Risk Management

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources. Thanks to all authors and sources made those contents public and usable for educational purpose

Basics

- Vulnerability Assessment – Base Metric, Temporal Metric and Environment Metric.
- Vulnerability Scan
- Penetration Testing
- Security
- Safety
- Risk
- Risk Assessment
- Risk Management
- Fault Tolerance
- Resilience

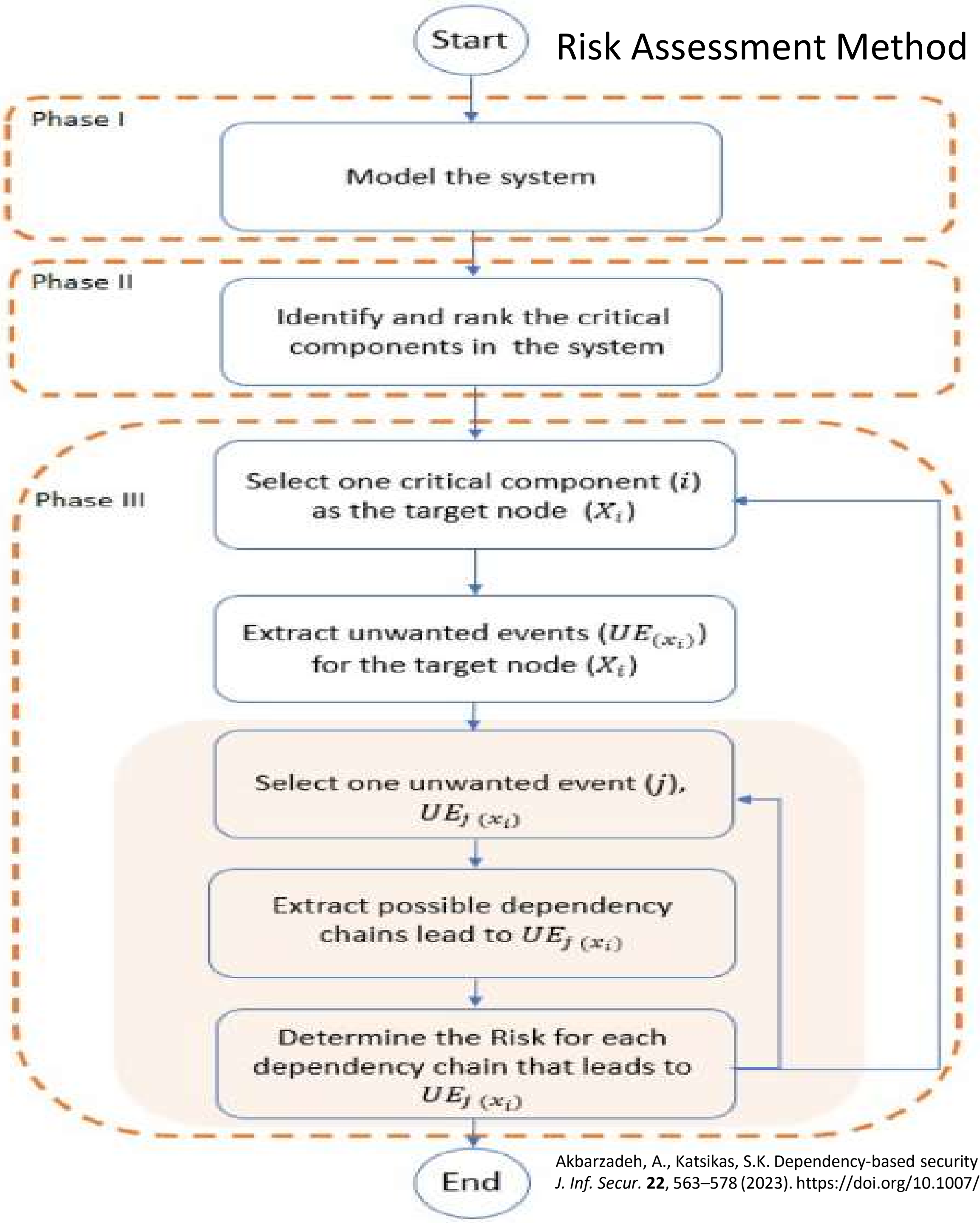
Introduction

- ISA 99/IEC62443 states risk assessment and management for a complete ICS.
  - Functional safety - functional safety is aimed at protecting and monitoring devices from accidental failures or failings in order to achieve or maintain a safe state of the process.
  - Physical safety - by hazards including explosions, fires, floods, chemical spills, biochemical spills and releases, potential crashes of vehicles etc.
  - Cybersecurity - to protect the cyber environment of the authorised users or organisation, including networks, devices, all software, processes, information in storage or transit etc.

Priorities

Priority	CPS	ITS
High	Availability	Confidentiality
Medium	Integrity	Integrity
Low	Confidentiality	Availability

Risk Assessment Method


Start
Phase I
Model the system
Phase II
Identify and rank the critical components in the system
Phase III
Select one critical component (i) as the target node (X_i)
Extract unwanted events ($UE_{(x_i)}$) for the target node (X_i)
Select one unwanted event (j), $UE_{j\ (x_i)}$
Extract possible dependency chains lead to $UE_{j\ (x_i)}$
Determine the Risk for each dependency chain that leads to $UE_{j\ (x_i)}$
End

Akbarzadeh, A., Katsikas, S.K. Dependency-based security risk assessment for cyber-physical systems. *Int. J. Inf. Secur*. **22**, 563–578 (2023). https://doi.org/10.1007/s10207-022-00608-4

Metric

- Access Vector – Remote, Adjacent, Local-Physical, Local-Cyber.

- Required Knowledge/Skills – High, Average, None.

- External Factors – Required (Opportunity) and None.

Impact

- Confidentiality
- Availability
- Integrity
- Economic Effect
- Public Effect
- Environment Effect

Risk Assessment Focus

- Identification of assets.
- Analysis of vulnerabilities.
- Evaluation and measurement of possible damages.

- **CPS Risk Management Solutions**
  - **Asset Inventory**.
  - **Risk Assessment.**
  - **Security Gaps**.
  - **Compliance**.
  - **Collaboration (**IT-IoT-OT**)**.

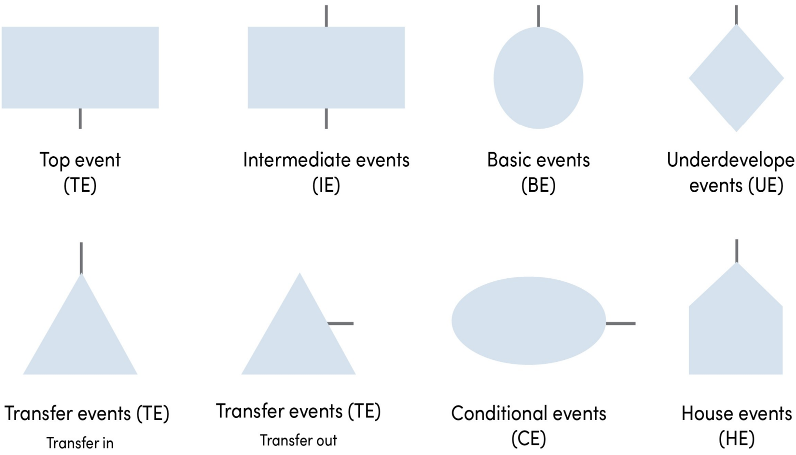
Risk Assessment Methods

- Qualitative assessment relies heavily on expert experience.

- Quantitative assessment can calculate the exact risk value of the system.

Fault tree analysis

Event symbol legend



Top event
(TE)

Intermediate events
(IE)

Basic events
(BE)

Underdeveloped
events (UE)

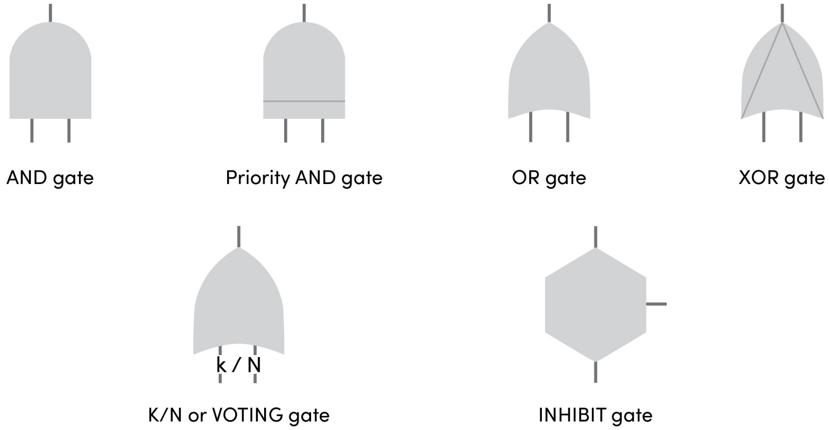
Transfer events (TE)
Transfer in

Transfer events (TE)
Transfer out

Conditional events
(CE)

House events
(HE)

Gate symbol legend



AND gate

Priority AND gate

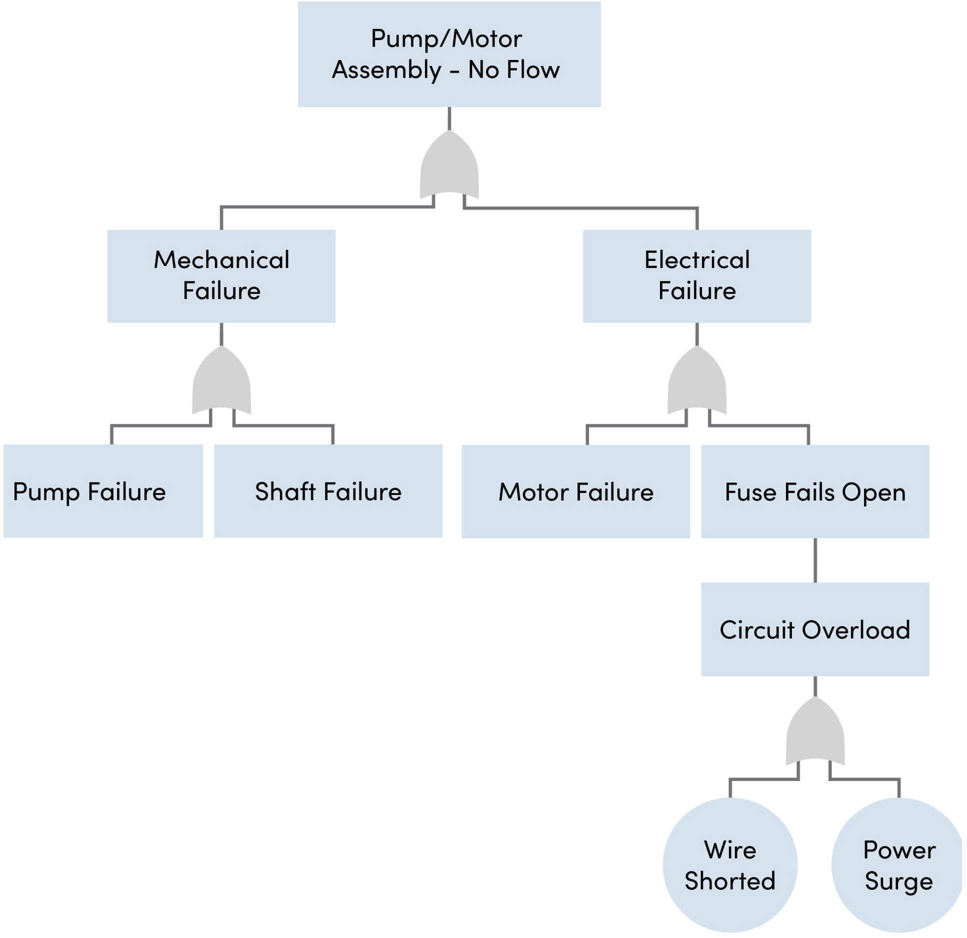
OR gate

XOR gate

k / N

K/N or VOTING gate

INHIBIT gate



Pump/Motor
Assembly – No Flow

Mechanical
Failure

Electrical
Failure

Pump Failure

Shaft Failure

Motor Failure

Fuse Fails Open

Circuit Overload

Wire
Shorted

Power
Surge

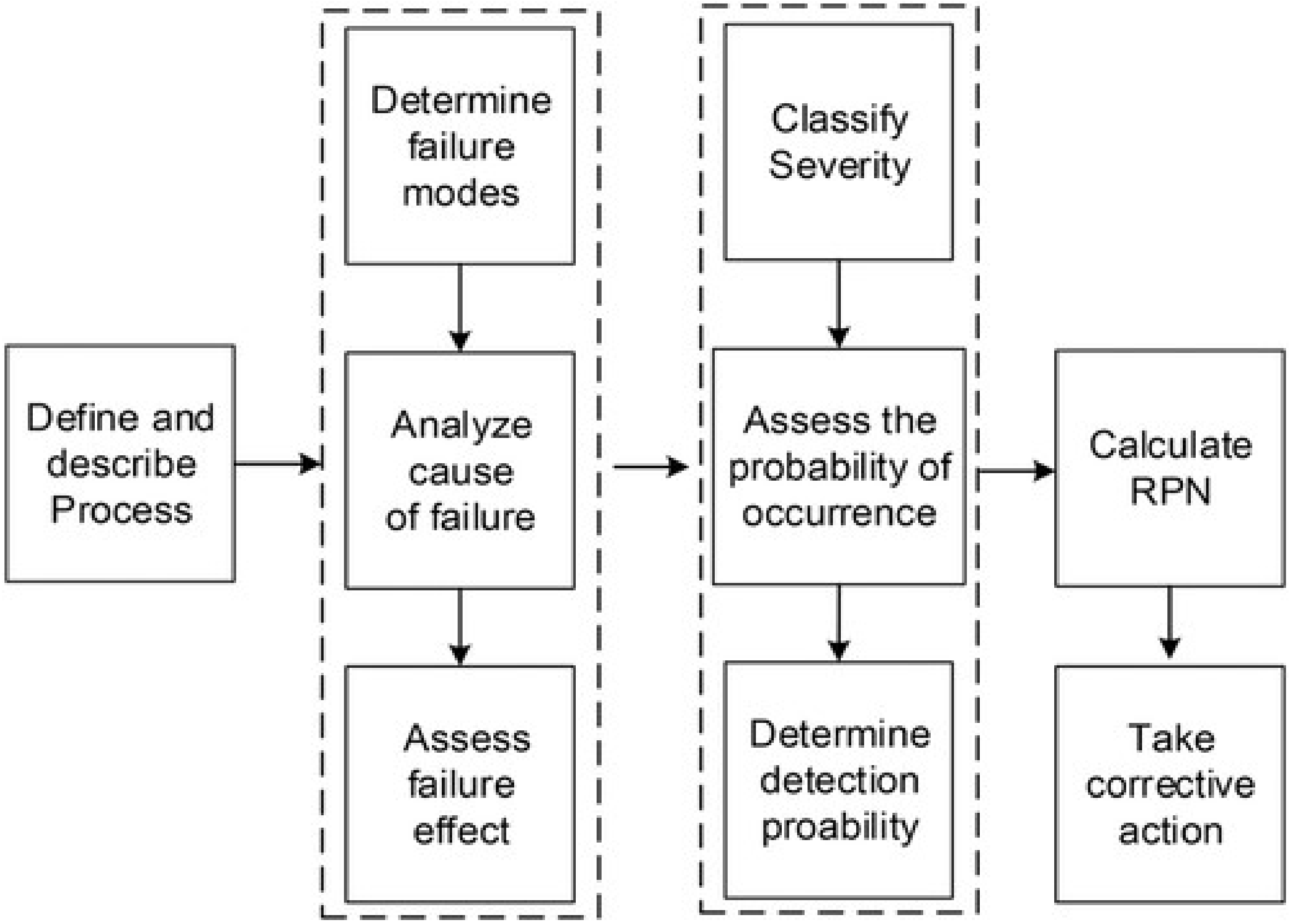
Failure modes and effects analysis

- A structured and team-based method for system safety analysis to recognise, evaluate, and score potential failures and their effects.

- Failure mode refers to the way in which something might fail, effect analysis is used to score the severity of various failure modes.

- The term risk priority number (RPN) is a part of FMEA quantitative analysis; it is the product of the severity, probability of occurrence, and detection probability.

FMEA

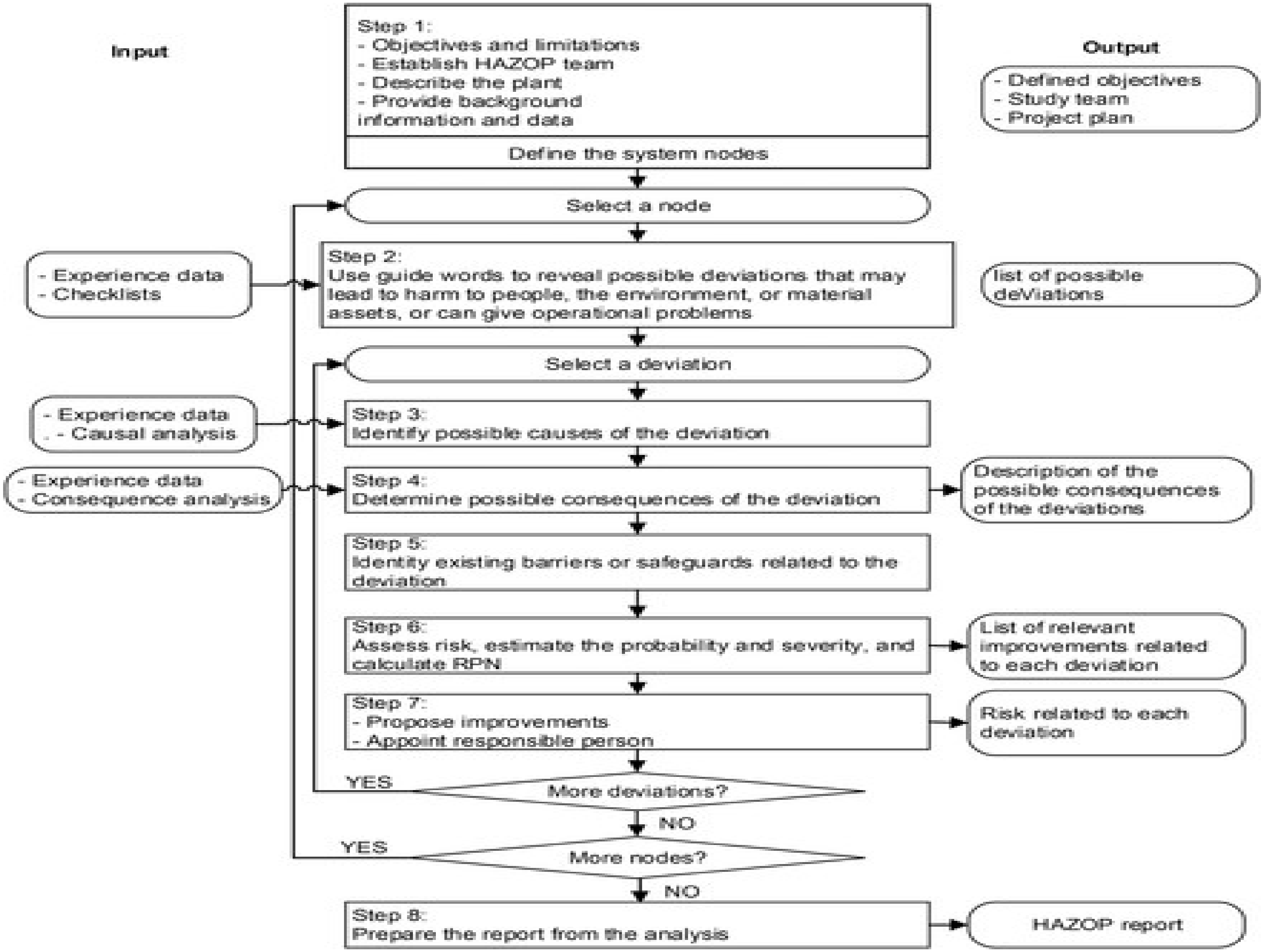

Define and describe Process
Determine failure modes
Analyze cause of failure
Assess failure effect
Classify Severity
Assess the probability of occurrence
Determine detection proability
Calculate RPN
Take corrective action

Hazard and Operability Methodology

- It is a process hazard analysis (PHA) technique
  - used worldwide for studying not only the hazards of a system
  - but also its operability problems, by exploring the effects of any deviation from design conditions.

- This analysis technique can identify
  - how a process deviates from its design intent and enters a fault or error state
  - by identifying possible hazards and potential operational problems in facilities

Steps



Input

Output

Step 1:
- Objectives and limitations
- Establish HAZOP team
- Describe the plant
- Provide background information and data

Define the system nodes

- Defined objectives
- Study team
- Project plan

Select a node

- Experience data
- Checklists

Step 2:
Use guide words to reveal possible deviations that may lead to harm to people, the environment, or material assets, or can give operational problems

list of possible deViations

Select a deviation

- Experience data
. - Causal analysis

Step 3:
Identify possible causes of the deviation

- Experience data
- Consequence analysis

Step 4:
Determine possible consequences of the deviation

Description of the possible consequences of the deviations

Step 5:
Identity existing barriers or safeguards related to the deviation

Step 6:
Assess risk, estimate the probability and severity, and calculate RPN

List of relevant improvements related to each deviation

Step 7:
- Propose improvements
- Appoint responsible person

Risk related to each deviation

YES

More deviations?

NO

YES

More nodes?

NO

Step 8:
Prepare the report from the analysis

HAZOP report

Model-based Engineering

- First, the procedure considers the system safety to determine a set of expected properties.

- Extracts properties of the physical environment, computing units and the cyber-physical interactions.

- Finally, analyses on the abstract model to evaluate the expected properties and verify safety requirements.

System Theoretic Process Analysis

- System Theoretic Process Analysis (STPA) has been developed by Nancy Leveson (2004) to identify unsafe control actions and hazardous states that may lead to system losses/accidents and generating detailed safety requirements to prevent the occurrence of the identified hazardous scenarios.

- STPA is a top-down process addressing system components interactions and hazards such as design errors, software, or component interaction failures.

- STPA can find more component interaction, software, and human hazards than traditional methods.

- An existing model, focuses particular attention on the role of constraints in safety management.

- Instead of defining safety in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations.

States

- Safe Failure
- Dangerous Failure
- No effect Failure

Security risk assessment in CPS

- Security risk assessment and management becomes a more and more important issue in CPS.

- When CPS are hacked by unauthorised users or under other malicious attacks, it could lead to the disclosure of important data and trigger a series of other major security issues.

- Security issue should be treated as important as safety issue in CPS.

Integration of safety and security risk assessment in CPS

- Safety and security share identical goals, which are protecting CPS from failing.
- Has mutual reinforcements (support each other), conditional dependencies.
- Weakening safety could enable malicious attackers and cause serious security incidents.
- On the other hand, the vulnerability in the CPS security protection could disable the system functions and lead to a degraded process performance, or even a disaster in the operations.
- If safety and security can work well together, there will be a solid foundation for Robust CPS.
- Safety and security issues are increasingly converging on CPS, leading to new situations in which these two closely interdependent issues should now be considered together, rather than separately or in sequence.

Resiliency

- In case the compromise happened due to a cyber-attack.

- It is the ability to come back to the required state of functionality/ performance from a compromised state of functionality.

- How fast or slow you will recover to the desired state.

Prioritize based on Risk to ensure Availability

Sl.No.	Attributes	Weight
1	Web Servers	
2	Firewall	
3	Proxy	
4	Leased Line 1	
5	Leased Line 2	
6	UPS Server Room	
7	Generator	
8	Main Power Supply	
9	Outside facing Router 1	
10	Outside facing Router 2	
11	Integrating Router	
12	Distribution Switch	
13	End Device (Computer, Laptop)	
14	LDAP	
15	Internal OFC from Server Room	
16	CAT 6 Cable connecting Individual Machine	
17	Individual Building L3 Switches	
18	Layer 2 switches	
19	Network Monitoring Device	
20	AVIR	
21	Access Point	
22	UPS Individual Building	
23	Solar Plant	
24	Light	
25	AC	
26	Fan	
27	Telephone Line	
28	Projector	
29	DMZ escape	
30	Subscription – Email	
31	Subscription – Webex	
32	Power Supply to Individual Building	
33	Individual building Network Wiring	
34	Wireless Controller	
35	Audio System	

References

- Xiaorong Lyu, Yulong Ding, Shuang-Hua Yang Safety and security risk assessment in cyber-physical systems

- https://www.linkedin.com/pulse/cyber-physical-systems-risk-management-critical-technology-bren