Control System HAZOP Methodology

JinHyung Park
Yokogawa Electric Korea
TUV Rheinland FS Expert

Safety Case
Symposium 2019
Singapore
Mar 26 - 27, 2019

YOKOGAWA

JinHyung Park

Yokogawa Electric Korea

FS Expert (TUV Rheinland, #158/10, SIS)

Outside Professor of Korea OSHA

Incident Example

Incident by control system failure

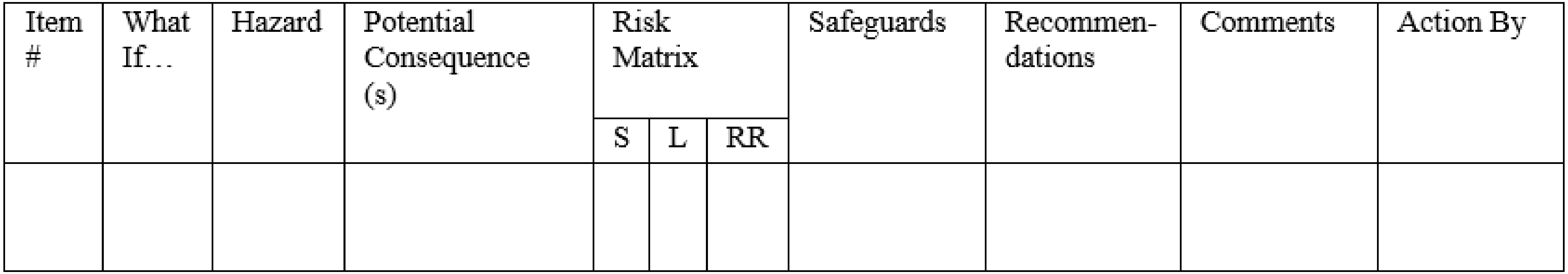
1999.6.10 Bellingham, Washington’s Whatcom Falls Park
Olympic Pipeline Company

3 fatalities, 8 injuries
Caused by SCADA system failure and relief valve failure

History of CHAZOP

History of CHAZOP

- BAPCO first developed the below Control System HAZOP format in 2005.
- BAPCO applied What-If analysis for Control System HAZOP.

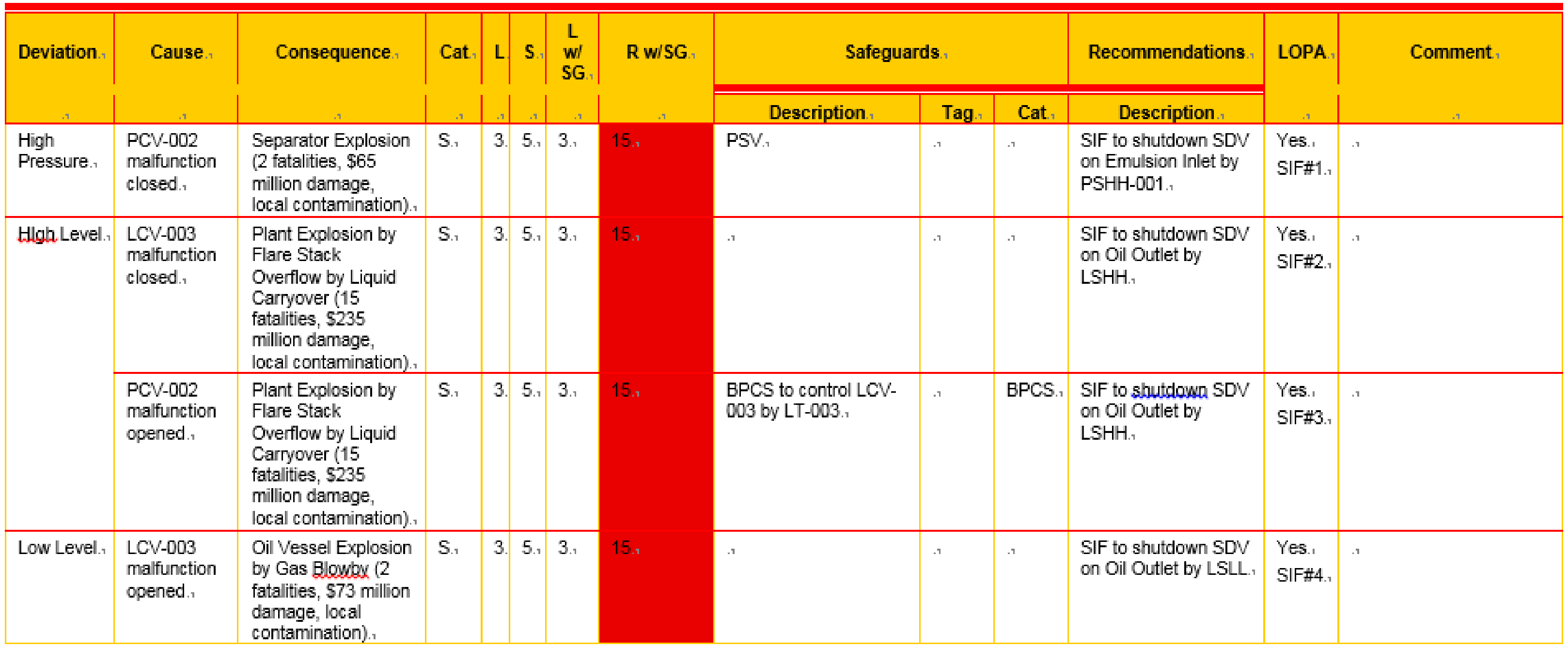


Item #	What If…	Hazard	Potential Consequence (s)	Risk Matrix			Safeguards	Recommen-dations	Comments	Action By
				S	L	RR				

Difference among HAZOP, FMEA and CHAZOP

The difference between HAZOP and CHAZOP

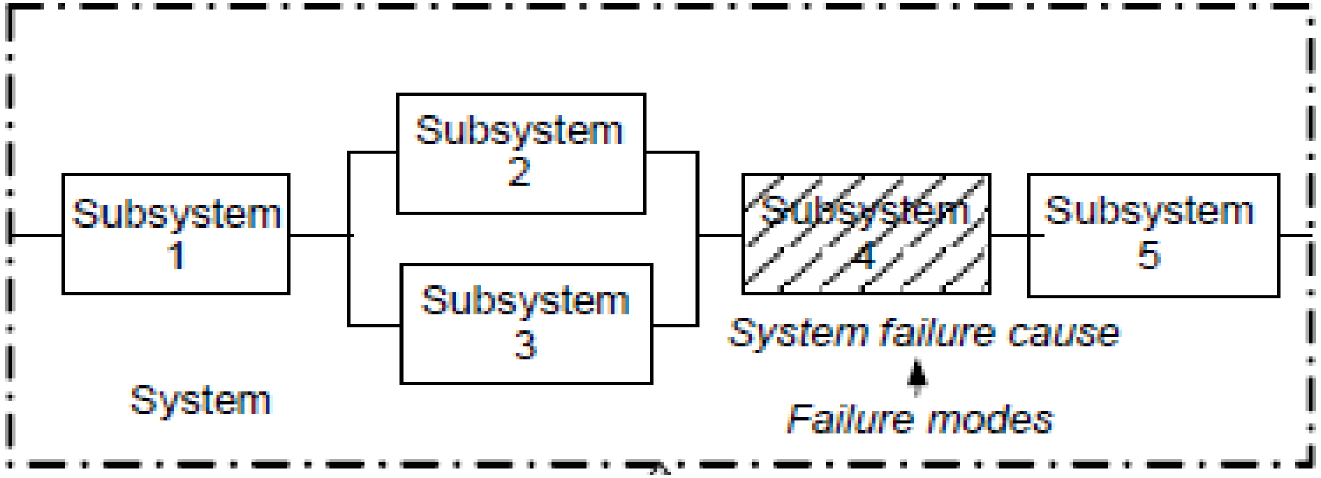
- HAZOP workshop is executed based on P&ID.
- The main causes of HAZOP report are sensor failure or final element failure of BPCS or field equipment failure.
- The failure of parts of control system in BPCS is missing parts in HAZOP methodology.



Deviation	Cause	Consequence	Cat	L	S	L w/ SG	R w/SG	Safeguards			Recommendations	LOPA	Comment
								Description	Tag	Cat	Description		
High Pressure	PCV-002 malfunction closed	Separator Explosion (2 fatalities, $65 million damage, local contamination)	S	3	5	3	15	PSV			SIF to shutdown SDV on Emulsion Inlet by PSHH-001	Yes SIF#1	
High Level	LCV-003 malfunction closed	Plant Explosion by Flare Stack Overflow by Liquid Carryover (15 fatalities, $235 million damage, local contamination)	S	3	5	3	15				SIF to shutdown SDV on Oil Outlet by LSHH	Yes SIF#2	
	PCV-002 malfunction opened	Plant Explosion by Flare Stack Overflow by Liquid Carryover (15 fatalities, $235 million damage, local contamination)	S	3	5	3	15	BPCS to control LCV-003 by LT-003		BPCS	SIF to shutdown SDV on Oil Outlet by LSHH	Yes SIF#3	
Low Level	LCV-003 malfunction opened	Oil Vessel Explosion by Gas Blowby (2 fatalities, $73 million damage, local contamination)	S	3	5	3	15				SIF to shutdown SDV on Oil Outlet by LSLL	Yes SIF#4	

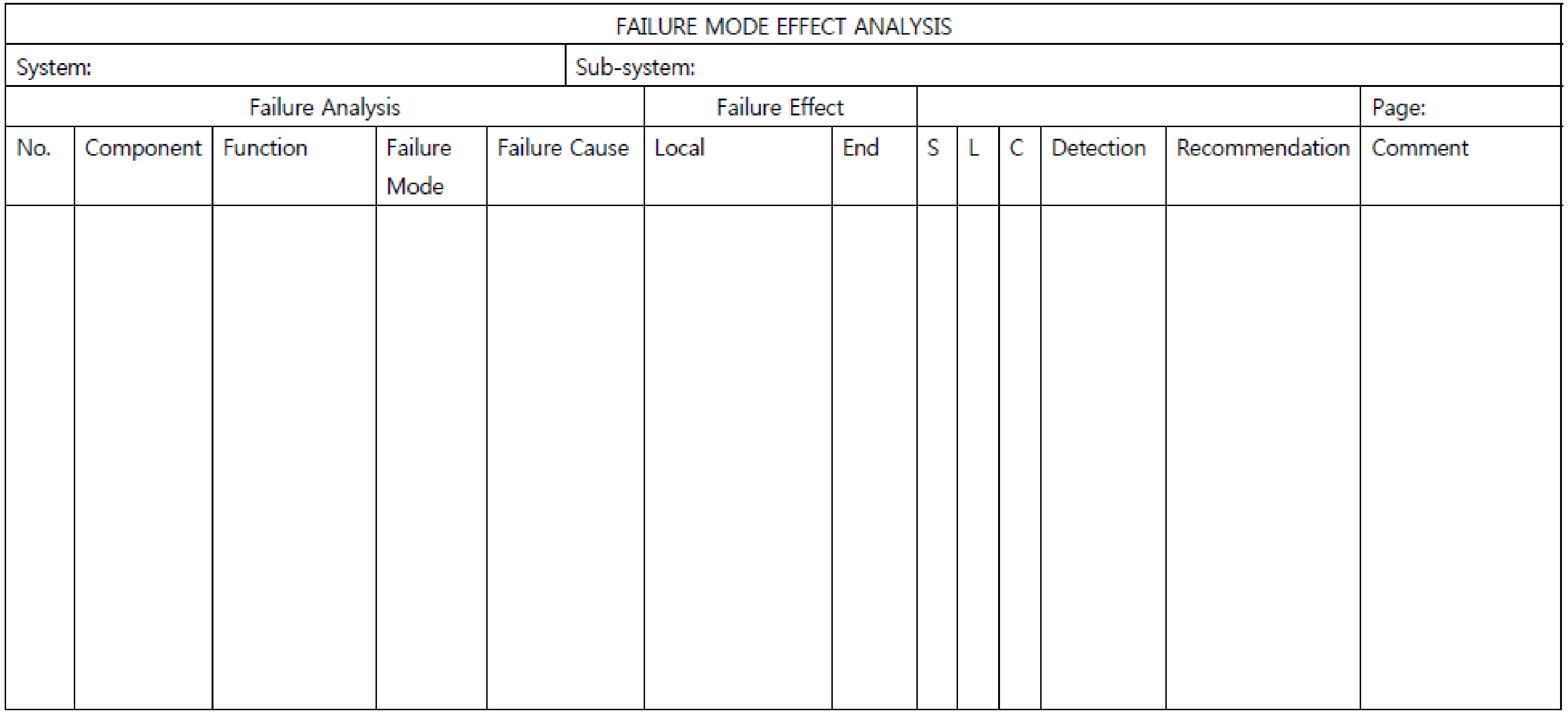
The difference between FMEA and CHAZOP

- The FMEA workshop is executed based on reliability block diagram.
- Common causes like general security failure, power failure, grounding failure, HVAC failure, time synchronization failure, fire detection failure are not discussed during FMEA.
- Countermeasures to common causes can be analysed during CHAZOP workshop.



The difference between FMEA and CHAZOP

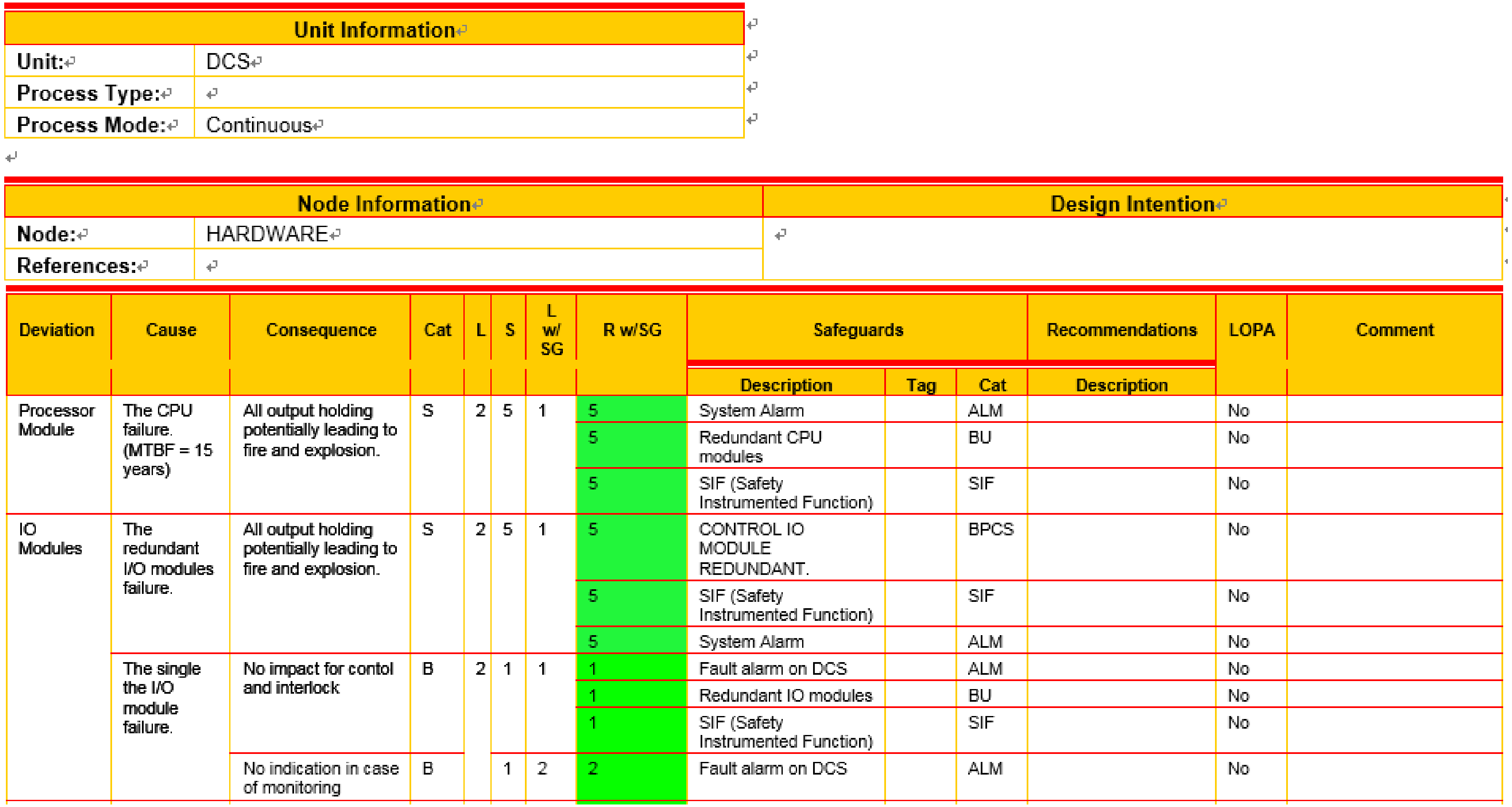
- Normal FMEA format



FAILURE MODE EFFECT ANALYSIS												
System:				Sub-system:								
Failure Analysis					Failure Effect							Page:
No.	Component	Function	Failure Mode	Failure Cause	Local	End	S	L	C	Detection	Recommendation	Comment

CHAZOP Detailed Methodology

CHAZOP Format and Example about Hardware Failure



Unit Information	
Unit:	DCS
Process Type:	
Process Mode:	Continuous

Node Information		Design Intention
Node:	HARDWARE	
References:		

Deviation	Cause	Consequence	Cat	L	S	L w/ SG	R w/SG	Safeguards			Recommendations	LOPA	Comment
								Description	Tag	Cat	Description		
Processor Module	The CPU failure. (MTBF = 15 years)	All output holding potentially leading to fire and explosion.	S	2	5	1	5	System Alarm		ALM		No	
							5	Redundant CPU modules		BU		No	
							5	SIF (Safety Instrumented Function)		SIF		No	
IO Modules	The redundant I/O modules failure.	All output holding potentially leading to fire and explosion.	S	2	5	1	5	CONTROL IO MODULE REDUNDANT.		BPCS		No	
							5	SIF (Safety Instrumented Function)		SIF		No	
							5	System Alarm		ALM		No	
	The single the I/O module failure.	No impact for contol and interlock	B	2	1	1	1	Fault alarm on DCS		ALM		No	
							1	Redundant IO modules		BU		No	
							1	SIF (Safety Instrumented Function)		SIF		No	
		No indication in case of monitoring	B		1	2	2	Fault alarm on DCS		ALM		No	

CHAZOP Methodology

Team effort:

- Facilitator (Chairman/ Scriber)
- Process Eng. (End User)
- Instrument Eng. (End User)
- System Eng. (Vendor)
- Safety Eng (part time, End User)
- Cyber Security Eng. (part time, Vendor)

Form : team brainstorm sessions

Basis: system configuration diagram

Use of component list (deviation cell)

Results:

Overview of all possible unwanted disturbances

Determine what safeguards are already in place

Recommendation for improvements of the process or required clarifications

Role and Responsibilities of CHAZOP Team Members

- Chairman: shall be independent from design engineering team and operation team and is responsible for concept and scope and shall propose methodology and is also responsible for the selection of parameter and review of CHAZOP report.
- Scriber: shall be the experienced system engineer and is responsible for CHAZOP report documentation.
- Coordinator: is responsible for the communication between CHAZOP team and system vendor and chairman and planning and scheduling CHAZOP.
- Process engineer: shall explain overall process and should actively join the discussion about consequence, safeguard and recommendation and the revamping period and cost after asset failure.
- Security Engineer: Check and consult if there is any missing equipment in relation with security
- Instrument engineer (End User): shall propose the replacement cycle of computer and the revamping period and cost after asset failure.

Input Documents and Questions of CHAZOP

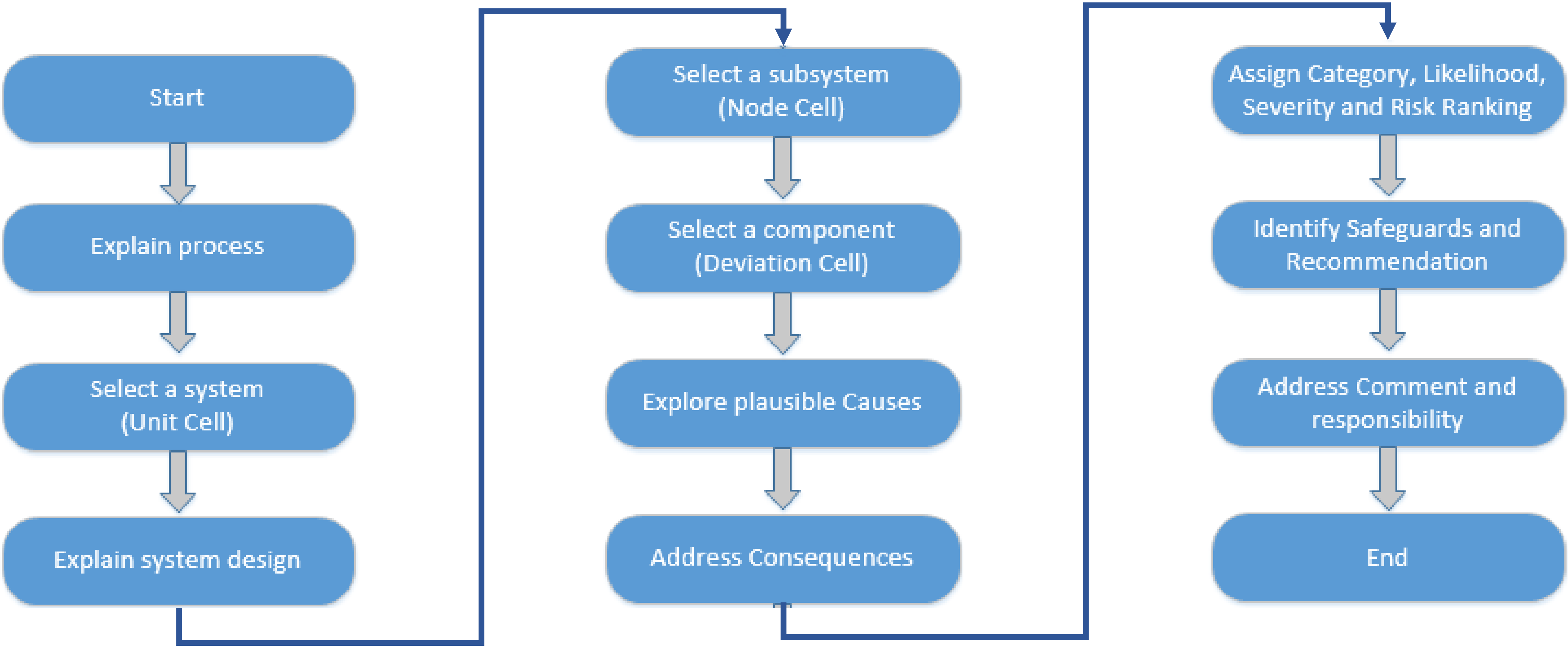
Critical Documents:

- HAZOP Report
- PFD
- System Configuration
- Controller architecture
- Typical loop configuration

Items to be questioned:

- System alarm philosophy
- Control philosophy
- Fail safe concept
- Maintenance philosophy
- Provision for fault detection and switchover
- Environment protection
- Security and access control

CHAZOP Procedure


Start

Explain process

Select a system
(Unit Cell)

Explain system design

Select a subsystem
(Node Cell)

Select a component
(Deviation Cell)

Explore plausible Causes

Address Consequences

Assign Category, Likelihood, Severity and Risk Ranking

Identify Safeguards and Recommendation

Address Comment and responsibility

End

How to Determine Likelihood and Severity

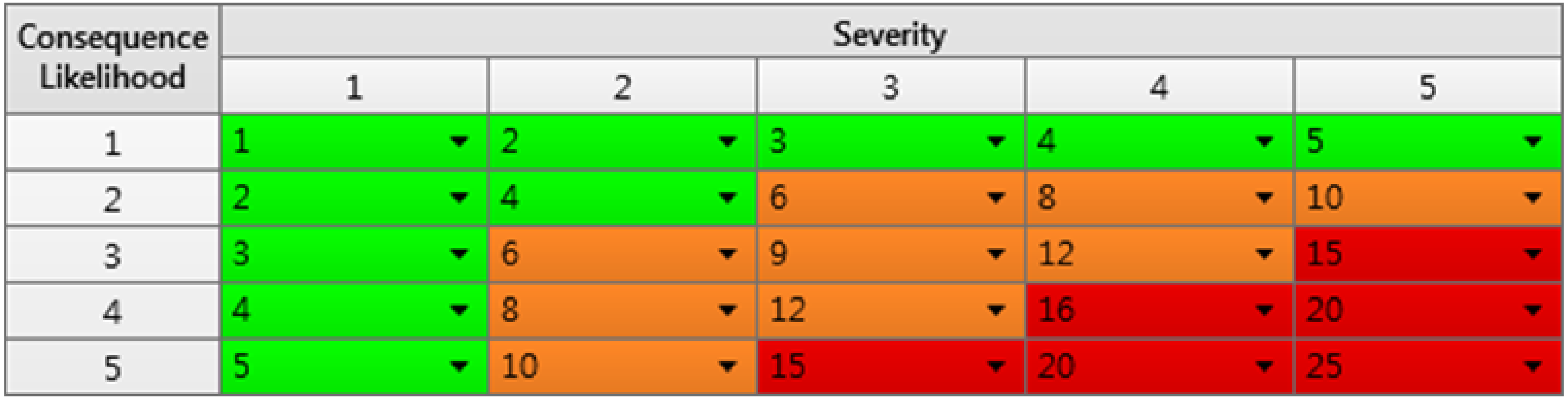
LIKELIHOOD

- LOPA initiation likelihood criteria table shall be referred to, to determine the likelihood of HAZOP. It is recommended that CHAZOP risk ranking matrix shall be made based on HAZOP risk criteria.

SEVERITY

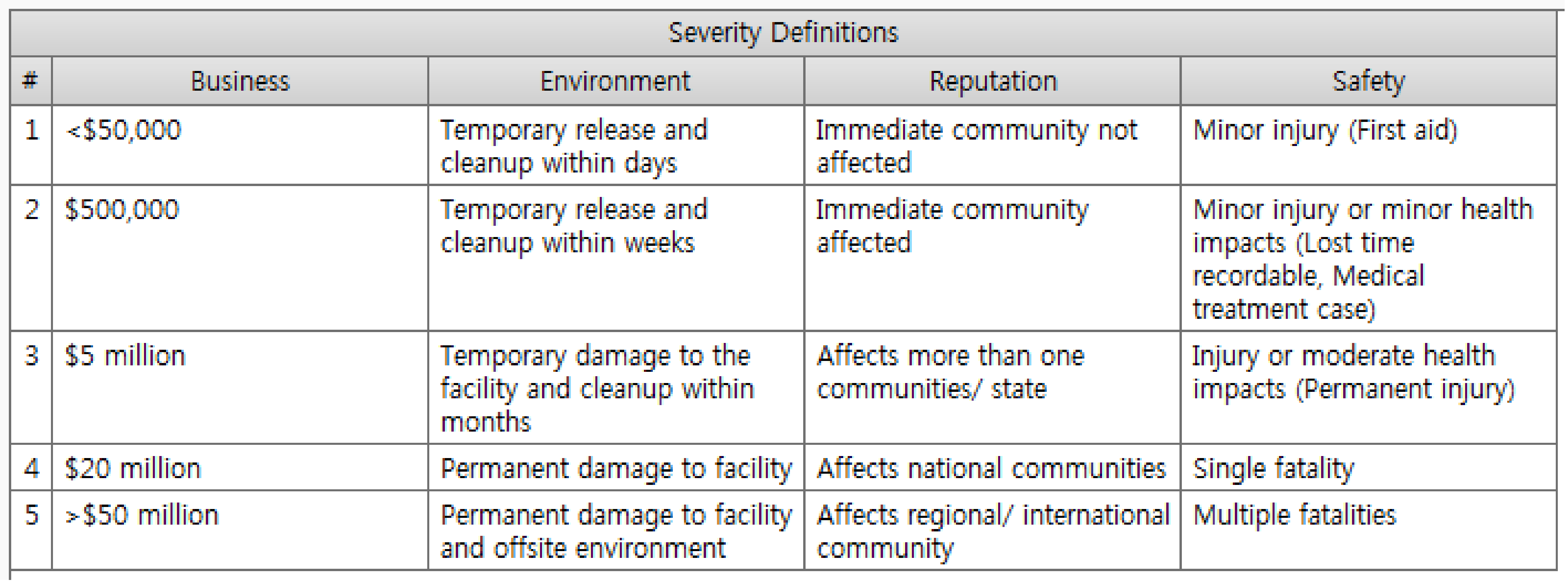
- Severity shall be determined not considering the safeguard activation. Suppose that there is no safeguard and then determine the severity of consequence. It is recommended that CHAZOP risk ranking matrix shall be made based on HAZOP risk criteria.

Risk Ranking



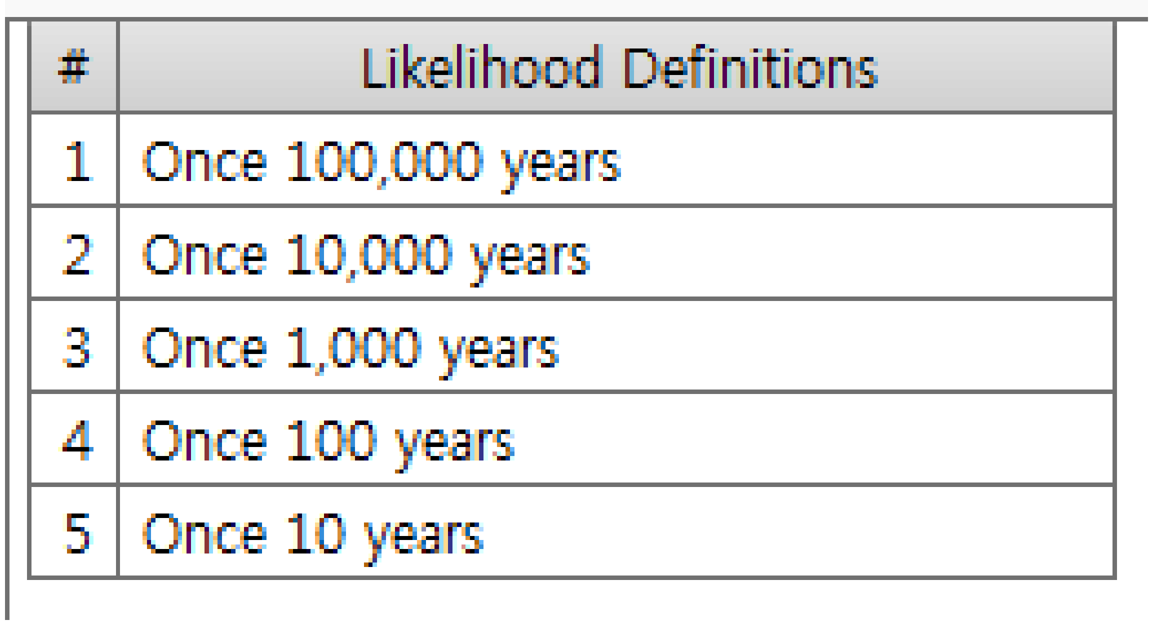
Consequence Likelihood	Severity				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Risk Ranking (S: Severity)



Severity Definitions				
#	Business	Environment	Reputation	Safety
1	<$50,000	Temporary release and cleanup within days	Immediate community not affected	Minor injury (First aid)
2	$500,000	Temporary release and cleanup within weeks	Immediate community affected	Minor injury or minor health impacts (Lost time recordable, Medical treatment case)
3	$5 million	Temporary damage to the facility and cleanup within months	Affects more than one communities/ state	Injury or moderate health impacts (Permanent injury)
4	$20 million	Permanent damage to facility	Affects national communities	Single fatality
5	>$50 million	Permanent damage to facility and offsite environment	Affects regional/ international community	Multiple fatalities

Risk Ranking (L: Likelihood)



#	Likelihood Definitions
1	Once 100,000 years
2	Once 10,000 years
3	Once 1,000 years
4	Once 100 years
5	Once 10 years

Cause and Consequence

- The cause of control system HAZOP shall be any unit which can be replaced during maintenance.
- Even though the purpose of control system HAZOP is to study the effect after the failure of components of control system, the components to be analyzed cannot be the detailed components inside each module like diode, microprocessor and transistor, etc.

Double Jeopardy :

- Double Jeopardy rule shall be applied during Control System HAZOP workshop.
- Only one failure or cause shall be written on cause cell.
- Double jeopardy doesn’t mean that cause and safeguards cannot fail at the same time.
- Consequence shall be written under the condition that the cause and all of safeguards fail at the same time. If somebody assume that safeguards and cause does not fail at the same time, double jeopardy rule cannot be applied and a lot of scenarios shall be analyzed accordingly.

Overall System Scope (Unit)

- Distributed Control System
- General Security
- PIMS
- OPC
- Printer
- Safety Instrumented System
- FGS
- Turbine Control System
- Vibration Monitor / Machine Monitoring System
- Motor Control System
- Local Control Panel
- Analyser

Overall Subsystem Scope (Node)

- Hardware
- Software
- Cabinet components
- Individual security
- Common mode failure
- Data interfacing between other systems
- Other failures

Overall Items of General Security (Deviation)

- Physical access restriction
- Logical access restriction
- Restricting unauthorized modification of data
- Incident detection and response plan

System Hardware Scope (Deviation)

- Processor modules
- I/O module
- Hard disks
- Chassis / node communication modules
- Chassis / node power supplies
- Network device failures (L2 Switches, FO converters)
- Network cables and bus
- IO BUS (among chassis / node)
- Grounding
- Filters
- Fan
- EWS / OWS monitors
- EWS / OWS workstations

System Software Scope (Deviation)

- Operating software
- Application software
- Database configuration

Cabinet (Deviation)

(Marshalling / Relay / Auxiliary Console)

- Cabinet Power Supplies
- Barrier / Isolator
- Relay
- System Cable
- Annunciator
- Push Button
- Grounding
- Filters
- Fan

Individual Security (Deviation)

- Physical access restriction
- Individual ICS components prevention
- Restricting unauthorized modification of data

Common Mode Failures Scope (Deviation)

- Power failure and grounding
- Routing of communication cables
- HVAC
- Dust
- Fire detection and protection

Data Interfacing between Other System (Deviation)

- Communication devices (communication modules, L2 switch, FO converter)
- Cables
- Interface programs (Modbus address mapping, OPC)

Other Failures (Deviation)

- System loading / Scan time
- Network loading
- Field device
- Time synchronization
- EMI / Lightening protection

Safeguards and Recommendations

- Failure detection
- Redundancy
- Separation
- SIF
- PSV
- Other system
- Diode
- Fuse

- Armored cable
- Filter
- Overhaul cleaning service by annual maintenance service
- Fire and gas system
- Quality management by ISO9000
- GPS time synchronization

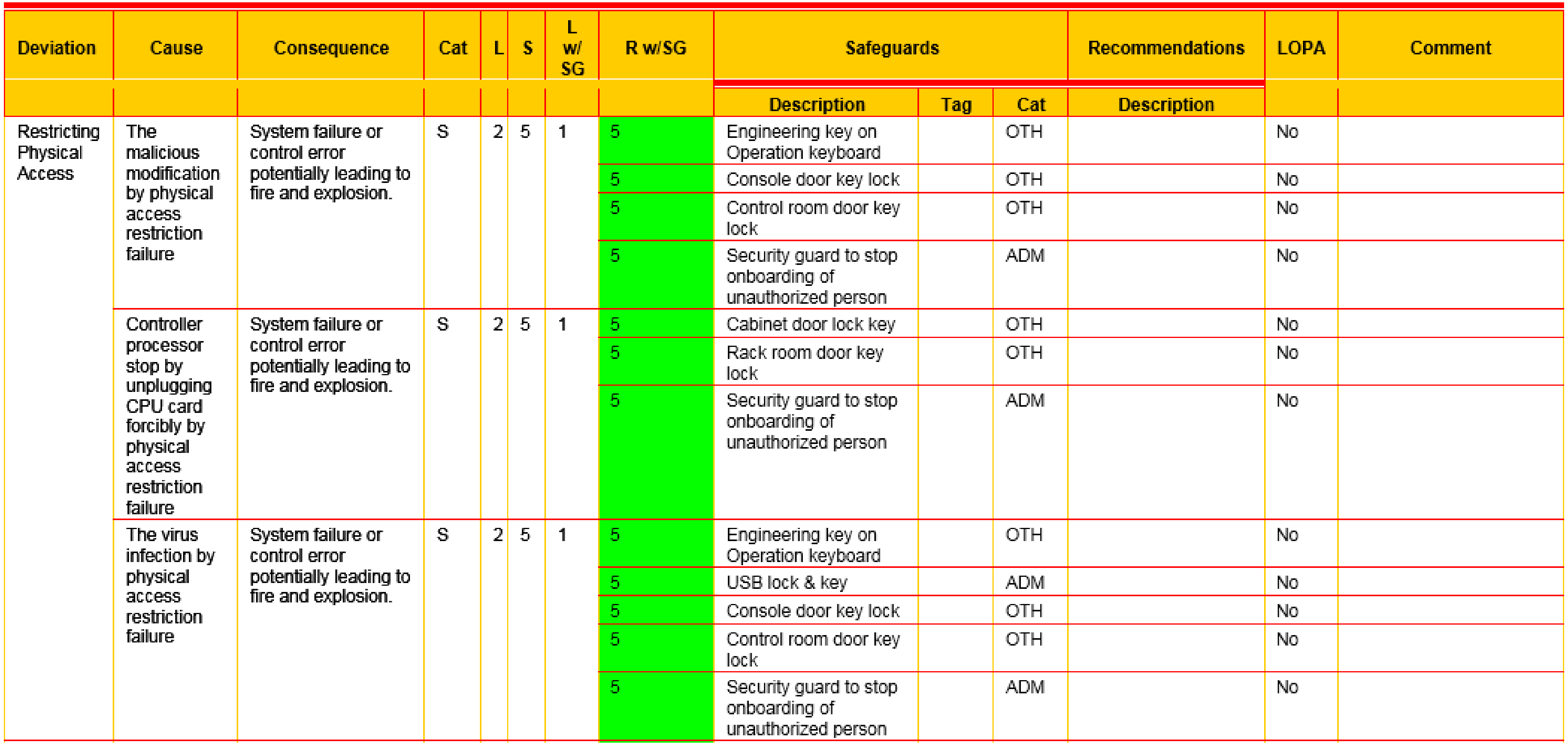
Safeguards and Recommendations (General Security)

- Physical access restriction
  - Guards
  - Cabinet / Room Door Key
- Logical access restriction
  - DMZ network architecture with firewall
  - Unidirectional gateway (e.g. data diode)
  - Central authentication system (e.g. Microsoft Active Directory, LDAP, Kerberos, RADIUS, TACACS+)
  - MAC (Message Authentication Code)
- Incident detection and response plan
  - Incident detection
  - Incident response plan
  - System recovery plan

Safeguards and Recommendations (Individual Security)

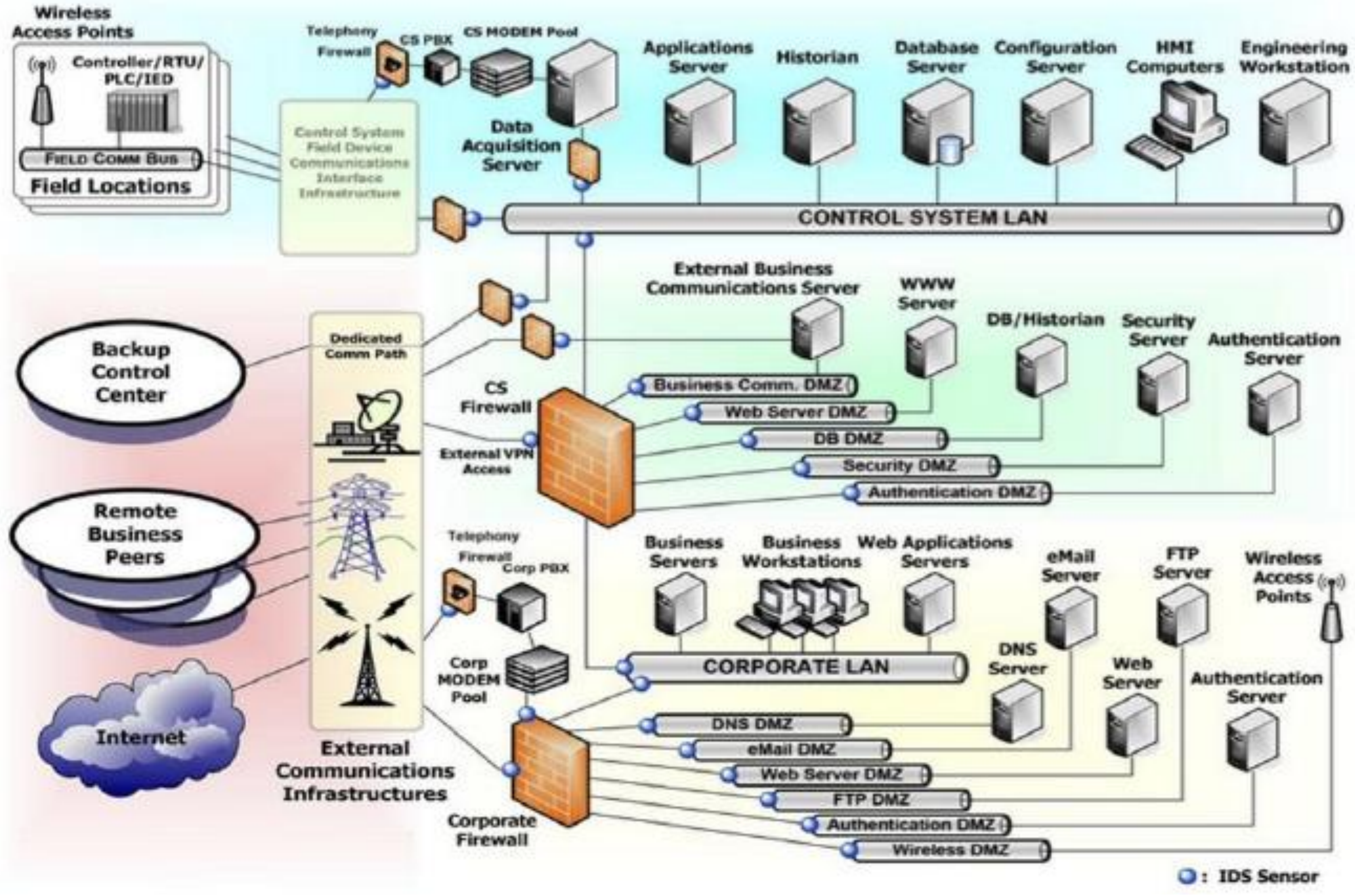
- Physical access restriction
  - Lock
  - Card reader for personal identity verification (authentication)
  - USB lock & key
- Individual ICS components prevention
  - Disabling all unused ports
  - Antivirus software
  - ICS user privilege (authorization)
  - File integrity checking software for malware detection
  - Security audit
  - Intrusion detection software
  - Critical component redundant
- Restricting unauthorized modification of data
  - Central authentication system (e.g. Microsoft Active Directory, LDAP, Kerberos, RADIUS, TACACS+)
  - MAC (Message Authentication Code)

Example of CHAZOP about Security (Physical Access)

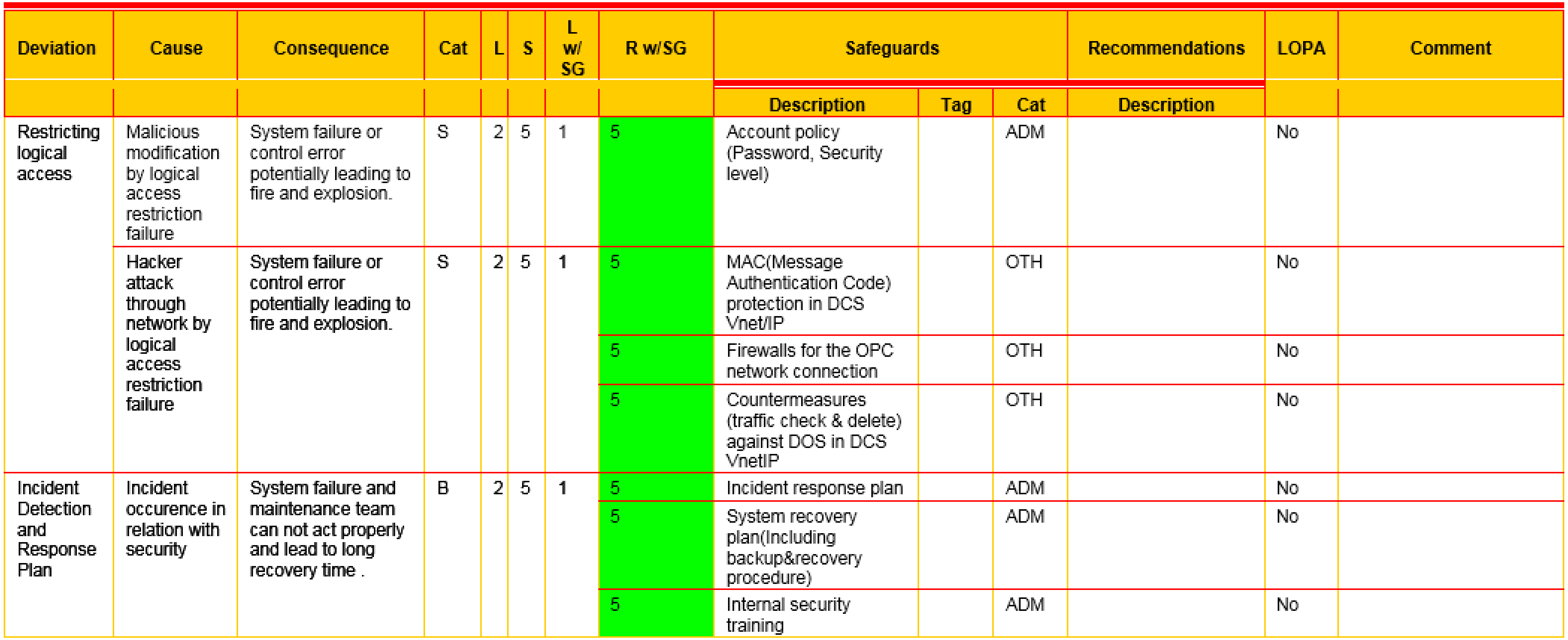


Deviation	Cause	Consequence	Cat	L	S	L w/ SG	R w/SG	Safeguards			Recommendations	LOPA	Comment
								Description	Tag	Cat	Description		
Restricting Physical Access	The malicious modification by physical access restriction failure	System failure or control error potentially leading to fire and explosion.	S	2	5	1	5	Engineering key on Operation keyboard		OTH		No	
							5	Console door key lock		OTH		No	
							5	Control room door key lock		OTH		No	
							5	Security guard to stop onboarding of unauthorized person		ADM		No	
	Controller processor stop by unplugging CPU card forcibly by physical access restriction failure	System failure or control error potentially leading to fire and explosion.	S	2	5	1	5	Cabinet door lock key		OTH		No	
							5	Rack room door key lock		OTH		No	
							5	Security guard to stop onboarding of unauthorized person		ADM		No	
	The virus infection by physical access restriction failure	System failure or control error potentially leading to fire and explosion.	S	2	5	1	5	Engineering key on Operation keyboard		OTH		No	
							5	USB lock & key		ADM		No	
							5	Console door key lock		OTH		No	
							5	Control room door key lock		OTH		No	
							5	Security guard to stop onboarding of unauthorized person		ADM		No	

CSSP Recommended Defense-In-Depth Architecture



Example of CHAZOP about Security (Logical Access)



Deviation	Cause	Consequence	Cat	L	S	L w/ SG	R w/SG	Safeguards			Recommendations	LOPA	Comment
								Description	Tag	Cat	Description		
Restricting logical access	Malicious modification by logical access restriction failure	System failure or control error potentially leading to fire and explosion.	S	2	5	1	5	Account policy (Password, Security level)		ADM		No	
	Hacker attack through network by logical access restriction failure	System failure or control error potentially leading to fire and explosion.	S	2	5	1	5	MAC(Message Authentication Code) protection in DCS Vnet/IP		OTH		No	
							5	Firewalls for the OPC network connection		OTH		No	
							5	Countermeasures (traffic check & delete) against DOS in DCS VnetIP		OTH		No	
Incident Detection and Response Plan	Incident occurence in relation with security	System failure and maintenance team can not act properly and lead to long recovery time .	B	2	5	1	5	Incident response plan		ADM		No	
							5	System recovery plan(Including backup&recovery procedure)		ADM		No	
							5	Internal security training		ADM		No	

Conclusion

Conclusion

- There are several merits of CHAZOP compared with FMEA and HAZOP.
- The more items including general security failure, power failure, grounding failure, HVAC failure, time synchronization failure, fire detection failure can be discussed and reported during CHAZOP compared with FMEA.
- In this paper, the CHAZOP report has same format as normal HAZOP, so the title of each row can be confused. The CHAZOP guideline shall clearly describe the detailed methodology to prevent this kind of confusion.

Thank you for your listening.

JinHyung Park

Yokogawa Electric Korea

e-mail: jinhyung.park@kr.yokogawa.com

Safety Case
Symposium 2019
Singapore
Mar 26 - 27, 2019
www.SafetyCaseSymposium.com