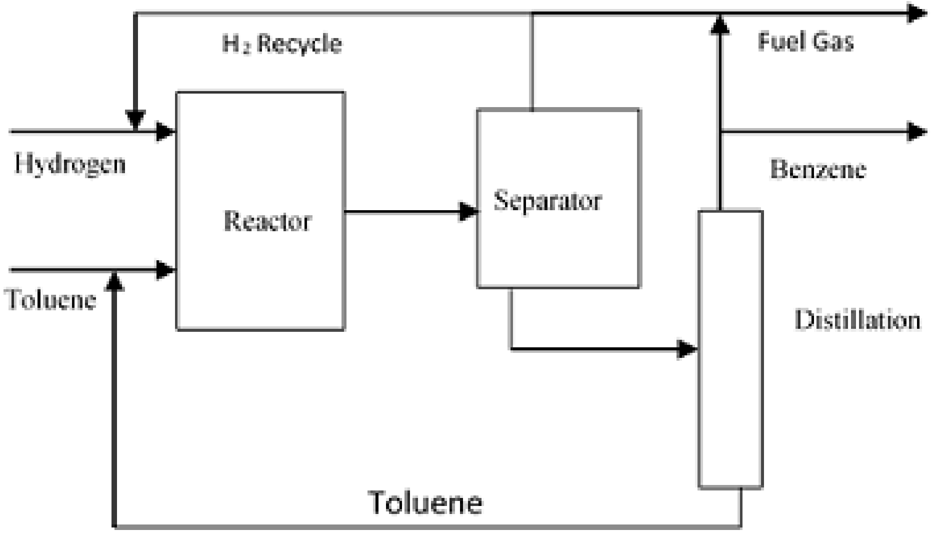

Figure 3.1: Process Flow Diagram

3.2. HYDRODEALKYLATION

HDA Process [2]: The HDA process begins with mixing fresh toluene with a stream of recycled unreacted toluene, the mixing is achieved in a storage tank. The toluene is then pumped to combine it with a stream of mixed hydrogen and fresh hydrogen gas. The mixture of hydrogen and toluene is preheated before it is introduced to the heater or furnace. In the furnace the stream is heated to 600^o C, the reaction temperature, then introduced into the reactor. The reactor is where the main reaction happens.

$C_7H_8 + H_2 \rightarrow C_6H_6 + CH_4 +$ energy

The products are then cooled and introduced into a pair of separators that separate the unreacted hydrogen. A portion of the unreacted hydrogen is compressed and recycled back to the feed and the reactor. The products leaving the separators are then heated before being introduced into a distillation column, where toluene is separated from the stream and recycled to the feed. This allows for greater conversion. Then further fractionation separates methane and toluene from the benzene product.

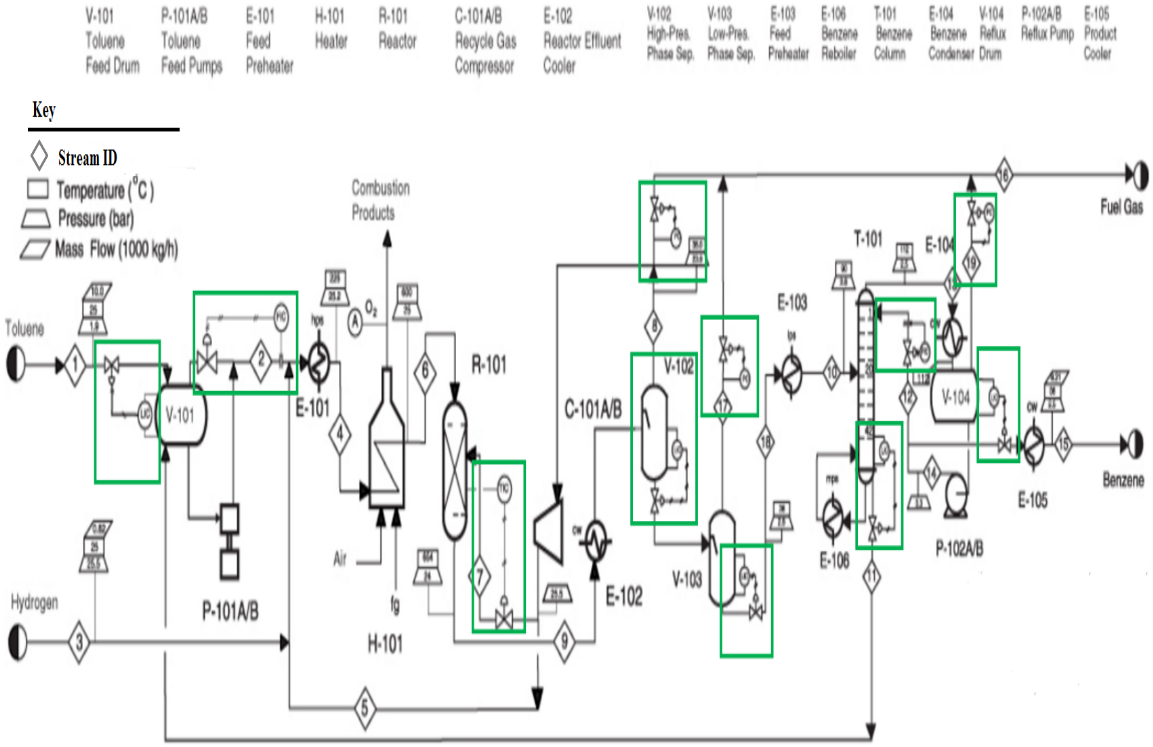

Figure 3.2: P&ID [2]

The mixture of toluene and hydrogen is preheated to get a vaporized mixture and sent into heater H-101 (Figure 3.2) to heat the mixture to 600^o c and this stream is then fed to the reactor R-101 (Figure 3.2) which is filled with catalysts where the reaction takes place, the reaction being exothermic, a constant stream of hydrogen through stream 7 (Figure 3.2) is fed to the reactor to control the temperature. If the temperature of the reactor is not properly regulated, it might lead to bad quality of benzene, inefficiency in converting toluene to benzene, can damage the connected processing units and in the worst case the reactor could blow up.

Examples of critical information in the benzene plant are as follows:

- Temperature readings: In the benzene process, the feed to the reactor is substantially hotter than the rest of the process and is crucial to the operation of the process. In addition, the reaction is exothermic, and the reactor effluent temperature must be carefully monitored.

- Pressure readings: The pressures of the streams to and from the reactor in the benzene process are also important. The difference in pressure between the two streams gives the pressure drop across the reactor. This, in turn, gives an indication of any maldistribution of gas through the catalyst beds.

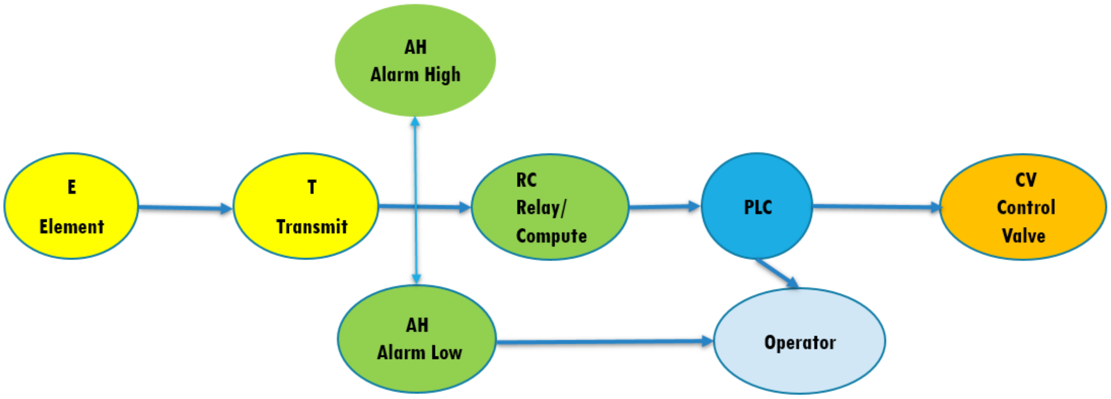

Figure 3.3: Skeleton of an information path

Different types of information flow paths in the plant are; flow information, pressure information, temperature information, and level information (Figure 3.3). Following are a few of the information flow paths at physical infrastructure in the benzene plant (Figure 3.2). Each information path is enclosed within a box, the detailed view of the individual components of each information path look like components in the Figure 3.3. Here, the operator need not necessarily be a human, it can also be another attached control process.

- Toluene Feed Drum (V-101): level and pressure information paths

- High pressure phase separator (V-102): level and pressure information paths

- Low pressure phase separator (V-103): level and pressure information paths

- Reflux Drum (V-104): level and pressure information paths
- Reactor (R-101): temperature information path
- Distillation column (T-101): temperature, flow and level information paths

4. PROBLEM STATEMENT

The biggest threat to CPS is from the targeted attacks where the attackers have a deep knowledge of the targeted controller and various processes controlled by it. This thesis models stuxnet-like [13] attacks in a chemical plant using MSDND and BIT logic to locate points of vulnerability. The major focus of these attacks is hiding critical information rather than stealing it. Once into the system, these viruses stay dormant and learn the behaviour of the system and then corrupt the information. There are two basic ways to hide this information: make it impossible to evaluate the desired question ϕ , or to disrupt the actual valuation function to return an unreliable valuation of the question ϕ. It is bad for the system if it is MSDND secure with respect to integrity since by the definition of MSDND the observer does not have valuation functions for the states of the system; i.e., the observer cannot determine which state is true and which state is false (he cannot determine if there is any change in information). However, it is good for the system with respect to confidentiality, because any observer will not be able to know any changes made to the system.

4.1. ATTACK MODEL

Let us assume a stuxnet-like attack on the PLC in the pressure information path related to stream 8 in Figure 4.1 of a benzene plant. The process of producing benzene takes place at high temperatures and also the reaction taking place in the reactor is highly exothermic. This is one of the critical information path because the hydrogen(H_2) gas is compressed and pumped back to the reactor to regulate the temperature of the reactor through this stream. This stream also contains methane (CH_4), a highly combustible gas. A particular pressure is used to separate CH_4 and

H_2 into two streams. CH_4 is sent out as a fuel and H_2 to the reactor to regulate temperature. Imagine the catastrophic damages that can be caused by manipulating the pressure of H_2 in a way that it has least impact in regulating the temperature of the reactor or pumping CH_4 into the reactor causing combustion and possibly blowing the reactor.

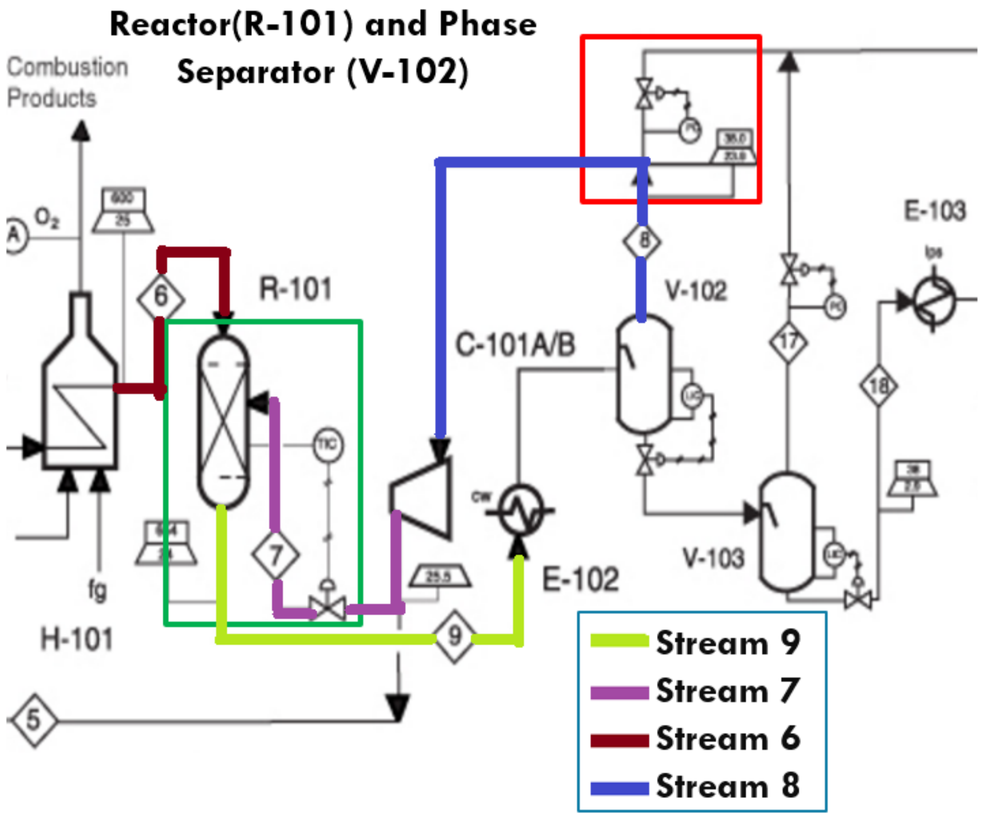

Figure 4.1: Components of interest

We divide the information path into several security domains as shown in the Figure 4.2. Each of these security domains are independent of each other and are self contained. Table 4.1 shows the entities contained in each security domain. Each of the information path for several other parameters like temperature t, pressure p, flow rate f, level indicator l in the chemical plant are divided into similar security domains.

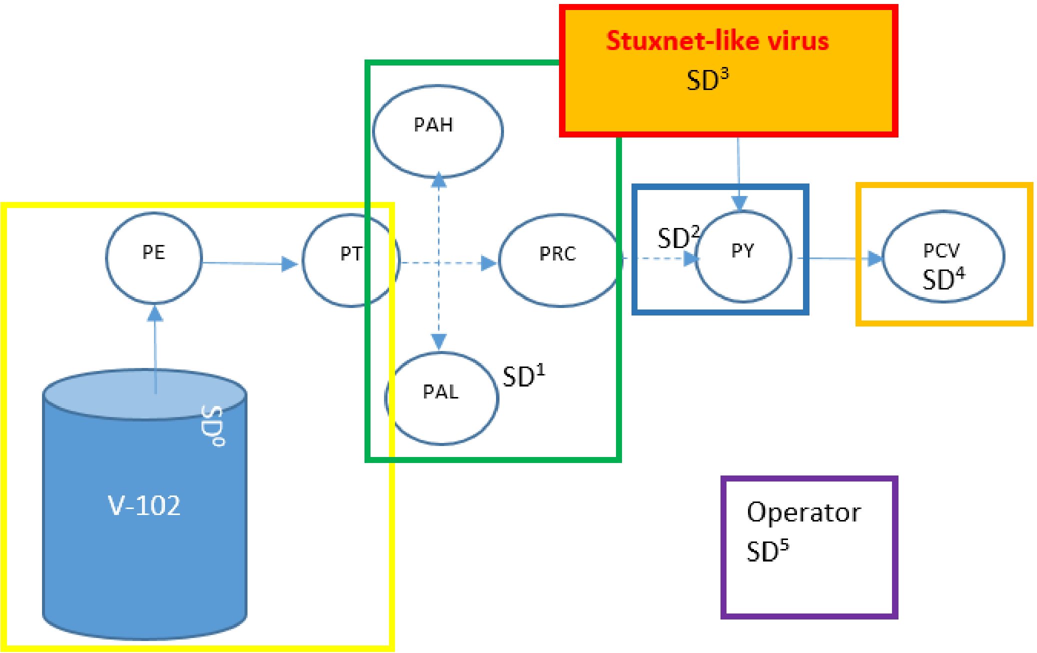

Figure 4.2: Security Domains

Table 4.1: Security Domains

Domain	Unit
SD^0	Physical unit(sensor)
SD^1	Relay/Computational unit
SD^2	PLC
SD^3	Stuxnet-like virus
SD^4	Control Valve
SD^5	Operator

5. RELATED EFFORTS

As mentioned earlier, NIST [4] has produced an extensive framework document including cybersecurity requirements for several infrastructures. The US Department of Homeland Security CFATS standards [14] describe processes for security assessment of chemical plants. A number of international standards have sprung up illustrating the importance of security and cybersecurity for ICS. This paper provides a mathematical technique for both assessment, and guidance for mitigation of cyber security attacks. A complementary approach to ours based on learning was proposed by [15] to determine anomalous behavior within a plant. Both approaches treat information flow as a key element.

Similar work has been carried out in [1], but that work is limited to accepting commands from a single source and it does not cover all the possible state transitions in the system. The major drawback is the inability to represent the state transitions and interactions in a concise way and our work covers this by segregating the system into multiple security domains. These security domains contain multiple states and the security issues between the state interactions are considered.

6. SECURITY OF CHEMICAL PLANT - PHASE-I

In this section a detailed mathematical analysis of the impact of stuxnet-like attack on the pressure information path (stream 8 in Figure 4.1) on phase-I of the chemical plant is shown.

6.1. MSDND ANALYSIS OF PRESSURE p OF THE ATTACK MODEL

Stuxnet-like attacks have the capability to hide critical information or falsify the critical information and produce information that it desires. This section presents a detailed analysis of how MSDND can be applied along with the invariant equations derived from the chemical and physical processes of the plant to make the system more secure and difficult to break. MSDND analysis from integrity standpoint is considered here because of the assumption that the process of the plant is already known to the attacker and thus the process is not confidential (stuxnet-like viruses learn the system behavior, that means they are already aware of the process to some extent or whole).

6.1.1. MSDND Under Normal Working Conditions. The following are some of the critical assumptions taken into consideration while modeling the security of the chemical plant:

1. under normal working conditions every sensor and actuator report accurate data.
2. none of the alarms are faulty
3. operators are not corrupt

Theorem 1. *The parameter readings p, t, f, l in the chemical plant are not MSDND secure under normal conditions.*

Proof. Under normal conditions, the data received by the PLC, control unit, operator is correct and they operate as intended, giving the desired results. Here, the chemical plant functions normally and the reaction happens as usual. The information path is divided into security domains as shown in Figure 4.2 and in Table 4.1.

Let β denote a parameter in consideration. ($\beta \in \{p, t, f, l\}$ Let p be the correct pressure range for normal working conditions of the system. p $\oplus$ ∼p is always true [either pressure is in the desired range or not].

1. $\beta \oplus \sim \beta =$ true;

2. $S_\beta \oplus S_{\sim\beta} =$ true; system is either normal or not normal

3.

Domain	Valuation	Correctness
SD^0	$V^0_\beta(\sim \beta)$	True
SD^1	$V^1_\beta(\sim \beta)$	True
SD^2	$V^2_\beta(\sim \beta)$	True
SD^3	$V^3_\beta(\sim \beta)$	True
SD^4	$V^4_\beta(\sim \beta)$	True
SD^5	$V^5_\beta(\sim \beta)$	True

4. The valuations V^i_β are correctly evaluated for all the domains, $i \in$ {0,1,2,3,4,5}

5. MSDND(ES) $= \exists$ w $\in$ W $\vdash [\,(\,S_\beta \oplus S_{\sim\beta}\,)\,] \wedge [\,\mathrm{w} \models (\,\exists\, V^i_{\sim\beta}(\,\mathrm{w}) \;\wedge \exists\, V^i_\beta(\,\mathrm{w}\,)\,)]$ and $i \in$ {0,1,2,3,4,5}

From the above proof we can see that there exist valuations for the a given parameter reading β in all the security domains, which contradicts the second part of MSDND definition. Therefore the parameter reading β is not MSDND secure under normal conditions. □

6.1.2. MSDND Under Attack - Without Alarms. The next theorem shows what happens in case of an attack where the computational unit (PLC) is compromised and the pressure control valve can be operated in such a way that pressure is altered without being observed.

Theorem 2. *The pressure reading p is MSDND secure under attack in the absence of alarms.*

If the system is infected and a stuxnet-like virus is in the recording phase, all messages are recorded and then relayed.

Proof. The pressure is not normal, ∼p = true. During the attack phase, the virus in SD^3 receives sensor reports and always reports to the PLC in SD^2 that the pressure is within desired range. The virus has corrupted the information path between the sensor and the PLC. Refer to Figure 6.1 to clearly understand the proof.

1. $\mathrm{p} \oplus \sim\mathrm{p} = \mathrm{true}$;
2. $S_p \oplus S_{\sim p} = \mathrm{true}$; system is either normal or not normal
3. $\sim\mathrm{p} = \mathrm{true}$; pressure is not normal
4. $\mathrm{w} \models V_p^0(\mathrm{w}) = \mathrm{false}$; the reading is not normal the valuation function in world w is false
5. $I_{3,0} \sim\mathrm{p}$; sensor reports problem to virus
6. $B_3 I_{3,0} \sim\mathrm{p}$; virus believes sensor report
7. $T_{3,0} \sim\mathrm{p}$; virus trusts the sensors
8. $B_3 I_{3,0} \sim\mathrm{p}; \wedge T_{3,0} \sim\mathrm{p} \rightarrow B_3 \sim\mathrm{p}$; virus believes the reading
9. $I_{2,3}\mathrm{p}$; virus always reports readings are correct

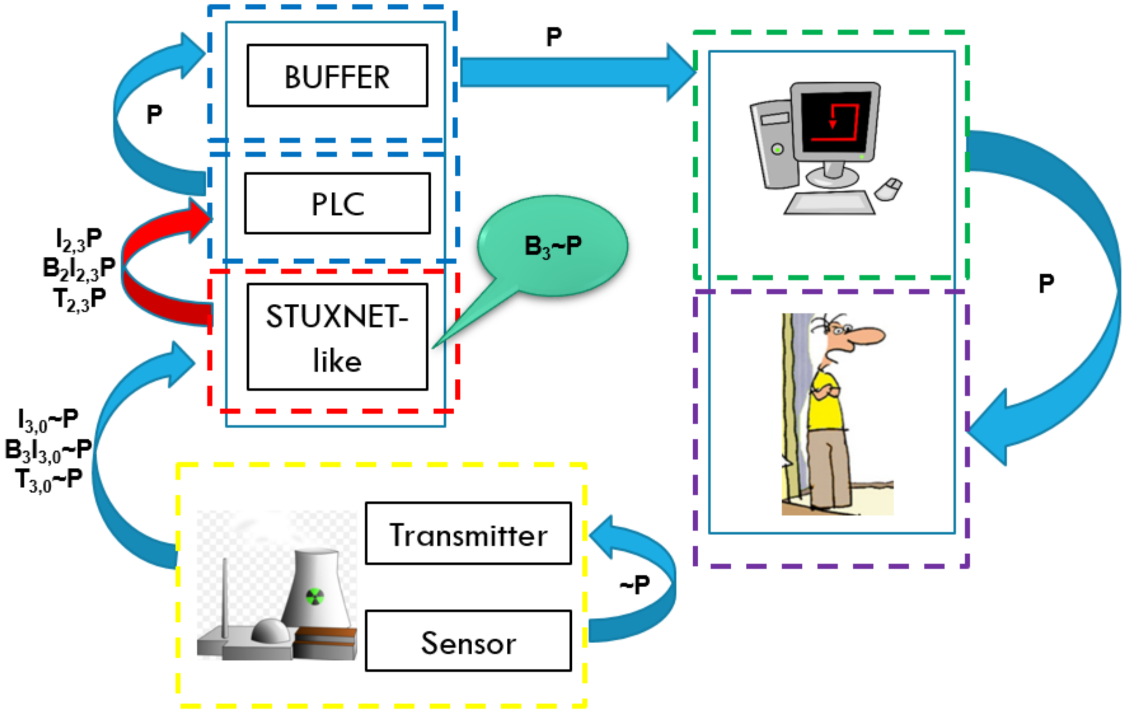

Figure 6.1: Information Flow when p is not normal

10. $B_2 I_{2,3}$p; PLC believes interface report

11. $T_{2,3}$p; PLC trusts reports

12. $B_2 I_{2,3}\text{p} \wedge T_{2,3}\text{p} \rightarrow B_2$p; PLC believes readings are correct

13. w $\models V_p^2(\text{w}) = \text{true}$; V_p^2(w) always returns true

$$\text{MSDND(ES)} = \exists\ \text{w} \in \text{W} \vdash [\,(\,S_p \oplus S_{\sim p}\,]\ \wedge [\,\text{w} \models (\ \nexists\ V_{\sim p}^2(\,\text{w}\,)\ \wedge\ \nexists\ V_p^2(\,\text{w}\,)\,)\,]$$

Since $B_2 I_{2,3}\text{p} \wedge T_{2,3}\text{p} \rightarrow B_2$p, the PLC believes the lie told in step 9 in all cases. Therefore, unknown to entities in SD^2, V_p^2 (w) and $V_{\sim p}^2$ (w) cannot be evaluated. Therefore p is MSDND secure from SD^2. □

6.1.3. MSDND Under Attack With Alarms - p Is Beyond Threshold.

Corollary 2.1. *In presence of high and low pressure alarms placed strategically on the information path before the PLC, the pressure reading p beyond the threshold will trigger the alarm making the information not MSDND secure.*

Proof. In this situation, the pressure p is not normal. Refer Figure 6.2 to clearly understand the proof.

1. p $\oplus$ $\sim$p = true;

2. $S_p \oplus S_{\sim p}$ = true; system is either normal or not normal

3. $\sim$p = true; pressure is not normal

4. w $\models V_p^0$(w) = false; the reading is not normal the valuation function in world w is false

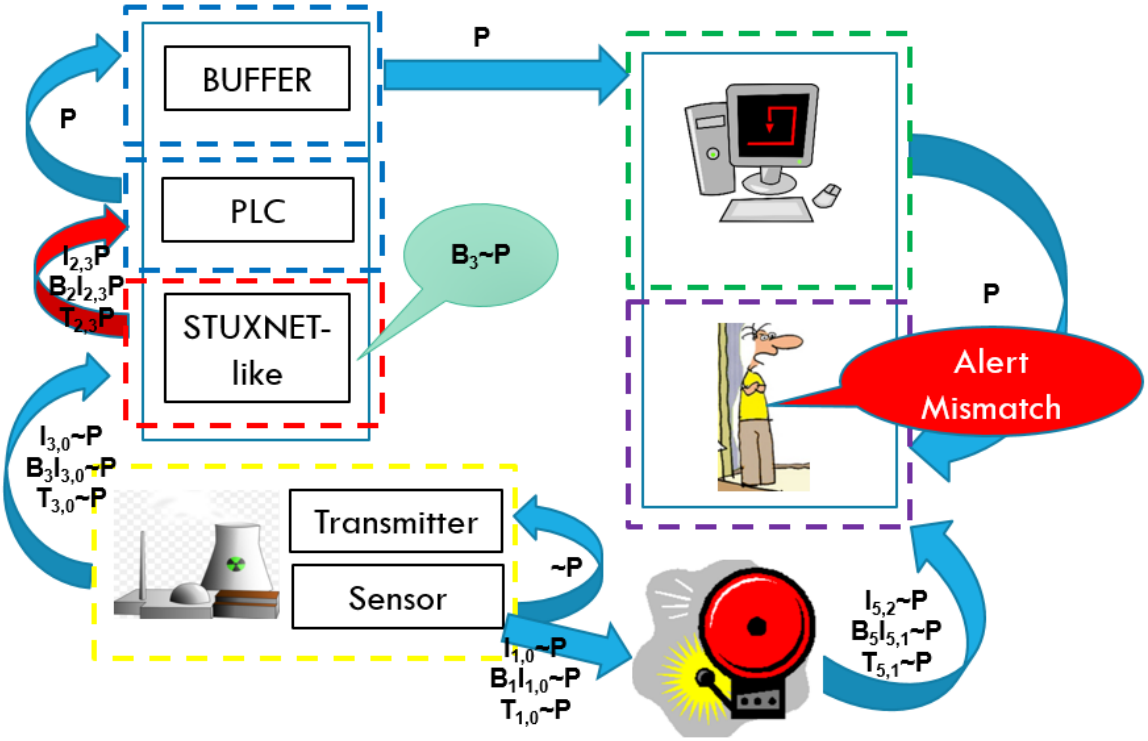

Figure 6.2: Information Flow when p is not normal and alarm triggers

5. $I_{1,0}$ ∼p; sensor reports problem to alarm/control room

6. $B_1 I_{1,0}$ ∼p; alarm believes sensor report

7. $T_{1,0}$ ∼p; alarm trusts the sensors

8. $B_1 I_{1,0}$ ∼p ∧ $T_{1,0}$ ∼p → B_1 ∼p; alarm believes the reading

9. $I_{5,2}$ ∼p; alarm triggers

10. $B_5 I_{5,1}$ ∼p; operator believes alarm

11. $T_{5,1}$ ∼p; operator trusts alarm

12. $B_5 I_{5,1}$ ∼p; ∧ $T_{5,1}$ ∼p → B_5 ∼p; operator believes readings are correct but not normal

13. w $\models V^5_{\sim p}(\mathrm{w}) =$ true; $V^5_{\sim p}(\mathrm{w})$ always returns true

$$\mathrm{MSDND(ES)} = \exists\ \mathrm{w} \in \mathrm{W} \vdash [\,(\,S_p \oplus S_{\sim p}\,)\,] \wedge [\,\mathrm{w} \models (\,\exists\ V^5_{\sim p}(\,\mathrm{w}) \ \wedge\ \nexists\ V^5_p(\,\mathrm{w})\,)\,]$$

Since $B_5 I_{5,1}$ ∼p ∧ $T_{5,1}$ ∼p → B_5 ∼p. Therefore, in SD^5, $V^5_{\sim p}(\mathrm{w})$ can be evaluated. The operator knows that pressure is not in desired range. Therefore p is not MSDND secure from SD^5. □

Remark: If there is a physical alarm on the information path and an entity i looks because he or she does not trust the electronic reports, the pressure of the vessel is not MSDND secure with respect to any entity that checks the physical alarm. But what happens if the agents believe the cyber reports from the attacker and there is no alarm as a backup? In this case, the attacker uses the implicit trust that the operators have in their monitoring systems to introduce MSDND into the attack and to hide the attack. This allows the attacker to disrupt the flow of critical information, i.e. the pressure of the vessel is outside of optimal range. The CPS has been compromised.

While designing a typical chemical plant, engineers also consider a few heuristic rules to determine the dimensions, orientations, locations etc of the physical instruments in the plant. The physical properties of these instruments along with few readings from the actual reaction usually determine the bounds (low/high) on the alarms for a given parameter like temperature, pressure, flow rate etc. These parameters should be in the optimal range for the plant to work safely and properly, and usually there is only one source (sensors) of information for these readings. Combining these readings along with ground truths; i.e., the invariants, we can determine if there is a cyber attack in the plant or if there is a faulty sensor. The following theorems and proofs help us in understanding the critical role invariants play in making the system secure.

Some of the invariants for the benzene plant are [2]:

- The overall material balance for the benzene process
  total input = total output

- The conversion per pass of toluene to benzene

- Temperature of the reactor
  $t_{R-101} = t_{s6} + t_{reaction} - t_{s7}$

6.2. MSDND ANALYSIS OF TEMPERATURE t AT THE REACTOR

Interaction between reactor (R-101) and Phase separator (V-102): During the normal operation of the system, since the reaction is exothermic, H_2 is continuously pumped back from V-102 to the reactor to regulate the temperature for reactor. There are several factors influencing the temperature of the reactor; however, considering only the temperature parameter related to various streams, the following invariant gives us the net temperature of the reactor.

$$t_{R-101} = t_{s6} + t_{reaction} - t_{s7} \tag{6.1}$$

t_{R-101} is in desired range iff t_{s6}, $t_{reaction}$, t_{s7} are in desired ranges.

Note: The security domains on the temperature information path are similar to that of the pressure information path in Figure 4.2.

6.2.1. MSDND Under Normal Working Conditions.

Theorem 3. *The temperature reading t is not MSDND secure if all the components of the systems are working normally.*

Proof. $t_{R-101} \oplus \sim t_{R-101}$ is always true [temperature of the reactor is either in the desired range or not].

1. $t_{R-101} \oplus \sim t_{R-101} = \text{true}$
2. $S_t \oplus S_{\sim t} =$ true; system is either normal or not normal
3.

Domain	Valuation	Correctness
T-101	V_t^{r-101}(∼t)	True
Stream 6	V_t^{s6}(∼t)	True
Stream 7	V_t^{s7}(∼t)	True
Reaction	$V_t^{reaction}$(∼t)	True

4. $\text{MSDND(ES)} = \exists\ \text{w} \in \text{W} \vdash [\,(\,S_t \oplus S_{\sim t}\,)\,]\ \wedge [\,\text{w} \models (\,\exists\ V^i_{\sim t}(\text{w})\ \wedge\ \nexists\ V^i_t(\text{w})\,)\,]$
5. Clearly, if all the devices are working correctly, the valuations V_p^i, V_t^i of the domains can be evaluated which contradicts the second part of the MSDND definition.

Therefore the system is not MSDND secure under normal working conditions. □

Note: We can deduce the valuation of any one variable if we know the other three variables [ignoring external factors].

6.2.2. MSDND Under Attack With Alarms - *t* Is Beyond Threshold.

Under attack, the pressure is not normal, which implies the H_2 gas that is pumped to R-101 to regulate the temperature is not in desired quantities, as a result the temperature of R-101 increases which might cause damage. However, the temperature control valve on R-101 tries to regulate the H_2 to maintain the desired temperature, but if H_2 being pumped is not enough (due to attack on V-102 that produces H_2) R-101 cannot maintain its temperature. The operator monitoring cannot deduce if the rise is temperature is due to lack of H_2, faulty valve system, high temperature of input feed from stream 6 or faulty reaction. This would imply that the attack is MSDND secure. With the addition of the invariant (6.1), however, we get a different result.

Theorem 4. *The temperature reading t is not MSDND secure when there is an attack on the connected pressure information path in presence of alarms.*

Proof. Assuming the following equation for temperature measurements. Refer Figure 6.3 to clearly understand the proof.

$t_{R-101} = t_{s6} + t_{reaction} - t_{s7}$ ($t_{reaction}$ is constant assuming the behavior of the reaction won't change) t_{R-101} is out of range $\Rightarrow$ t_{s6} or t_{s7} is faulty or both are faulty or the sensor at t_{R-101} is faulty.

Suppose t_{s7} is faulty:

1. t $\oplus$ ∼t = true
2. $S_t \oplus S_{\sim t}$ = true; system is either normal or not normal
3. ∼t = true; temperature is not normal

4. w $\models V_t^0$ (w) = false; the reading is not normal, the valuation function in world w returns false

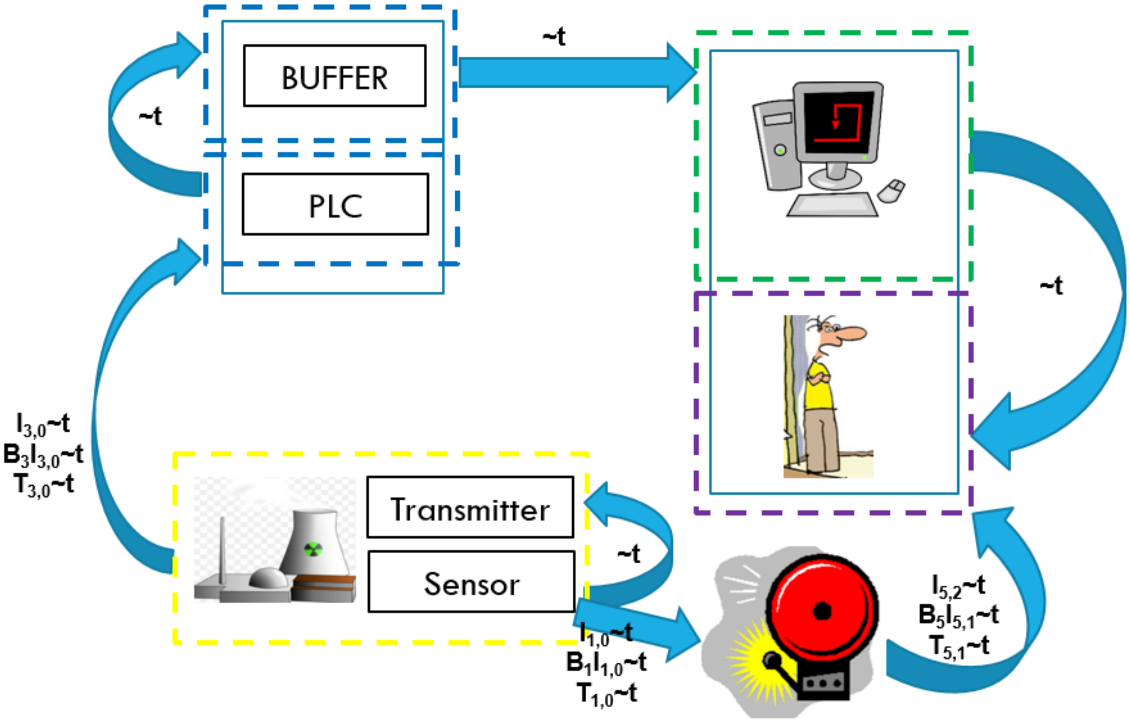

Figure 6.3: Information flow when t is not normal

5. $I_{1,0}$ $\sim$t; sensor reports problem to alarm/control room

6. $B_1I_{1,0}$ $\sim$t; alarm believes sensor report

7. $T_{1,0}$ $\sim$t; alarm trusts the sensors

8. $B_1I_{1,0}$ $\sim$t $\wedge$ $T_{1,0}$ $\sim$t $\rightarrow$ B_1 $\sim$t; alarm believes the reading

9. $I_{5,2}$ $\sim$t; alarm triggers

10. $B_5I_{5,1}$ $\sim$t; operator believes alarm

11. $T_{5,1}$ $\sim$t; operator trusts alarm

12. $B_5I_{5,1}$ $\sim$t $\wedge$ $T_{5,1}$ $\sim$t $\rightarrow$ B_5 $\sim$t; operator believes readings are correct but not normal

13. w $\models V^5_{\sim t}$(w) = true; $V^5_{\sim t}$(w) always returns true

$$\text{MSDND(ES)} = \exists\ \text{w} \in \text{W} \vdash [\,(\,S_t \oplus S_{\sim t}\,)\,] \wedge [\,\text{w} \models (\,\exists\, V^5_{\sim t}(\,\text{w}) \wedge \nexists\, V^5_t(\,\text{w})\,)\,]$$

Since $B_5 I_{5,1}$ ∼t ∧ $T_{5,1}$ ∼t → B_5 ∼t. Therefore, in SD^5, $V^5_{\sim t}$(w) can be evaluated. The operator knows that temperature is not in desired range. Therefore t is not MSDND secure from SD^5. □

Similarly, the temperature t is not MSDND secure from SD^5 when t_{s6} is faulty or both t_{s6} and t_{s7} are faulty or the sensor at R-101 is faulty or all three are faulty. However, we can infer that even though the temperature information is not MSDND secure in case of attack, the origin of the attack cannot be deduced.

Remark: What if the pressure valve is manipulated in such a way that the temperature of the reactor lies between the desired limits, i.e. the alarm will not trigger? Temperature being in the desired range indicates that the reaction is as per the process. However, we can still see that there is something wrong in the pressure information path due to the presence of the virus. Can we detect it? The alarms are very coarse and do not detect subtle attacks that compromise the product quality and process efficiency.

6.2.3. MSDND Under Attack - *t* Is Within Limits.

Theorem 5. *The temperature reading t is MSDND secure when the actual temperature is not normal but the reading is normal.*

Proof. In this world the actual temperature t is not normal, but the readings are normal (the system operates within the broad threshold limits of the alarms, Refer Figure 6.4).

1. t $\oplus$ ~t = true

2. $S_t \oplus S_{\sim t}$ = true; system is either normal or not normal

3. ~t = true; temperature is not normal

4. w $\models V_t^0$ (w) = true; the reading is normal in this world

5. $I_{1,0}$t; sensor report temperature is normal/fine to alarm/control room

6. $B_1 I_{1,0}$t; control room monitor believes sensor report

7. $T_{1,0}$t; control room monitor trusts the sensor

8. $B_1 I_{1,0}\text{t} \wedge T_{1,0}\text{t} \rightarrow B_1$t; control room monitor believes the reading

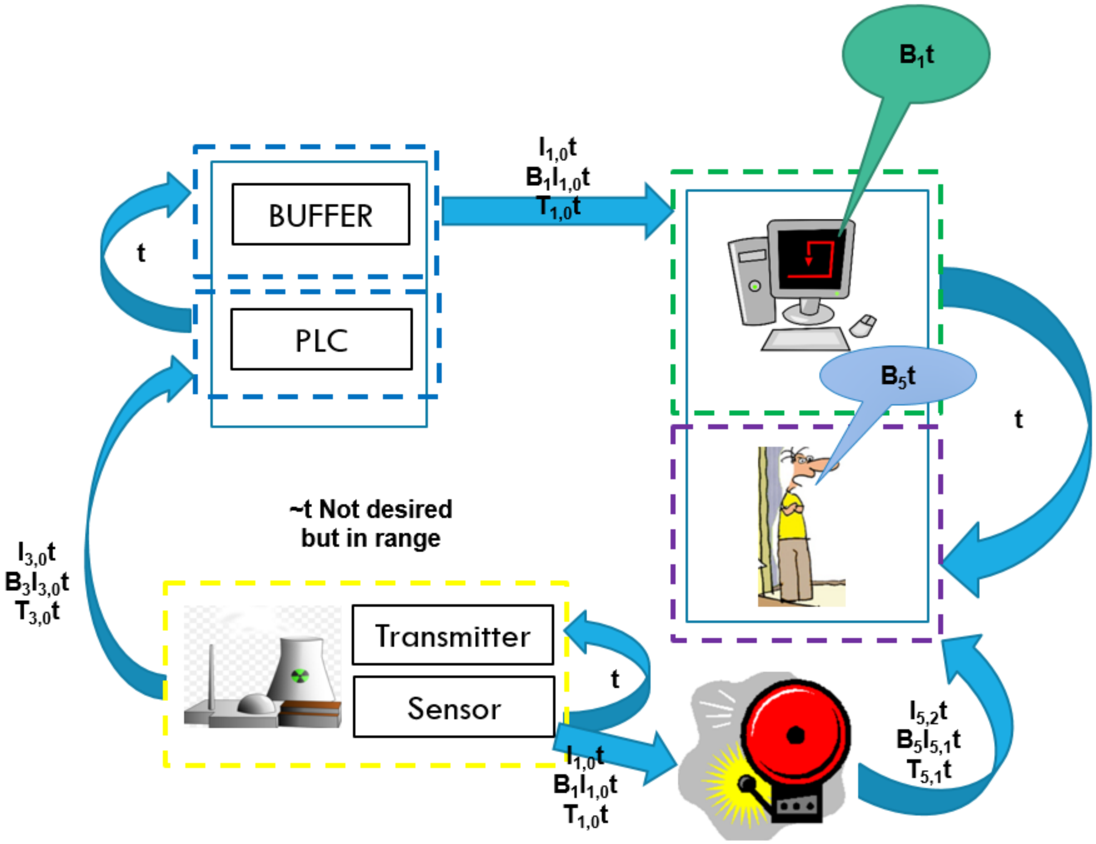

Figure 6.4: Information Flow when t is normal

9. $I_{5,1}$t; operator observes the monitor

10. $B_5 I_{5,1}$t; operator believes monitor

11. $T_{5,1}$t; operator trusts monitor

12. $B_5 I_{5,1}\text{t} \wedge T_{5,1}\text{t} \rightarrow B_5$t; operator believes readings are correct and normal

13. w $\models V_t^5(\text{w}) = \text{true}$; $V_t^5(\text{w})$ always returns true

MSDND(ES) $= \exists \text{ w} \in \text{W} \vdash [\,(\,S_t \oplus S_{\sim t}\,)\,] \wedge [\text{w} \models (\,\nexists\, V_{\sim t}^5(\,\text{w}) \,\wedge\, \nexists\, V_t^5(\,\text{w})\,)\,]$

The operator believes that temperature is in desired range. However, unknown to entities in SD^5 (operator), V_t^5(w) and $V_{\sim t}^5$(w) cannot be evaluated. Therefore, t is MSDND secure from SD^5. The temperature reading is consistent with both working and non-working states of the system. This proof clearly shows that even though there is a problem in the connecting system, if it somehow manages to operate within the range it can go undetected. □

6.2.4. MSDND Analysis Of Temperature *t* In Presence Of Invariant.

For a reaction between reactants A and B to produce C.

$$aA + bB \rightarrow cC \tag{6.2}$$

the reaction rate is found to be of the form[16]

$$r = K(T)[A]^m[B]^n \tag{6.3}$$

Here k(T) is the reaction rate constant that depends on temperature. [A] and [B] are the molar concentrations of substances A and B in moles per unit volume of solution, assuming the reaction is taking place throughout the volume of the solution.

The Arrhenius equation gives the quantitative basis of the relationship between the activation energy and the reaction rate at which a reaction proceeds. The rate constant is then given by

$$K = Ae^{E_a/RT} \tag{6.4}$$

$$r = Ae^{E_a/RT}[A]^m[B]^n \tag{6.5}$$

where E_a is the activation energy, and R is the gas constant and A is the frequency factor.

So, if the threat goes undetected for a long period of time and since the rate of the reaction is exponentially proportional to the temperature, it might cause sudden failure to the system with adverse consequences.

However, when we take the invariant (6.1) into consideration, the operator now has two valuation sources for the same parameter and s/he can compare and come to a consensus. If the values from the invariant and the sensor match, the system is working correctly and if both are different, there is something wrong in the system.

Theorem 6. *The temperature reading t is not MSDND secure when the actual temperature is not normal and the reading is normal if the invariant (6.1) is taken into consideration.*

Proof. Let us assume that t_{s6} and $t_{reaction}$ are correct. Let the invariant $t_{R-101} = t_{s6}$ + $t_{reaction}$ – t_{s7} be in a security domain SD^6 (Refer Figure 6.5)

1. t ⊕ ∼t = true

2. $S_t \oplus S_{\sim t}$ = true; system is either normal or not normal

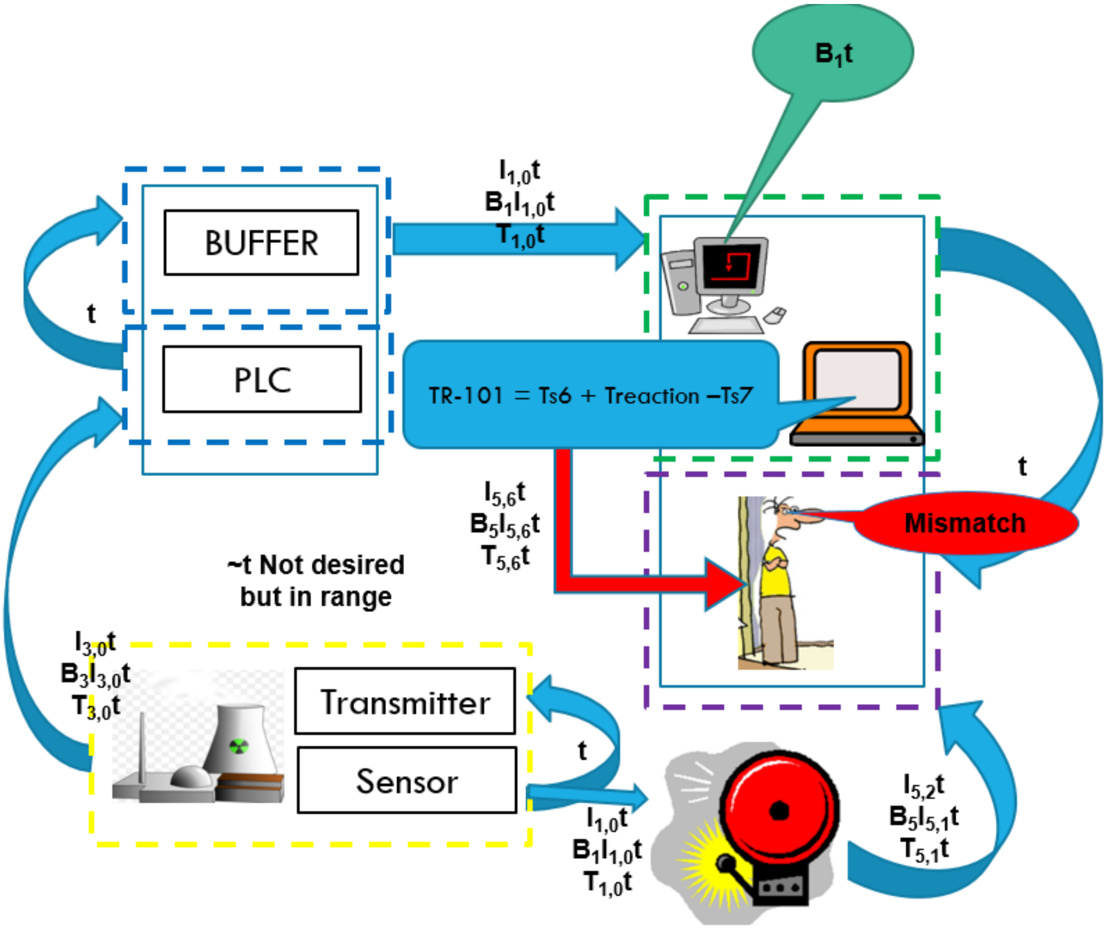

Figure 6.5: Information Flow when t is normal and using invariant

3. ∼t = true; temperature is not normal

4. w $\models V_t^0$ (w) = true; the reading is normal in this world

5. $I_{1,0}$t; sensor report temperature is fine to alarm/control room

6. $B_1I_{1,0}$t; control room monitor believes sensor report

7. $T_{1,0}$t; control room monitor the sensors

8. $B_1I_{1,0}$t $\wedge$ $T_{1,0}$t $\rightarrow$ B_1t; control room monitor believes the reading

9. $I_{5,1}$t; operator observes the monitor

10. $B_5I_{5,1}$t; operator believes monitor

11. $T_{5,1}$t; operator trusts monitor

12. $B_5 I_{5,1}$t $\wedge$ $T_{5,1}$t $\rightarrow$ B_5t; operator believes readings are correct and normal

13. $\sim t_{R-101} \implies$ ∼t; from assumption and invariant

14. $I_{5,6}$t; operator observes the invariant

15. $B_5 I_{5,6}$t; operator believes the invariant

16. $T_{5,6}$t; operator trusts the invariant

17. $B_5 I_{5,6}$t $\wedge$ $T_{5,6}$t $\rightarrow$ B_5t; operator believes readings are correct and normal

18. $S_{invariant} \wedge S_t = S^{"}$; system is working normally if and if only this is true

19. w $\models V_t^5$ (w) = true

$$\text{MSDND(ES)} = \exists \text{ w} \in \text{W} \vdash [\,(\,S^{"} \oplus S_{\sim t}\,)\,] \wedge [\text{w} \models (\,\nexists\, V^5_{\sim t}(\,\text{w}) \wedge \exists\, V_t^5(\,\text{w})\,)\,]$$

V_t^5(w) exists, it can be evaluated from the invariant, which contradicts the second part of MSDND definition. Therefore, the system is not MSDND secure, and a potential threat can be detected. This is good for the plant and bad for the attacker. □

A careful analysis can lead to several invariant equations that govern the operation of the entire plant. A few of the invariant equations are as follows [2]:

- The overall material balance for the benzene process

  Input = Output

  Stream 3 + Stream 1 = Stream 15 + Stream 16

  [Toluene feed + Hydrogen feed] == [Benzene produced + Fuel gas produced]

- conversion per pass of toluene to benzene in R-101 Toluene introduced= 144 (Stream 6) + 0.04 (Stream 7) = 144.04 kmol/h

  Benzene produced = 116 (Stream 9) - 7.6 (Stream 6) - 0.37 (Stream 7) = 108.03 kmol/h

  $\epsilon = 108.03/144.04 = 0.75$

  Alternatively, the following can be written:

  Moles of benzene produced= Toluene in - Toluene out == 144.04 - 36.00 = 108.04 kmol/h

  $\epsilon = 108.04/144.04 = 0.75$

- $t_{R-101} = t_{s6} + t_{reaction} - t_{s7}$

6.3. MSDND ANALYSIS OF FLOW RATE *f* OF STREAMS IN AND OUT OF THE REACTOR

The streams that are flowing into the reactor are stream 6, stream 7 and out of the reactor is stream 9, these can be clearly seen in Figure 6.6. The flow rates of each stream are critical, stream 6 carries the input feed(heated mixture of toluene and hydrogen) while stream 7 carries the compressed hydrogen from phase separator into the reactor to regulate the temperature of the reactor. stream 9 carries the outputs (benzene and other unreacted and residual components). The flow rates of these streams contribute to the amount of materials present in the reactor, temperature of the reactor and also the efficiency benzene production; i.e., the conversion ratio ϵ.

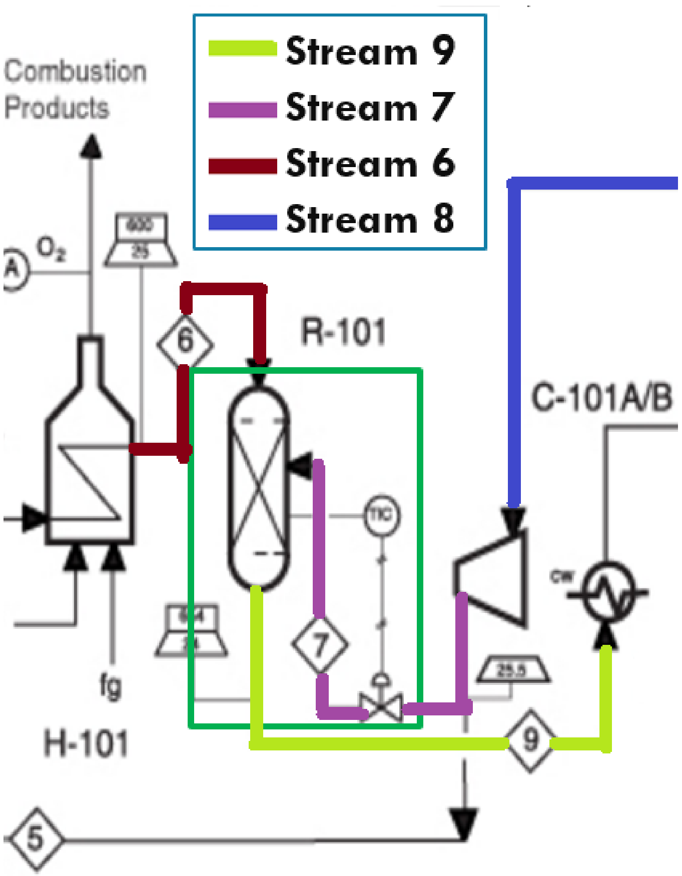

Figure 6.6: Information Flow when f is normal

6.3.1. MSDND Under Attack - f Is Beyond Threshold.

Since, there is an attack on the pressure information path at stream 8 in Figure 6.6, the flow rate of stream 7 and stream 9 may not be normal. This can lead to a cascading failure or huge damage to the reactor, few other impacts on the plant are increase in temperature of the reactor, decrease in efficiency, material accumulation and overflow of the reactor etc.

Theorem 7. *The flow rate f is not MSDND secure if it triggers the alarms.*

Proof. The value of f is beyond the threshold and the alarms are triggered. We know that $\mathrm{f} \oplus \sim\mathrm{f}$ is true all the time [either flow rate is in the desired range or not].

1. $\mathrm{f} \oplus \sim\mathrm{f} = \mathrm{true}$;

2. $S_f \oplus S_{\sim f}$ = true; system is either normal or not normal

3. ∼f = true; flow rate is normal

4. w $\models V_f^0$ (w) = false; the reading is not normal in this world

5. $I_{1,0}$ ∼f; sensor report problem to alarm/control room

6. $B_1 I_{1,0}$ ∼f; alarm believes sensor report

7. $T_{1,0}$ ∼f; alarm trusts the sensors

8. $B_1 I_{1,0}$ ∼f ∧ $T_{1,0}$t → B_1t; alarm believes the reading

9. $I_{5,2}$ ∼f; alarm is triggered and operator observes the alarm

10. $B_5 I_{5,1}$ ∼f; operator believes alarm

11. $T_{5,1}$ ∼f; operator trusts the alarm

12. $B_5 I_{5,1}$ ∼f ∧ $T_{5,1}$ ∼f → B_5 ∼f; operator believes readings are correct and not normal

13. w $\models V_{\sim f}^5$(w) = true; $V_{\sim f}^5$(w) always returns true

MSDND(ES) = $\exists$ w $\in$ W $\vdash$ $[\,(\,S_f \oplus S_{\sim f}\,)\,] \wedge [\,\mathrm{w} \models (\,\exists\, V_{\sim f}^5(\,\mathrm{w}\,) \wedge \nexists\, V_f^5(\,\mathrm{w}\,)\,)\,]$

$V_{\sim f}^5$(w) exists, which contradicts the second part of MSDND definition. Therefore, f is MSDND secure. This is clearly good for the plant since the attack can be detected. □

6.3.2. MSDND Under Attack - *f* Is Within Limits.

Theorem 8. *The flow rate f is MSDND secure if f lies within the broad threshold limits of the alarms.*

Proof. In this situation the actual f is not normal, however the readings show that f is normal.

1. f $\oplus$ ∼f = true; either flow rate is in the desired range or not
2. $S_f \oplus S_{\sim f}$ = true; system is either normal or not normal
3. ∼f = true; flow rate is not normal
4. w $\models V_f^0$ (w) = true; the reading is normal in this world
5. $I_{1,0}$f; sensor report flow rate is fine to alarm/control room
6. $B_1 I_{1,0}$f; control room monitor (or alarm) believes sensor report
7. $T_{1,0}$f; control room monitor (or alarm) trusts the sensors
8. $B_1 I_{1,0}$f $\wedge$ $T_{1,0}$f $\rightarrow$ B_1f; control room monitor (or alarm) believes the reading
9. $I_{5,1}$f; operator observes the monitor (or alarm)
10. $B_5 I_{5,1}$f; operator believes monitor (or alarm)
11. $T_{5,1}$f; operator trusts monitor (or alarm)
12. $B_5 I_{5,1}$f $\wedge$ $T_{5,1}$f $\rightarrow$ B_5f; operator believes readings are correct and normal
13. w $\models V_f^5$(w) = true; V_f^5(w) always returns true

$$\text{MSDND(ES)} = \exists\, \text{w} \in \text{W} \vdash [\,(\,S_f \oplus S_{\sim f}\,)\,] \wedge [\,\text{w} \models (\,\nexists\, V^5_{\sim f}(\,\text{w}\,) \wedge \nexists\, V^5_f(\,\text{w}\,)\,)\,]$$

Therefore, unknown to entities in SD^5, V_f^5 (w) and $V_{\sim f}^5$ (w) are consistent with both working conditions and not working conditions of the system. Therefore f is MSDND secure from SD^5. This is bad for the system. □

6.3.3. MSDND Analysis Of Flow Rate f In Presence Of Invariant.

If the flow rate resides within the threshold limits, can we detect the stuxnet like attack in the plant? It can be clearly seen from the above proof that if the virus operates in such a way that the values reside within the threshold limits, the threat goes undetected. The following theorem and proof will help understanding the effectiveness of invariants in determining the security of the system. The invariant that can be used in this case is the conversion ratio.

$$\epsilon = \frac{(stream7 + stream6)benzene}{(stream9 - stream6 - stream7)toluene} \tag{6.6}$$

Theorem 9. *The flow rates f_7 and f_9 are MSDND secure in presence of an invariant.*

Proof. The critical part of this proof is the construction of an invariant. Considering the conversion ratio (6.6); i.e., conversion per pass of toluene to benzene, we get the following:

1. f $\oplus$ ~f = true; either flow rate is in the desired range or not
2. $S_f \oplus S_{\sim f}$ = true; system is either normal or not normal
3. f(f_7 && f_9) = true; flow rate is normal
4. w $\models V_f^0$ (w) = true; the reading is normal in this world
5. $I_{1,0}\ f_7$; sensor reports flow rate is normal to alarm/control room
6. $B_1 I_{1,0}\ f_7$; alarm/control room monitor believes sensor report
7. $T_{1,0}\ f_7$; alarm/control room monitor trusts the sensors
8. $B_1 I_{1,0}\ f_7 \wedge T_{1,0}\ f_7 \rightarrow B_1\ f_7$; alarm/control room monitor believes the reading
9. $I_{5,1}\ f_7$; operator observes the monitor

10. $B_5 I_{5,1}\ f_7$; operator believes sensor report

11. $T_{5,1}\ f_7$; operator trusts the monitor

12. $I_{1,0}\ f_9$; sensor reports flow rate is normal to alarm/control room

13. $B_1 I_{1,0}\ f_9$; alarm/control room monitor believes sensor report

14. $T_{1,0}\ f_9$; alarm/control room monitor trusts the sensors

15. $B_1 I_{1,0}\ f_9 \wedge T_{1,0} f_9 \rightarrow B_1 f_9$; alarm/control room monitor believes the reading

16. $I_{5,1}\ f_9$; operator observes the monitor

17. $B_5 I_{5,1}\ f_9$; operator believes sensor report

18. $T_{5,1}\ f_9$; operator trusts the monitor

19. ϵ= original conversion ratio as per the process

20. ϵ_c = conversion ratio calculated from f_7 and f_9 readings from the sensors

21. if $\epsilon = \epsilon_c$ the system is working correctly.

22. if $\epsilon\ != \epsilon_c$ the system is not working correctly.

$$\text{MSDND(ES)} = \exists\ \text{w} \in \text{W} \vdash [\,(\,S_f \oplus S_{\sim f}\,)\,] \wedge [\,\text{w} \models (\,\exists\ V^5_{\sim f}(\,\text{w}) \wedge \nexists\ V^5_f(\,\text{w})\,)\,]$$

$V^5_{\sim f}$(w) exists, which contradicts the second part of MSDND definition. This can be evaluated from the invariant. Therefore, f is not MSDND secure even though the values lie within the threshold limits of the alarms. This is good for the plant and bad for the attacker. □

7. DISTILLATION COLUMN - PHASE-II

A detailed analysis of the impact of stuxnet-like attack on the pressure path (modeled in the previous section) on phase-II of the chemical plant; i.e., the distillation column of the plant, is shown in this section.

7.1. DISTILLATION PROCESS

This is the final phase (phase-II) of the benzene production process. In this phase, the desired product is separated from the byproducts and the unreacted components. That is, benzene is separated from unreacted toluene, unreacted hydrogen and the by-product methane. The distillation column is used to purify the benzene product by separating all the unreacted components and the byproducts (Figure 7.1). This tower consists of 42 sieve trays, a reboiler, a condenser, a reflux drum, and a reflux pump. Toluene exits as a liquid in the bottom at a temperature of 112^0C and 2.43 bar. The overhead containing benzene, traces of hydrogen and methane, is condensed at a temperature of 112^0C and a pressure 2.5 bar. Cooling water is used to condense the vapor exiting the column. The remaining hydrogen and methane are then separated in the reflux drum; this vapor stream is combined with the other gaseous streams at the overhead of the first separator, and the overhead of the second separator, which are combined to form the fuel gas. The liquid stream exiting the bottom of the reflux drum is pumped to a discharge pressure of 3.3 bar. The pumped stream is separated into two streams. One stream is fed to tray one of the column and the other stream is cooled down to 38^0C in the heat exchanger. The cooled product stream is then sent to storage.

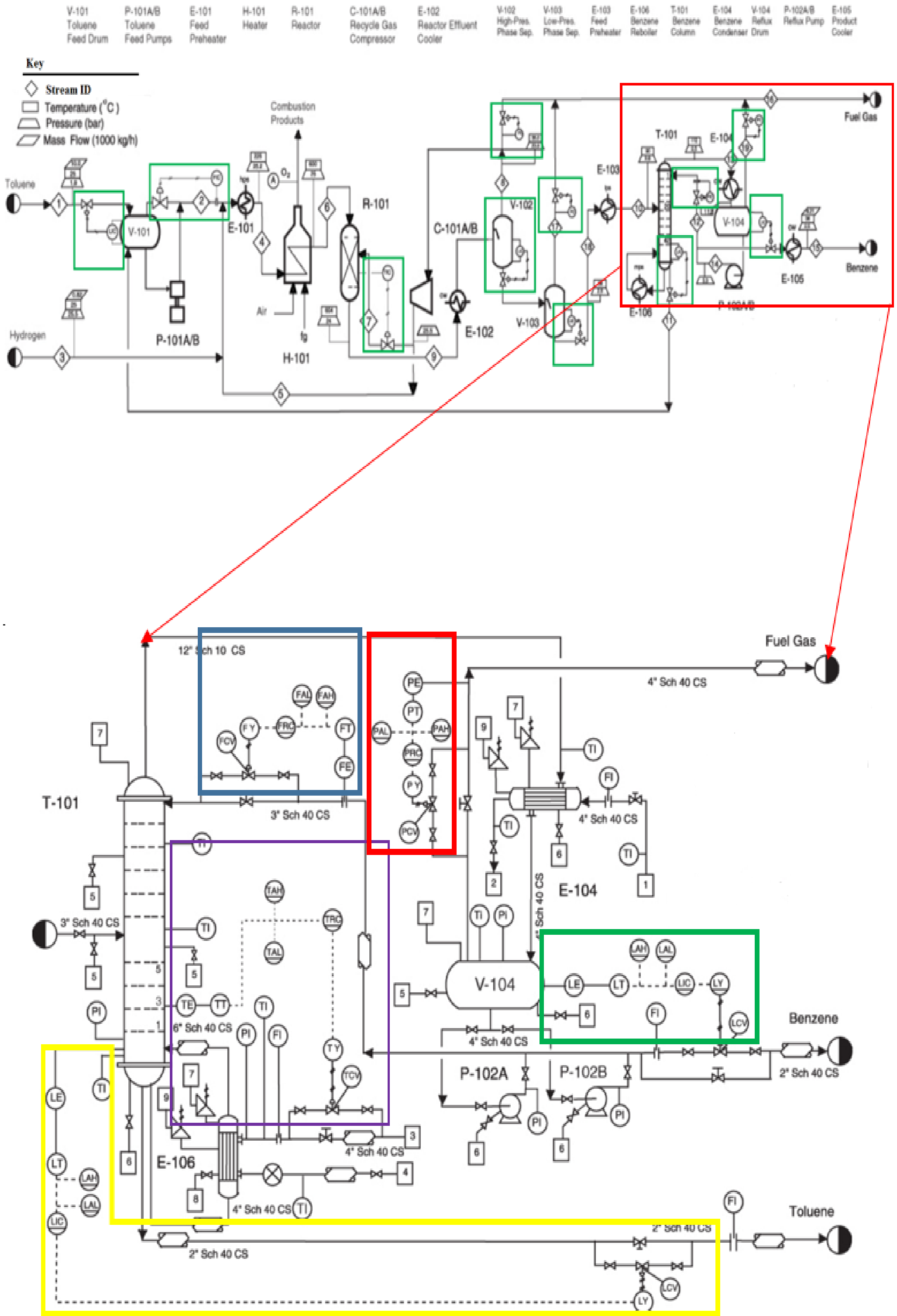

Figure 7.1: Distillation column and information paths[2]

Information flow: A level sensing element (LE) is located on the reflux drum V-104. A level transmitter (LT) also located on V-104 sends an electrical signal (designated by a dashed line) to a level indicator and controller (LIC). This LIC is located in the control room on the control panel or console (as indicated by the horizontal line under LIC) and can be observed by the operators. From the LIC, an electrical signal is sent to an instrument (LY) that computes the correct valve position and in turn sends a pneumatic signal (designated by a solid line with cross hatching) to activate the control valve (LCV). In order to warn operators of potential problems, two alarms are placed in the control room. These are a high-level alarm (LAH) and a low-level alarm (LAL), and they receive the same signal from the level transmitter as does the controller. It is a simple matter to infer that if there is an increase in the level of liquid in V-104, the control valve will open slightly and the flow of benzene product will increase, tending to lower the level in V-104. For a decrease in the level of liquid, the valve will close slightly.

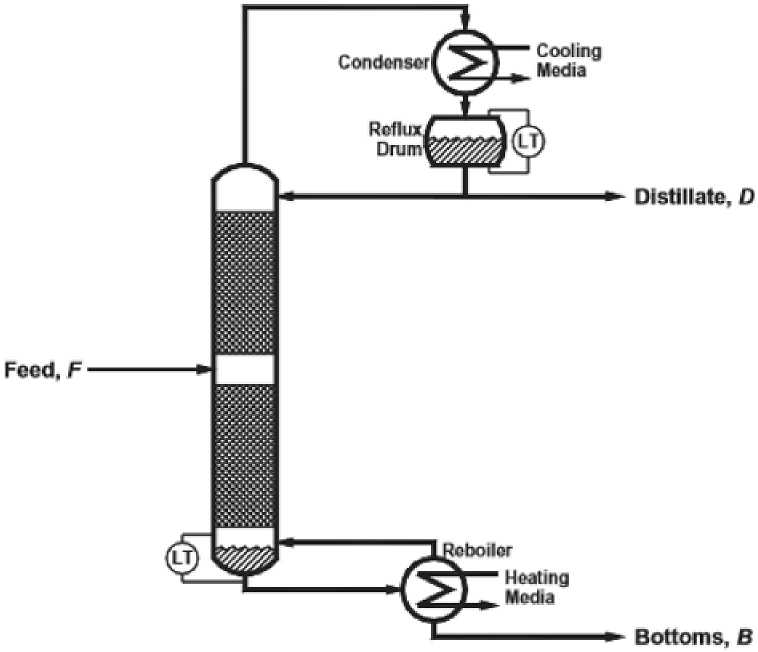

Figure 7.2: Simplified distillation column [3]

Invariants in the distillation column designed from the material balances are the most fundamental equations that can be written for any process. From Figure 7.2 we can see that F = D + B, where F is feed, D is distillate and B is bottoms.

$$F = D + B \tag{7.1}$$

Any long-term change in the distillate flow must be offset by an equal and opposite change in the bottoms flow and similarly any long-term change in the bottoms flow must be offset by an equal and opposite change in the distillate flow [3].

Most distillation columns operate in a fixed service, which means that

- the feed flow F is explicitly specified or is determined by upstream unit operations
- the feed composition is determined by upstream unit operations

When the distillation column goes into unsteady state, the following possibilities arise:

1. Feed rate exceeds the sum of the product rates. Material accumulates somewhere within the tower.
2. Feed rate is less than the sum of the product rates. Material depletes somewhere within the tower.

Material accumulates or depletes primarily either in the reflux drum, in the bottom of the column, or both.

7.2. MSDND ANALYSIS IN THE DISTILLATION COLUMN

The most important parameters in consideration are level indicator l, and flow rate f. We also know that if the flow rate, time and level are given we can calculate the molar masses. [assuming we know the chemical components of each stream]. In this section, a structured analysis of MSDND for the parameters f and l is shown.

7.2.1. Effects Of The Attack On Flow Rate And Level. Since there is a stuxnet-like attack in the chemical plant, let us assume that the feed to distillation column is affected, two cases arise

1. $$F < D + B \tag{7.2}$$

2. $$F > D + B \tag{7.3}$$

The responsibility of every level controller is to close some material balance. To assure that the column material balance closes, every column control configuration must contain one of the following:

1. The reflux drum level is controlled by manipulating the distillate flow.

2. The bottom level is controlled by manipulating the bottom flow.

In the presence of effectively placed alarms, if F > B + D, then the holdup increases (material is accumulated) until some limiting condition is attained, the limiting condition being either

1. the level in the reflux drum actuates the high level switch or

2. the level in the bottoms actuates the high level switch.

If F < B + D. The holdup decreases until some limiting condition is attained, the limiting condition being either

1. the level in the reflux drum actuates the low level switch or

2. the level in the bottoms actuates the low level switch.

7.2.2. MSDND Under Attack - f And l Are Beyond Threshold.

The following proofs show that in presence of alarms and the readings going beyond the threshold the information is not MSDND secure, which is good for the plant.

Theorem 10. *The flow rate f is MSDND secure in presence of alarms. This statement holds true for f at F, B and D as shown in Figure 7.2 if they are affected.*

Proof. Assuming the alarms are working and will trigger if the values go beyond a certain threshold.

1. $\sim$f = true; flow rate is not normal
2. w $\models V_f^0$ (w) = false; the reading is not normal, the valuation function in world w returns false
3. $I_{1,0}$ $\sim$f; sensor reports problem to alarm/control room
4. $B_1 I_{1,0}$ $\sim$f; alarm believes sensor report
5. $T_{1,0}$ $\sim$f; alarm trusts the sensors
6. $B_1 I_{1,0}$ $\sim$f $\wedge$ $T_{1,0}$ $\sim$f $\rightarrow$ B_1 $\sim$f; alarm believes the reading
7. $I_{5,2}$ $\sim$f; alarm triggers
8. $B_5 I_{5,1}$ $\sim$f; operator believes alarm
9. $T_{5,1}$ $\sim$f; operator trusts alarm
10. $B_5 I_{5,1}$ $\sim$f $\wedge$ $T_{5,1}$ $\sim$f $\rightarrow$ B_5 $\sim$f; operator believes readings are correct but not normal
11. w $\models V^5_{\sim f}$(w) = true; $V^5_{\sim f}$(w) always returns true

$$\text{MSDND(ES)} = \exists\, \text{w} \in \text{W} \vdash [\,(\,S_f \oplus S_{\sim f}\,)\,] \,\wedge\, [\,\text{w} \models (\,\exists\, V^5_{\sim f}(\,\text{w}) \,\wedge\, \nexists\, V^5_f(\,\text{w})\,)\,]$$

Since $B_5 I_{5,1}$ ∼f ∧ $T_{5,1}$ ∼f → B_5 ∼f. Therefore, in SD^5, $V^5_{\sim f}$(w) can be evaluated. The operator knows that flow rate is not in desired range. Therefore f is not MSDND secure from SD^5. □

Theorem 11. *The level indicator l is MSDND secure in presence of alarms. This statement holds true for l at F,B and D as shown in Figure 7.2 if they are effected.*

Proof. Assuming the alarms are working and will trigger if the values go beyond a certain threshold.

1. ∼l = true; flow rate is not normal
2. w $\models V^0_l$ (w) = false; the reading is not normal, the valuation function in world w returns false
3. $I_{1,0}$ ∼l; sensor reports problem to alarm/control room
4. $B_1 I_{1,0}$ ∼l; alarm believes sensor report
5. $T_{1,0}$ ∼l; alarm trusts the sensors
6. $B_1 I_{1,0}$ ∼l ∧ $T_{1,0}$ ∼f → B_1 ∼f; alarm believes the reading
7. $I_{5,2}$ ∼l; alarm triggers
8. $B_5 I_{5,1}$ ∼l; operator believes alarm
9. $T_{5,1}$ ∼l; operator trusts alarm
10. $B_5 I_{5,1}$ ∼l ∧ $T_{5,1}$ ∼l → B_5 ∼l; operator believes readings are correct but not normal

11. w $\models V^5_{\sim l}$(w) = true; $V^5_{\sim l}$(w) always returns true

$$\text{MSDND(ES)} = \exists \text{ w} \in \text{W} \vdash [\,(\,S_l \oplus S_{\sim l}\,)\,] \wedge [\text{w} \models (\,\exists\, V^5_{\sim l}(\,\text{w}) \wedge \nexists\, V^5_f(\,\text{w})\,)\,]$$

Since $B_5 I_{5,1} \sim\text{l} \wedge T_{5,1} \sim\text{l} \rightarrow B_5 \sim\text{l}$. Therefore, in SD^5, $V^5_{\sim l}$(w) can be evaluated. The operator knows that level is not in desired range. Therefore l is not MSDND secure from SD^5. □

The above proofs show that if a physical entity like an operator sees the physical alarms present in the plant while observing the sensor reports, a MSDND secure path can be converted into a not MSDND secure path which is good for the plant. However, when the virus operates in such a way that the values l and f reside within the threshold limits and alarms are not triggered, the system is MSDND secure which is bad for the plant as the threat goes undetected.

7.2.3. MSDND Under Attack - *f* And *l* Are Within Limits.

Theorem 12. *The flow rate f is MSDND secure if f lies within the broad threshold limits of the alarms.*

Proof. In this world, the actual flow rate f is not normal. However, the readings are normal.

1. f $\oplus$ ~f = true; either flow rate is in the desired range or not

2. $S_f \oplus S_{\sim f}$ = true; system is either normal or not normal

3. ~f = true; flow rate is is not normal

4. w $\models V^0_f$ (w) = true; the reading is normal in this world

5. $I_{1,0}$f; sensor reports flow rate is fine to alarm/control room

6. $B_1 I_{1,0}$f; control room monitor believes sensor report

7. $T_{1,0}$f; control room monitor the sensors

8. $B_1 I_{1,0}\text{f} \wedge T_{1,0}\text{f} \rightarrow B_1$f; control room monitor believes the reading

9. $I_{5,1}$f; operator observes the monitor

10. $B_5 I_{5,1}$f; operator believes monitor

11. $T_{5,1}$f; operator trusts monitor

12. $B_5 I_{5,1}\text{f} \wedge T_{5,1}\text{f} \rightarrow B_5$f; operator believes readings are correct and normal

13. w $\models V_f^5(\text{w}) = \text{true}$; $V_f^5(\text{w})$ always returns true

$$\text{MSDND(ES)} = \exists \text{ w} \in \text{W} \vdash [\,(\,S_f \oplus S_{\sim f}\,)\,] \wedge [\text{w} \models (\, \nexists\, V^5_{\sim f}(\,\text{w}) \wedge \nexists\, V^5_f(\,\text{w})\,)\,]$$

Unknown to entities in SD^5 (operator), $V_f^5(\text{w})$ and $V^5_{\sim f}(\text{w})$ cannot be evaluated. Therefore, f is MSDND secure from SD^5. The flow rate is consistent with both working and non-working states of the system. □

Theorem 13. *The level reading l is MSDND secure if l lies within the broad threshold limits of the alarms.*

Proof. In this world, the actual level l is not normal. However, the readings are normal.

1. l $\oplus \sim$l = true; either flow rate is in the desired range or not

2. $S_l \oplus S_\sim = \text{true}$; system is either normal or not normal

3. $\sim$l = true; level is normal

4. w $\models V_l^0\ (\text{w}) = \text{true}$; the reading is normal in this world

5. $I_{1,0}$l; sensor reports flow rate is fine to alarm/control room
6. $B_1 I_{1,0}$l; control room monitor believes sensor report
7. $T_{1,0}$l; control room monitor the sensors
8. $B_1 I_{1,0}\text{l} \wedge T_{1,0}\text{l} \rightarrow B_1$l; control room monitor believes the reading
9. $I_{5,1}$l; operator observes the monitor
10. $B_5 I_{5,1}$l; operator believes monitor
11. $T_{5,1}$l; operator trusts monitor
12. $B_5 I_{5,1}\text{l} \wedge T_{5,1}\text{l} \rightarrow B_5$l; operator believes readings are correct and normal
13. w $\models V_l^5(\text{w}) = \text{true}$; $V_l^5(\text{w})$ always returns true

$$\text{MSDND(ES)} = \exists \text{ w} \in \text{W} \vdash [\,(\,S_l \oplus S_{\sim l}\,)\,] \wedge [\text{w} \models (\,\nexists\, V^5_{\sim l}(\,\text{w}) \;\wedge\; \nexists\, V_l^5(\,\text{w})\,)\,]$$

Unknown to entities in SD^5 (operator), V_l^5(w) and $V^5_{\sim l}$(w) cannot be evaluated. Therefore, l is MSDND secure from SD^5. The level l is consistent with both working and non-working states of the system. □

7.2.4. MSDND Under Attack - With Invariant. Similar to the Theorems 6 and 9 the invariant (7.1) proves that the system is not MSDND secure even when the virus operates in such a way that the readings reside within the threshold limits of the alarms. The following proof illustrates the same.

Theorem 14. *The flow rates f at B and D are not MSDND secure when the invariant (7.1) is considered.*

Proof. Let the flow rate at B be f_b and flow rate at D be f_d.

1. f_b = true; flow rate is normal

2. w $\models V^0_{f_b}$ (w) = true; the reading is normal in this world

3. $I_{1,0}f_b$; sensor reports flow rate is fine to alarm/control room

4. $B_1 I_{1,0} f_b$; control room monitor believes sensor report

5. $T_{1,0}f_b$; control room monitor the sensors

6. $B_1 I_{1,0} f_b \wedge T_{1,0} f_b \rightarrow B_1 f_b$; control room monitor believes the reading

7. $I_{5,1}f_b$; operator observes the monitor

8. $B_5 I_{5,1} f_b$; operator believes monitor

9. $T_{5,1}f_b$; operator trusts monitor

10. $B_5 I_{5,1} f_b \wedge T_{5,1} f_b \rightarrow B_5 f_b$; operator believes readings are correct and normal

    Similarly, for the flow rate f_d we get,

11. f_d = true; flow rate is normal

12. w $\models V^0_{f_d}$ (w) = true; the reading is normal in this world

13. $I_{1,0}f_d$; sensor reports flow rate is fine to alarm/control room

14. $B_1 I_{1,0} f_d$; control room monitor believes sensor report

15. $T_{1,0}f_d$; control room monitor the sensors

16. $B_1 I_{1,0} f_d \wedge T_{1,0} f_d \rightarrow B_1 f_d$; control room monitor believes the reading

17. $I_{5,1}f_d$; operator observes the monitor

18. $B_5 I_{5,1} f_d$; operator believes monitor

19. $T_{5,1}f_d$; operator trusts monitor

20. $B_5 I_{5,1} f_d \wedge T_{5,1} f_d \rightarrow B_5 f_d$; operator believes readings are correct and normal

21. F = D + B; operator observes the invariant equation

22. F_{new} = f_d + f_b; operator calculates F_{new} from readings of f_b and f_d from steps 10 and 20 respectively.

23. F $\neq F_{new}$; operator observes the mismatch and thus has a valuation for system not working correctly.

24. w $\models V^5_{\sim f}$(w) = true; $V^5_{\sim f}$(w) always returns true

$$\text{MSDND(ES)} = \exists \text{ w} \in \text{W} \vdash [\,(\,S_f \oplus S_{\sim f}\,)\,] \;\wedge\; [\,\text{w} \models (\,\exists\, V^5_{\sim f}(\,\text{w}\,) \;\wedge\; \nexists\, V^5_f(\,\text{w}\,)\,)\,]$$

□

This is how invariants derived from physical and chemical processes of a system can be used to evaluate an information flow path (for various critical parameters) and convert a path from MSDND secure (bad for the plant) to not MSDND secure (good for the plant) to detect a possible threat. This analysis uses alternative information paths for a parameter in consideration to model security and therefore making it much more difficult for the attacker to compromise the system. In-order to damage the system without getting deduced by an operator, the attacker has to corrupt multiple information paths which is very difficult and therefore providing more resiliency to the system.

8. CONCLUSION

MSDND is useful to model attacks where the goal is to hide critical information from an operator rather than to steal information. MSDND secure is bad for the system and good for the attacker because information can be hidden by making it impossible to evaluate the desired question, or to falsify the actual valuation function to produce an invalid valuation and thus making the information MSDND secure and undetectable. A system with fewer MSDND secure information paths between the CPS and monitors/observers has fewer vulnerabilities. Stuxnet-like attacks in CPS adapt to the system and replay valid readings even though they disrupt the functionality. Attacks like these can be detected to some extent by strategically adding physical alarms on the information paths and an entity i monitoring them. However, when these attacks disrupt the functionality without kicking off the alarms, the invariants play a vital role by acting as a secondary source of information for the given parameter. We were able to prove that a system with a MSDND secure path can be reduced to a not MSDND secure system using a proper invariant, thus making the system much more secure and reliable. With the help of invariants it has been proved that an attack can be detected even if the system operates within the threshold limits and there are no alarms. The operator need not wait for the alarms to trigger before s/he notices there is something wrong with the system. Usage of invariants is especially critical when the attacker operates within tight bounds. By finding more information paths and invariants involving critical parameters and embedding them into the MSDND framework, the system can be made more resilient. The attacker now has to corrupt multiple information paths to compromise the system, making it even more difficult and tedious to the attacker. No system is 100 percent secure, this thesis provides a way to assess the information paths and the state of a system and provide a higher degree of security and resiliency. Some of the critical points to focus in future are to find a method to optimally divide the system into security domains and to automate the MSDND proof derivation based on the number of security domains and the information flowing in the given path.

Table 8.1 and Table 8.2 show the results of MSDND analysis of critical parameters in a benzene production plant.

Table 8.1: MSDND analysis results: reactor and phase separator

Theorem	Information Path	MSDND	Plant status
1	β under normal conditions	No	Good
2	p under attack(No alarms)	Yes	Bad
2.1	p under attack(with alarms)	No	Good
3	t under normal conditions	No	Good
4	t when p is attacked(with alarms)	No	Good
5	t when p is attacked, under threshold (with alarms)	Yes	Bad
6	t when p is attacked, under threshold (with invariant)	No	Good
7	f when p is attacked(with alarms)	No	Good
8	f when p is attacked, under threshold	Yes	Bad
9	f when p is attacked, under threshold with invariant	No	Good

Table 8.2: MSDND analysis results: distillation column

Theorem	Information Path	MSDND	Plant status
10	f when p is attacked (with alarms)	No	Good
11	l when p is attacked (with alarms)	No	Good
12	f when p is attacked, under threshold	Yes	Bad
13	l when p is attacked, under threshold	Yes	Bad
14	f when p is attacked, under threshold (with invariant)	No	Good

BIBLIOGRAPHY

[1] Gerry Howser and Bruce McMillin. A Multiple Security Domain Model of a Drive-by-Wire System. In *Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual*, pages 369–374. IEEE, 2013.

[2] R. Turton. *Analysis, Synthesis, and Design of Chemical Processes*. Prentice-Hall international series in engineering. Prentice Hall, 2012.

[3] Cecil L. Smith. *Distillation Control: An Engineering Perspective*. Wiley, 2012.

[4] Technical report, National Institute of Standards and Technology, http://www.nist.gov/cps/cpspwg.cfm, accessed December 30, 2015, 2014.

[5] David Sutherland. A model of Information. In *Proc. 9th National Computer Security Conference*, pages 175–183. DTIC Document, 1986.

[6] Gerry Howser and Bruce M. McMillin. A modal model of stuxnet attacks on cyber-physical systems: A matter of trust. In *Eighth International Conference on Software Security and Reliability, SERE 2014, San Francisco, California, USA, June 30 - July 2, 2014*, pages 225–234, 2014.

[7] Churn-Jung Liau. Belief, information acquisition, and trust in multi-agent systems: A modal logic formulation. *Artif. Intell.*, 149(1):31–60, September 2003.

[8] Churn-Jung Liau. A modal logic framework for multi-agent belief fusion. *ACM Trans. Comput. Logic*, 6(1):124–174, January 2005.

[9] Susan Owicki and David Gries. An axiomatic proof technique for parallel programs i. *Acta Informatica*, 6(4):319–340, 1976.

[10] T. Paul, J. W. Kimball, M. Zawodniok, T. P. Roth, B. McMillin, and S. Chellappan. Unified invariants for cyber-physical switched system stability. *IEEE Transactions on Smart Grid*, 5(1):112–120, Jan 2014.

[11] Sridhar Adepu and Aditya Mathur. *Using Process Invariants to Detect Cyber Attacks on a Water Treatment System*, pages 91–104. Springer International Publishing, Cham, 2016.

[12] T. Cruz, J. Barrigas, J. Proença, A. Graziano, S. Panzieri, L. Lev, and P. Simões. Improving network security monitoring for industrial control systems. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 878–881, May 2015.

[13] T. M. Chen. Stuxnet, the real start of cyber warfare? *IEEE Network*, 24(6):2–3, 2010.

[14] Technical report, Chemical Facility Anti-Terrorism Standards (CFATS), https://www.dhs.gov/chemical-facility-anti-terrorism-standards, accessed September 7, 2016.

[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, pages 133–144, New York, NY, USA, 2015. ACM.

[16] Keli Han and Tianshu Chu, editors. *Reaction Rate Constant Computations.* RSC Theoretical and Computational Chemistry Series. The Royal Society of Chemistry, 2013.

VITA

Prakash Dunaka was born in Hyderabad, India. He received his Bachelor's degree in Information Systems from the prestigious university, Birla Institute of Technology and Science, Pilani, Rajasthan, India in May 2012. He then worked with Scope International Pvt. Ltd. for three years as a Data Modeler/Software Developer in Chennai, India. His work was mainly focused on optimization and automation. He was responsible for performance tuning of SQL queries, data modeling, database architecture, and database optimization for the all core banking applications spread across the globe. He was also responsible for developing in-house automation tools to reduce redundant manual tasks. His interest to learn new things and gain greater knowledge motivated him to pursue graduate studies at the highly respected Missouri University of Science and Technology, Rolla, United States of America. During his graduate studies, he got fascinated with security aspects of cyber-physical systems. He worked with his adviser Dr. Bruce McMillin on security of cyber-physical systems, specifically on cyber-physical security of a chemical plant. Prakash published a paper on cyber-physical security of a chemical plant where he discusses about a framework and a concept of invariants which can applied to any cyber-physical system to make it more secure and resilient, which is the base for his thesis. He was awarded his Master's degree in Computer Science in May 2017.