INTRODUCTION

A. Background

Due to our over-reliance on web-based communication and technology, cyber security threats are common now. This menace has mainly targeted manufacturing and chemical sectors.

Services and operations can be seriously jeopardized by the cyber-attacks on the above-mentioned sectors exposing the entire population to a huge risk.

Safe and secure access to sensitive information and other hazardous entities has become a challenge due to the increased number of these sophisticated cyber-attacks.

Large-scale processing and manufacturing of chemicals are few of the typical attributes of an industrial process plant specifically a chemical plant. Such type of a plant is provided with a set of raw materials as an input, which performs certain reactions to give us the desired chemical and with some other residual output.

Unique equipments and technologies are used for the manufacturing process in these plants and industries. Along with the integrity, availability and information confidentiality enough attention is given to the safety and operational reliability. Having a vast infrastructure is a predicament to security breach and that's why physical security is as much crucial as cyber security.

Assume that a system is hacked by an intruder, causing some critical parameters like temperature, pressure and raw material ratio to be changed. This could prove to be calamitous.

Some significant consequences of security breach are as follows: [1]

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

Process & equipment safety are cited as major security concerns of a chemical industry, by the National Institute of Standards and Technology [2]**.** Besides high reliability and security, the required protection against attacks on system is only provided by cyber physical security.

While the privacy is discounted (as a concern) by the NIST document because of the absence of personally notable information, can realize covertness of the real processes as preferable. Targeted attacks are the biggest threat to CPS, where the attackers carry deep knowledge regarding the targeted controller and different processes controlled by it. For the sake of control over the system, attackers can run off with the vulnerabilities in CPS.

Cyber-attacks on Cyber physical system can follow in disturbance of the physical services and can cause a national disaster. According to the research on security of Cyber Physical Systems, it was reported that in many cases the lack of appropriate network security measures was putting processes at risk.

Most advanced network solutions like intrusion detection systems, cryptographic protocols, 7 & firewalls to industrial systems were suggested to adapt. Attacks on the IT infrastructure can be prevented by these defenses. An attacker like Stuxnet is assumed by this research, which can manipulate actuators, which in return can halt or hide the real process measurements from the control room.

Manipulated readings are identified by inspection of different methods. Attacks generating credible artificial values (the values that reside in the upper and lower threshold of the process) are generally considered, that present the data to the operator to deceive her about the true process.

Product efficiency or the process can be compromised by the impact of these on the system.

To be assured that the critical infrastructure is safe from all the cyber and physical processes, a strong blending is required between the physical and cyber controlling components. Hence, it is highly important to protect the CPS against every cyber-attack.

To protect the Cyber Physical System (CPS) from cyber-attacks or by malicious insiders, conventional security measures can be adapted. On the other hand, since the CPS being unique complex, conventional security techniques are inadequate to take care of the security challenges. To track and regulate the information flow of the system for the prevention of data leakage to unauthorized parties, a complimentary approach was proposed almost thirty years ago.

Security related to the information flow in CPS can lead to especially complex and structured security partitions. Cyber security tools & mechanism rarely function adequately to keep the physically tangible parts of the system from slipping the information. Just by fencing around the physical and observable parts of CPS is unsustainable in order to protect from cyber-attack. Electronic & cryptographic resolutions are not peculiar enough to control cyber-physical interfaces. A determined attacker with backing and time will hack in.

Current security models in use for information flow technology are examined in this thesis, additionally this work tries to identify some of the main obstacles of putting them into practice. A new information flow security model that minimizes the drawbacks of the traditional models is also introduced.

By modelling the security aspects of chemical plant, the effectiveness of this model can be described.

B. Motivation

Electricity, gas and water distribution systems, which are some critical infrastructure systems have been subject to changes in the past few decades. Practice of integrating information and communication technology to physical systems has arrived due to the distributed monitoring and control.

The first computerized based way to control and monitor has been SCADA (Supervisory Control and Data Acquisition). In fact, the term “Cyber-Physical System” has been unified by this, where physical processes, information exchange and computation are blended together for better efficiency, reliability.

An important matter of concern has always been of security in critical systems, even before the advent of cyber domain. There can be disastrous consequences and severe impacts on society by the attacks on the physical domain. Most of the security mechanisms in the past were implemented using physical protection.

Critical assets were usually located in controlled environments, preventing occurrence of undesired manipulations. This physical safety is not always totally practical in few cases. For example, special attention regarding critical infrastructure protection are required by chemical plants. More attention must be focused on integrity attacks rather than confidentiality in the thesis, as the process in the chemical plant is known.

In chemical plant, A lot remote access points are difficult to protect and control from attack or accident unlike in some other infrastructures.

This chapter provides the necessary information which helps to apprehend the rest of the thesis. At starting we described the basic terms and definitions.

1.1 Terms, definitions and concepts

Even though there has been indicative progress around the world, in different industrial and manufacturing field, nevertheless the confusions, misinterpretations, & ambivalence are still present in the sector of Risk Assessment. In this Chapter efforts have been built to give a good idea of this field, through the concepts obtained through the intense literature review.

The Risk Management field has faced problems in defining on principles. Risks are assessed & managed very different manner across the continents & countries as well as in industrial sector. One term has different interpretations as according to the sources explaining them. Risk Analysis, Risk Assessment and Risk Management has not been defined unitedly across the globe. So usually a lot complications and misunderstandings are there. These terms sometimes used reciprocally. Also, one term can have different meanings in different contexts and can be used accordingly. For e.g. word analysis may be wider than the management.

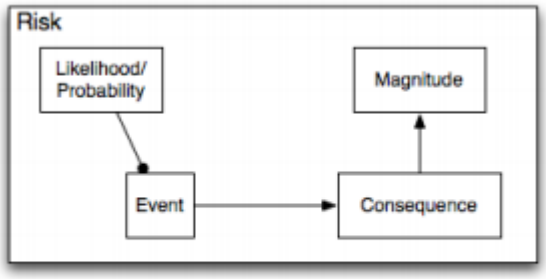


Figure 2.1-2 Simple View of Risk

DEFINITIONS:

Risk Analysis

1 The Society for Risk Analysis (SRA 2004) has defined the Risk analysis as "The process that includes risk assessment, risk characterization, risk communication, risk management, and policy relating to risk" [3]

2 "The use of available information to estimate the risk to individuals or populations, property or the environment from hazards. In general, Risk analysis follow these steps: scope definition, hazard identification, & risk estimation" [4]

Risk Assessment [5]

1. "The process of risk analysis and risk evaluation" (NOVA Chemicals Corporation, Canada, from CARAT 2001).
2. "The process in which analysed risk is judged for its acceptability" (RIVM the Netherlands, from CARAT 2001).

Risk Management [5]

1. "Risk management is the process of weighing policy alternatives and selecting the most appropriate regulatory action, integrating the results of risk assessment with additional data on social, economic and political concerns to reach a decision implying the following approach: identification of chemicals for consideration, risk assessment, risk evaluation, and risk mitigation or reduction." (EC 1997a).
2. "Risk management is a formal process for managing risks. The process consists of system definition, hazard identification, identification of accident scenarios, quantification of probabilities and consequences, assessment of risk, identification of risk control options, decision on implementation, identification and management of residual risk." (EC 1999).

Use of different approaches, terminology, definitions and methodologies are because of numerous factors including: (1) different perceptions, attitudes and values regarding risks in different socio-economic-political contexts. (2) different specifications and need of vast industrial sector and risk specifications in various countries. So, there are a lot of difficulties to agree on the convention in the risk analysis area, because almost every country and region has its own needs, preferences, and different legislation & government.

1.2 A universal approach of the risk management

As described before, society usually choose to embrace different aspects when it comes to risk management. Recently, some documentations might have broader view, the word **risk management system** (RMS) could be used to depict the widest concept, especially in the area of human health and safety, property & environmental safety.

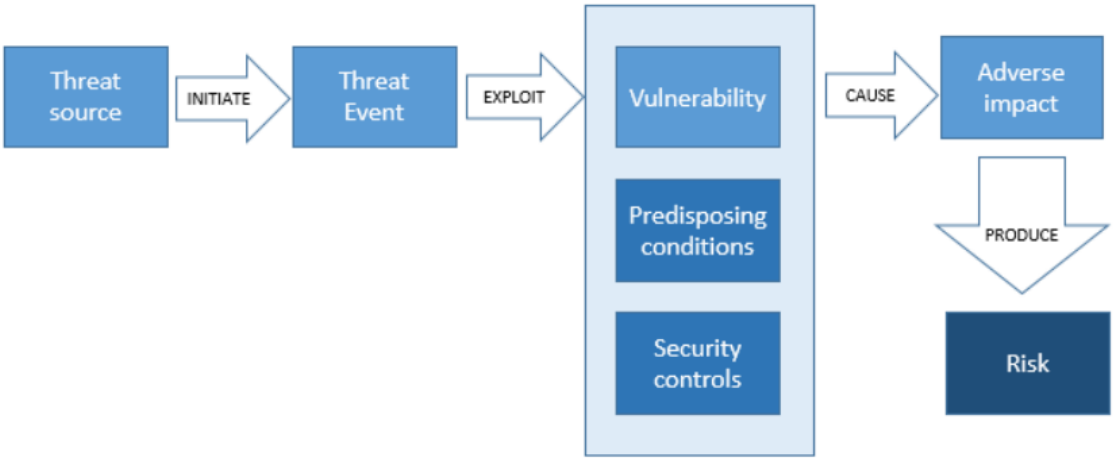
Some common alike terms in use are: [5]

- "Safety Management System" (SMS) (Demichela et al.2004) (Basso et al.2004)
- "Integrated Safety Management System" (Trbojevic and Carr 2000),

- "Risk Based Decision Making" (USCG 2001) (EC 2000b),
- "Integrated Socio-Economic Risk Management" (OECD 2000),

In the coming sections of this chapter efforts was done to describe a universal idea of the approaches associated with the RMS.

The RMS is overall unified procedure comprising of 2 interconnected and overlying, but basically two different components- *risk assessment and risk management.*



Glossary and basic terms:

We now introduce the concepts and terms which are used in Risk Assessments. We adopt (and reproduce) the definitions presented in the ISO/Guide 73:2009 (Risk management Vocabulary) [6]

By International Organization for Standardization

1. Terms relating to risk

1.1. Risk:

- "Effect of uncertainty on objectives."
- "An effect is a deviation from the expected — positive and/or negative."
- "Risk is often characterized by reference to potential events and consequences, or a combination of these."
- "Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence."

2. Terms relating to risk management

2.1. Risk management:

- "Coordinated activities to direct and control an organization with regard to risk."

2.2. Risk management framework:

- "Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization"
- "The foundations include the policy, objectives, mandate and commitment to manage risk."
- "The risk management framework is embedded within the organization's overall strategic and operational policies and practices."

2.3. Risk management policy:

- "Statement of the overall intentions and direction of an organization related to risk management.

2.4. Risk management plan:

- "Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk."
- "The risk management plan can be applied to a particular product, process and project, and part or whole of the organization."

3. Terms relating to the risk management process

3.1. Risk management process:

- "Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk."

3.2. Risk criteria:

- "Terms of reference against which the significance of a risk is evaluated."
- "Risk criteria are based on organizational objectives, and external and internal context."

4. Term relating to risk assessment

4.1. Risk assessment:

- "Overall process of risk identification, risk analysis and risk evaluation."

5. Terms relating to risk identification

5.1. Risk identification:

- "Process of finding, recognizing and describing risks."
- "Risk identification involves the identification of risk sources, events, their causes and their potential consequences."

5.2. Risk description:

- "Structured statement of risk usually containing four elements: sources, events, causes and consequences."

5.3. Risk source:

- "Element which alone or in combination has the intrinsic potential to give rise to risk."

5.4. Event, Consequences:

- Event: "The occurrence or change of a particular set of circumstances such as a system failure, an earthquake, an explosion or an outbreak of a pandemic." "An event can be one or more occurrences, and can have several causes."
- Consequences: The effects of the activity with respect to the values defined (such as human life and health, environment and economic assets), covering the totality of states, events, barriers and outcomes.

5.5. Hazard:

- "Source of potential harm."
- "A risk source where the potential consequences relate to harm. Hazards could for example be associated with energy (e.g. explosion, fire), material (toxic or eco-toxic), biota (pathogens) and information (panic communication)."

5.6 Harm, Damage, Adverse consequences, Impacts, Severity:

- Harm: "Physical or psychological injury or damage."
- Damage: "Loss of something desirable Adverse consequences: Unfavourable consequences."

- Impacts: “The effects that the consequences have on specified values (such as human life and health, environment and economic assets).”
- Severity: “The magnitude of the damage, harm, etc.”

5.6. Risk owner:

- “Person or entity with the accountability and authority to manage a risk.”

6. Terms relating to risk analysis

6.1. Risk analysis:

- “Process to comprehend the nature of risk and to determine the level of risk.”
- “Risk analysis provides the basis for risk evaluation and decisions about risk treatment.”

6.2. Probability, Likelihood:

- Probability: The classical interpretation applies only in situations with a finite number of outcomes which are equally likely to occur: The probability of A is equal to the ratio between the number of outcomes resulting in A and the total number of outcomes, i.e. $P(A)$ = Number of outcomes resulting in A divided by total number of outcomes
- Likelihood: “In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period].”

6.3. Exposure:

- “Extent to which an organization and/or stakeholder is subject to an event.”

6.4. Consequence:

- “An event can lead to a range of consequences.”
- “A consequence can be certain or uncertain and can have positive or negative effects on objectives.”

6.5. Uncertainty:

- “For a person or a group of persons, not knowing the true value of a quantity or the future consequences of an activity. Imperfect or incomplete information/knowledge about a hypothesis, a quantity, or the occurrence of an event.”

6.6. Probability:

- “Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty”

6.7. Frequency:

- “Number of events or outcomes per defined unit of time.”

6.8. Vulnerability:

- “Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.”

6.9. Risk matrix:

- “Tool for ranking and displaying risks by defining ranges for consequence and likelihood.”

7. Terms relating to risk evaluation

7.1. Risk evaluation:

- “Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.”
- “Risk evaluation assists in the decision about risk treatment.”

7.2. Risk attitude:

- “Organization's approach to assess and eventually pursue, retain, take or turn away from risk.”

7.3. Risk appetite:

- “Amount and type of risk that an organization is willing to pursue or retain.”

7.4. Risk tolerance:

- “Organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.”

7.5. Risk aversion:

- “Attitude to turn away from risk.”

7.6. Risk aggregation:

- “Combination of a number of risks into one risk to develop a more complete understanding of the overall risk”

7.7. Risk acceptance:

- "Risk acceptance is an informed decision to take a particular risk."

8. Terms relating to risk treatment

8.1. Risk treatment:

- Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".
- Risk treatment can create new risks or modify existing risks.

8.2 Control:

- "Controls include any process, policy, device, practice, or other actions which modify risk."

8.3 Risk avoidance:

- "Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk."

8.6. Risk retention:

- "Acceptance of the potential benefit of gain, or burden of loss, from a particular risk."

8.7 Residual risk:

- "Risk remaining after risk treatment."

8.8. Resilience:

- "Adaptive capacity of an organization in a complex and changing environment."

8.9 Safety analysis:

- "Systematic process to comprehend the nature of the safety of a system and to express the safety level. Systematic process to determine the degree of risk reduction that is sufficient to obtain a safe system."

9. Terms relating to monitoring and measurement

9.1. Monitoring:

- "Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected."
- "Monitoring can be applied to a risk management framework, risk management process, risk or control."

9.2. Review:

- “Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.”
- “Review can be applied to a risk management framework, risk management process, risk or control.”

9.3. Risk register:

- “Record of information about identified risks.”

9.4. Risk profile:

- “Description of any set of risks”.

AN OVERVIEW OF RISK ASSESSMENT TECHNOOGIES

Introduction

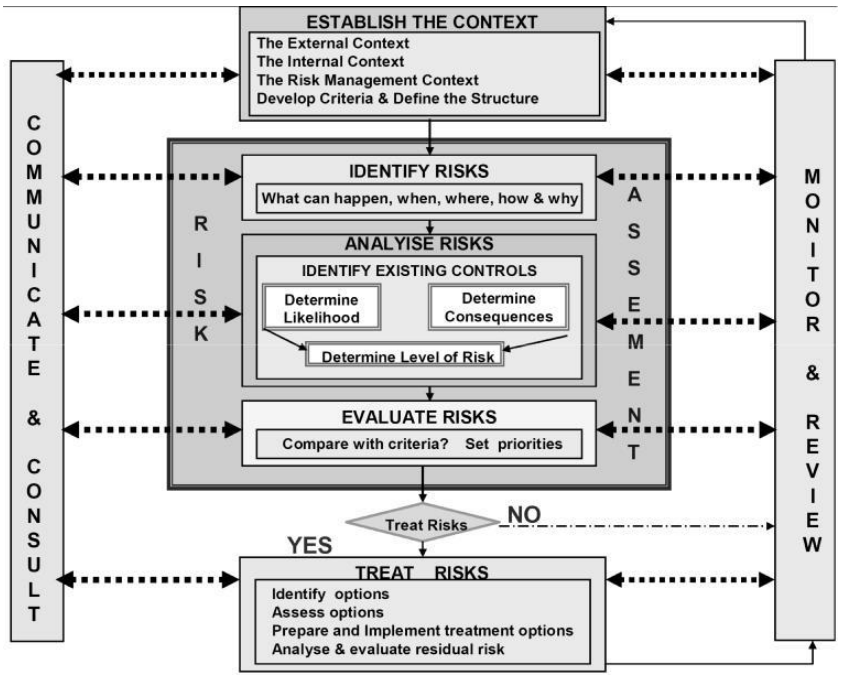
The range of risks are encountered by any type of organizations and may influence their reached goals. These intentions maybe linked to a range of the activities of the organization and are indicated in terms of technological, environmental, commercial, cultural, social, political, safety & security, and economic & financial scope. Therefore, the risk should be managed as these activities are associated with it. The risk management techniques are quite helpful in the decision making.

For the following purpose, risk management involves the use of systematic & logical approach.

- Communicating and consulting throughout this process;
- Establishing the context for identifying, analyzing, evaluating, treating risk associated with any activity, process, function or product;
- Monitoring and reviewing risks; and,
- Reporting and recording the results appropriately.

The main tool of risk management is the risk assessment which presents a systematic process that determines how aims can be influenced. Moreover, it includes the risk analysis in terms of repercussion & their likelihood, prior to the decision that whether further treatment is required. Following are the fundamental questions can be answered by Risk Assessment:

- What could happen & why?
- What would be the consequences?
- Probability of their future occurrence?
- Factors that mitigate the consequences of risk or that lessen the probability?
- Is the risk level being safe and tolerable or it requires further dealing?



2. Risk Assessment Techniques: [7]

2.1. Brainstorming

Generally, the word brainstorming is applied for any type of group discussion. It includes supportive and inspiring discussion in the bunch of people to determine risks, possible failure modes & related hazards, basis for decisions and alternatives for further dealing of risk[..]. Nonetheless, it is method actually concerns about significant techniques in order to assure that vision of each member is generated by the ideas and statements of others in the group.
It may be used for long discussions where problems are identified and can be used along with other risk assessment techniques to support imaginative reasoning at any point of the process of risk management.

2.2. Delphi technique

It is a process of getting a reliable general agreement of opinion from professionals. The main characteristics of this technique is that expert give their individual opinion anonymously even though they have approach to the view of another expert while the process proceeds. It can be used wherever a consensus of opinions is needed and can be implemented to any phase of the risk management or system life cycle.

2.3. Checklists

The lists of risks, hazards & control failures evolved from the experience due to past failures or the risk assessment are normally called checklists. Checklists can be applied at any stage of the system life cycle in order to diagnose risks & hazards or to evaluate the control efficiency. Moreover, there might be usage along with other type of risk assessment techniques.

2.4. Preliminary hazard analysis (PHA)

It is an inductive and uncomplicated technique, used to analyze hazards & circumstances and the events which can lead to the harm for a given system. Normally, it is implemented early in the development of a system. It can be beneficial for further analysis when given system is analysed to prioritise hazards and risks.

2.5. HAZOP

HAZOP stands for hazard and operability. It is a standardized & organized investigation of an existing system. This technique is used to identify the risks related to people, environment, equipment and organizational objectives. It is a qualitative method and works on the basis of using keywords which ask that how operating conditions might not be obtained at each stage in the system. Normally, it is implemented by the decision of a team that comprises of members from different disciplines. Initially, it is developed for analysing the systems of chemical process but later it has been expanded to other system types like mechanical, electronic, and software systems. Moreover, it can be used to review and design the legal contracts.

2.7. "What-if" Technique (SWIFT)

The origin of SWIFT was to create a simpler alternative for HAZOP. SWIFT works to identify risks by stimulating the participants within a boundary by the facilitator using a set consisting of 'prompt' words or expressions with the help of systematic, group-based study. In order to examine how an organization, plant, system or any item will react to the small deviations from normal behaviour and operations, team and facilitators use standard phrases like 'what -if' with the prompts. The detail level of SWIFT is lower than the HAZOP and it is applied at a system level. Initially SWIFT was only designed for the hazard studies related to chemical and petrochemical plants, whereas this technique is now generally applied to organizations, plants, systems, procedures and items. The consequences of the risks and changes created or altered can be examined by utilizing it.

2.11. Failure modes and effects analysis (FMEA)

The failure of the systems, components or processes can be identified by Failure modes and effects analysis (FMEA). This technique determines:

- All potential modes of failure for a system or its parts.
- Systems behavior due to these failure
- The cause of the failure
- How these failures can be avoided, and their effect on the system can be reduced.

Each fault mode which is identified is ranked with respect to its criticality or importance by an extension of FMEA called FMECA. This analysis can be converted to quantitative analysis from qualitative by using the actual failure rates.

2.12. Fault tree analysis (FTA)

FTA is a methodology used to identify or analyse the factors that are the root cause of a specific undesired event which is known as a TOP EVENT. After the identification of fundamental factors, they are prioritized logically and then a diagram called fault tree diagram is used to represent them, which shows the logical relationship of fundamental factors with the top event. These factors can be those events which are related to the hardware failure of the components, human errors, or other events that are related to cause of any unwanted event. Fault tree can be used in both qualitative or quantitative way depending on what we have to find, to identify the root cause of the failure (Top event) we use it quantitatively and qualitatively in order to determine the top event probability with the probabilities of casual events.

2.13. Event tree analysis (ETA)

To represent graphically the sequences of events which are mutually exclusive and follow an initiating event based on the functioning or not functioning of the several systems those are designed to ease its results, an Event tree analysis (ETA) can be used. It can be used both in qualitative or quantitative ways. ETA can be used to rank, to model or to calculate various accident scenarios following an initiating event. For any phase in the system or product life cycle ETA can be used. It may be used qualitatively to insist in brainstorming possible event scenarios and its sequences which follow an initiating event and how different treatments can alter outcomes, barriers or controls intended to lessen the undesired outcomes.

The information is represented in either a tree diagram or sometimes in a Fishbone (also known as Ishikawa). Depending on the context the effect may be negative (a problem) or positive (an objective). ETA is used to consider that all the causes generated by a group of professional or experts, or scenarios possible and consents an accord to be developed as to the most possible causes that can then be evaluated by the assessment of data or empirically. To broaden thinking regarding possible causes at the start of an analysis is very valuable and afterwards to form a possible hypothesis that be taken in account more formally.

2.17. Decision tree analysis

Outcomes and decision alternatives are represented in a sequence by Decision tree, which also considers uncertain outcomes. Like an event tree, decision tree starts from an initial decision or event and depicts different outcomes and pathways that can originate from different decisions that may be made or events may occur. In case of uncertainty decision tree is used to select the

best line of action and to manage risks of the project. The graphical presentation of the decision tree can also help to link reasons for decisions.

2.18. Human reliability assessment (HRA)

To deal with human influence on the systems & to calculate influence of the human errors on the system Human reliability assessment (HRA) can be used. When the time is less to make decisions or to operate there are a lot of chances of human error in many processes. There is small probability that the problem can lead to a serious issue. In some cases, only actions performed by humans can avoid initially failure to prevent accident. HRA importance has been demonstrated by many accidents in which serious errors caused by humans led to disastrous sequence of events. These casualties are warning for the assessments of the risk which only focus on the software or hardware of the system. They show how dangerous it can be to ignore the contribution of the human errors. Additionally, HRA can be helpful in identifying errors that can reduce production and showing the way how operators or maintenance crew can recover these failures and errors. HRA can be used quantitatively to give data of failures caused by humans to other techniques like FTA or it can be used as qualitatively to reduce the probability of error by identifying the human error potential.

CASE STUDY [8]

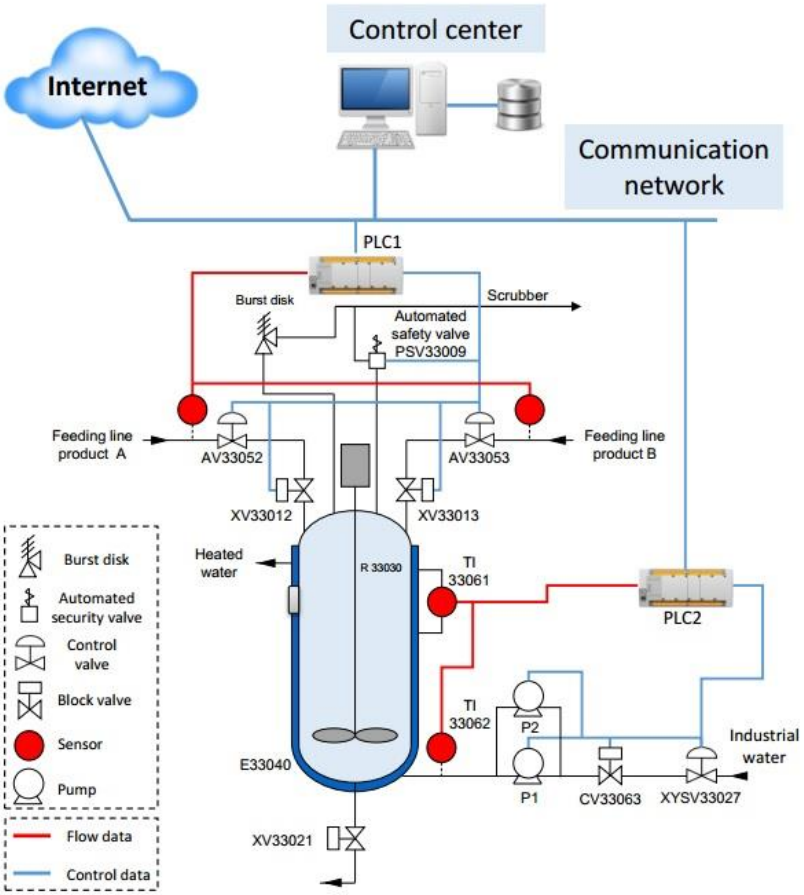


Figure 8: The chemical reactor with its SCADA system structure

Deviation/ Undesirable Scenario	Causes	Consequences	Automatic Protective Means
High Temperature	If the agitator breakdown	Very high temperature	
	Abnormal response of the cooling system		
Abnormal response of the cooling system	Failure of CV33063 fail closed	High temperature	
	TT Fails	High temperature	
	Pump Stuck/ Malfunction	High temperature	
	PLC2 Failure	High temperature	
Pump Stuck/ Malfunction	Pump1 fails	Abnormal response of the cooling system	Pump2 autopmatic startup
PLC 2Failure	Mechanical/Electrical Failure	Abnormal response of the cooling system	
	Security breach		
Security breach/ Attack on PLC	Unauthorized personnel have physical access to devices and equipment	PLC failure	
	SCADA is under attack	PLC failure	
	Unsecure remote access of ICS components	PLC failure	
Unauthorized personnel have physical access to devices and equipment		Security breach	
SCADA is under attack	Control center is compromised		
Unsecure remote access of ICS components			

REFERENCES

[1] P. R. Dunaka, "CYBER-PHYSICAL SECURITY OF A CHEMICAL PLANT," 2017.

[2] "Technical report, National Institute of Standards and Technology," 2004.

[3] M. Authors, "Glossary by Society for Risk Analysis (SRA)," 2004.

[4] *NOVA Chemicals Corporation Canada, from CARAT 2001,* Canada, 2001.

[5] A. Mullai, "RISK MANAGEMENT SYSTEM –RISK ASSESSMENT FRAMEWORKS AND TECHNIQUES," DaGoB publication, Turku, Finland, 2006.

[6] *Risk management Vocabulary (ISO/Guide 73:2009).*

[7] M. K. David VALIS, *SELECTED OVERVIEW OF RISK ASSESSMENT TECHNIQUES.*

[8] M. K. J.-M. F. F. M. H Abdo, *A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis,* 2017.