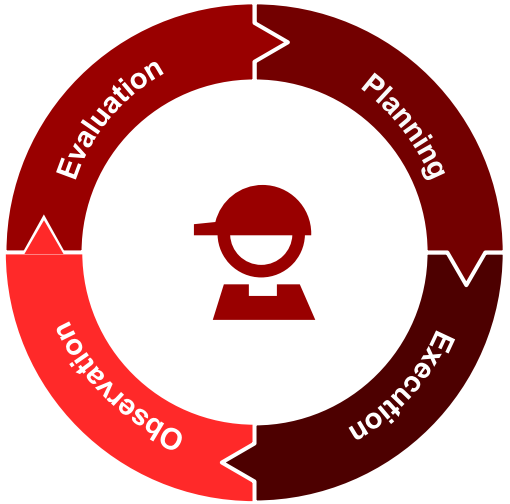
Recap from Lecture1

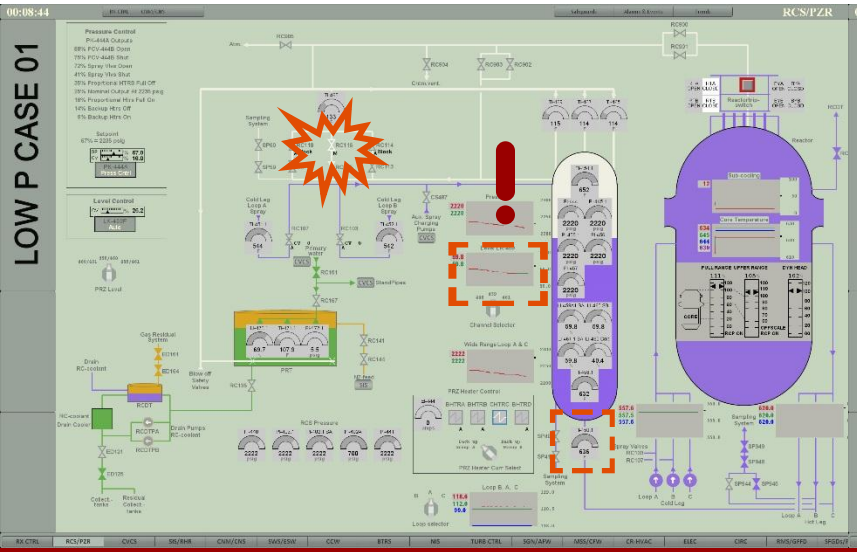
- 5 ECTS, project-based course

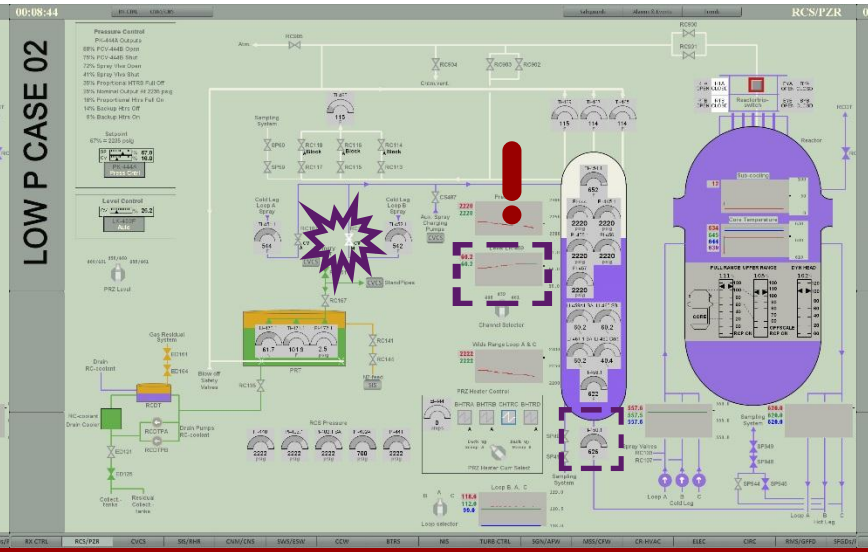
- Problem formulation
  - Troubleshooting is a routine practice in the control rooms.
  - Where is the process knowledge?
  - If we should adopt or develop a method for operator support, what factors are important?

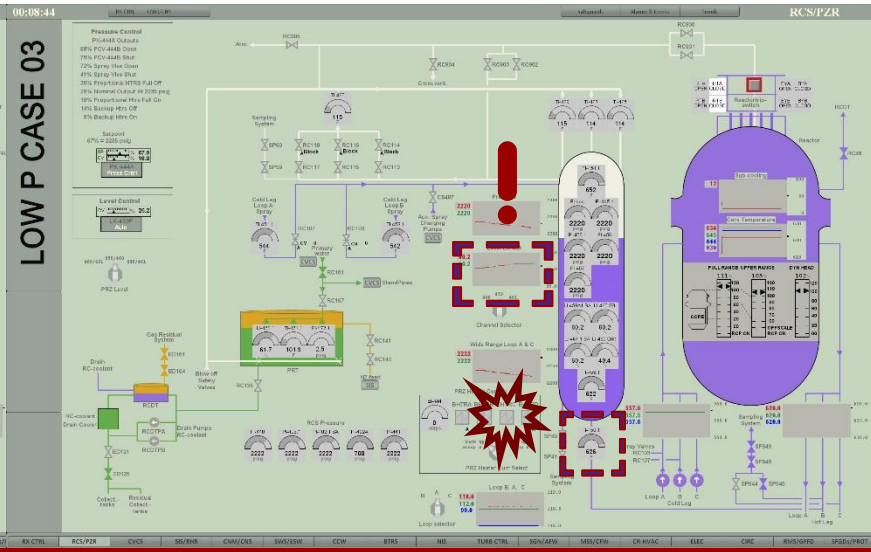
Provide support to human operators



Three low pressure cases, with different indicators support three different causes.







Lecture 2

Abnormal Situation and Hazard Identification

Discussion

- Why do we need control systems?
- Why do we need alarm systems?
- How do they related to system safety?

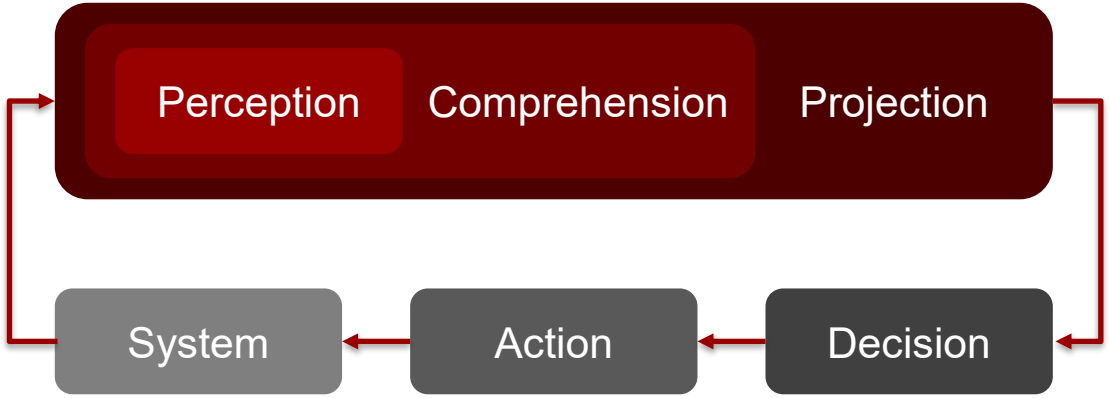
Abnormal Situation

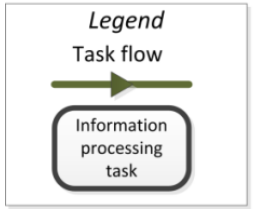
- Deviation from normal situation
  - Perceived abnormality
  - Actual abnormality

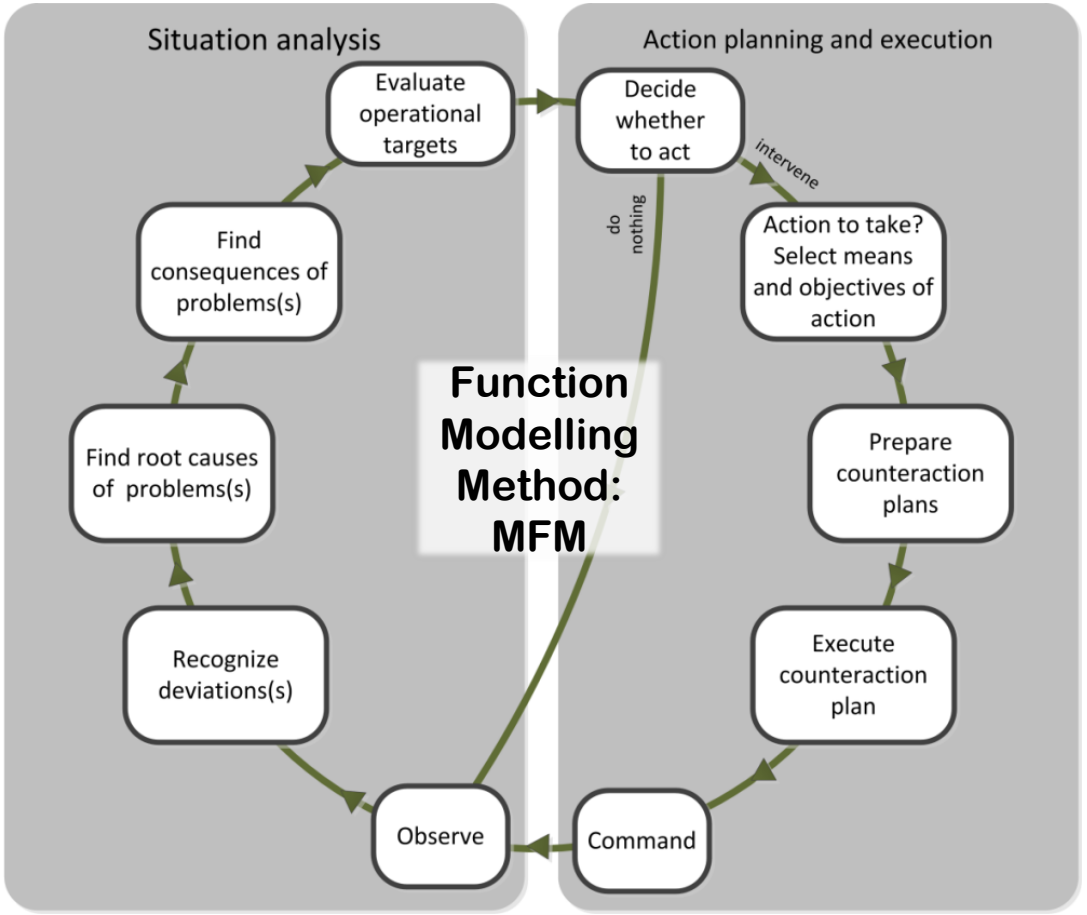
- Situation Awareness

Support situation awareness in the control rooms

- The model of “situational awareness“ or “situation awareness“, as defined by Endsley in 1995.







Alarm Systems

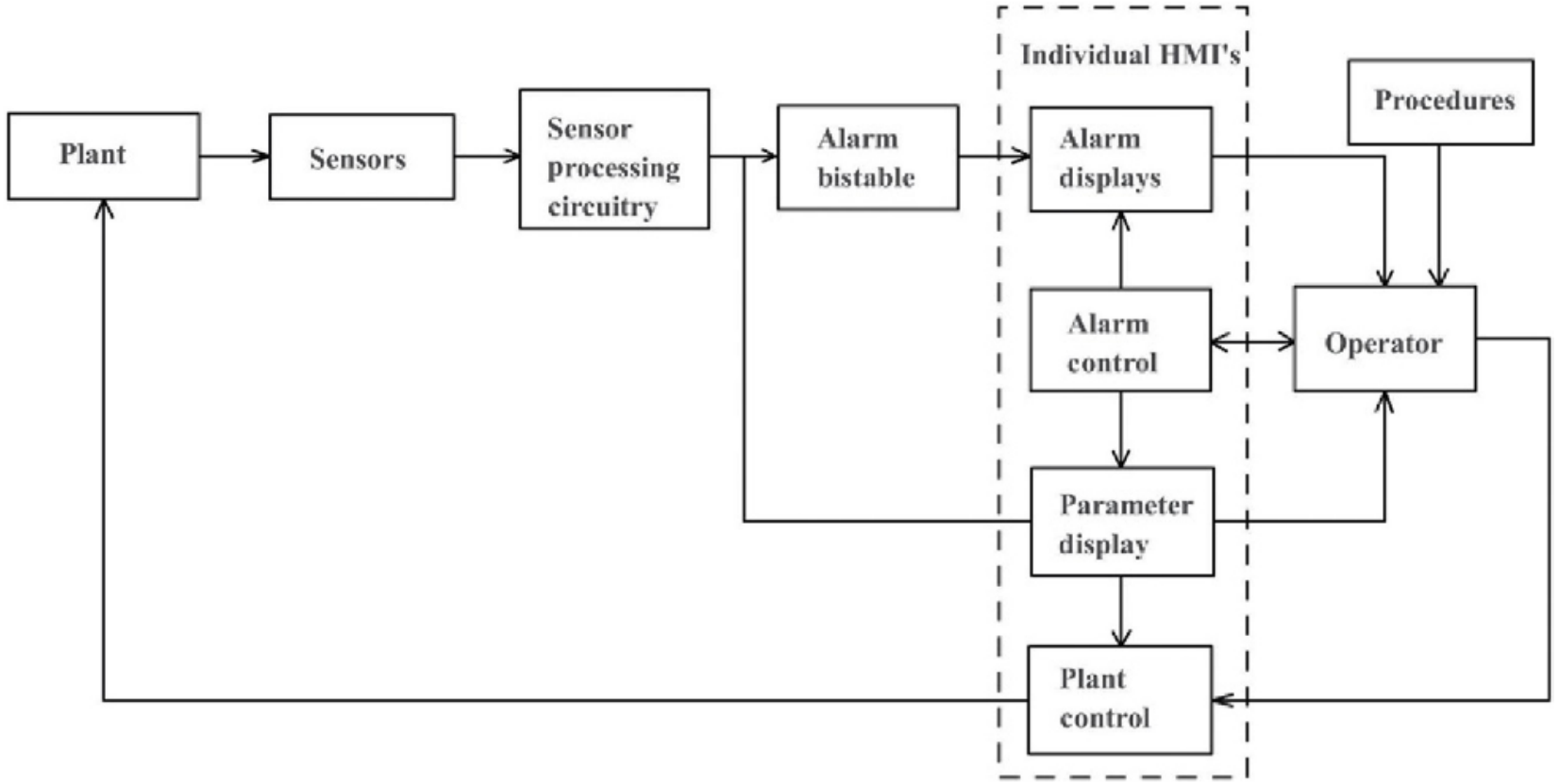


FIGURE 21.1

Conventional alarm system

Alarm Systems

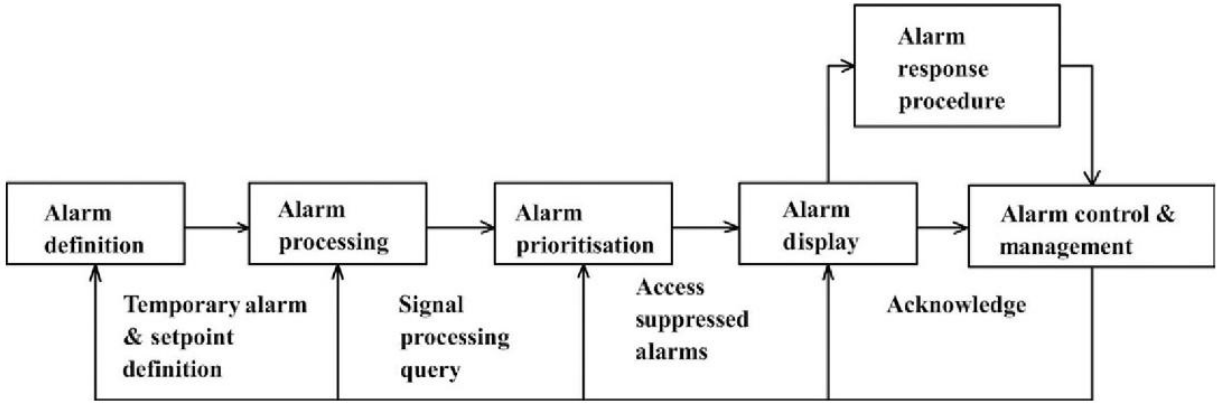


FIGURE 21.3

Alarm system functional elements

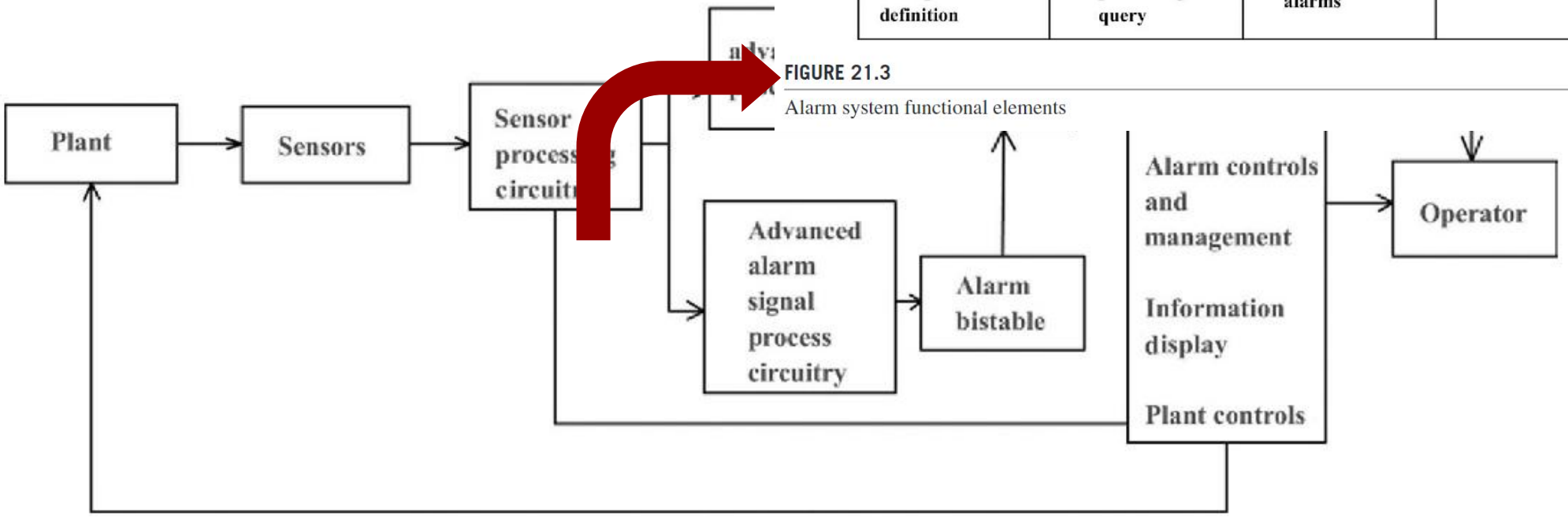


FIGURE 21.2

Advanced alarm system

Alarm Systems

- To support situational awareness for control room operators, we may want to provide information of:
  - Interpretation of alarm patterns and propose what to do about it.
- We want to mimic human problem solving procedure so the provided knowledge is explanable and trusted.
- Where to find the causal knowledge?
  - Before a system goes into operation, process knowledge is established and documented.

Causality in engineered systems

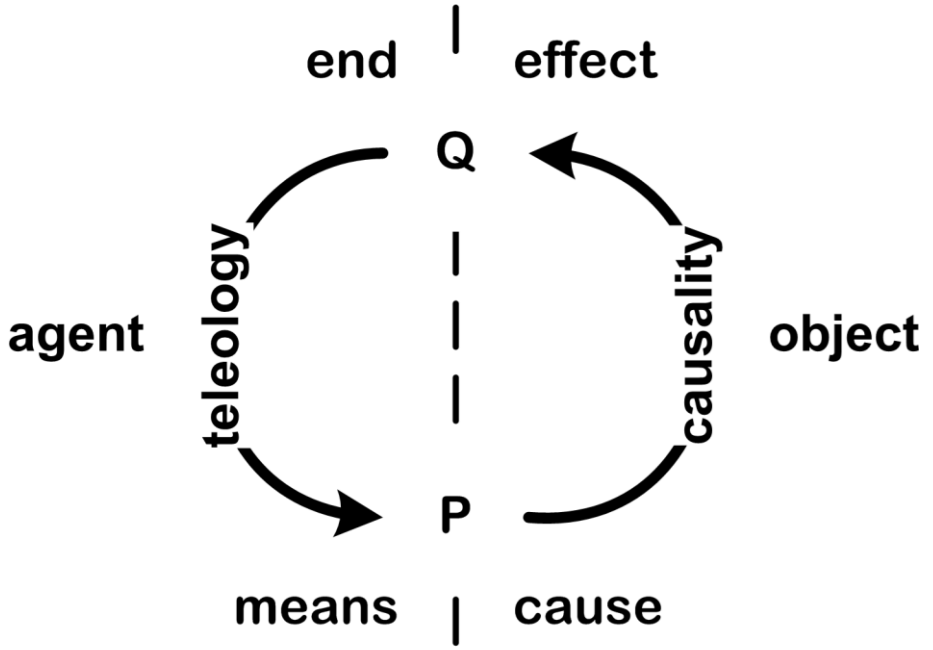
- The knowledge involved in the plant-wide diagnosis process root deeply in the nature of the engineered systems (artifacts). They are built as means to achieve an end.

- Teleology perspective
  - Teleology is a reason or explanation for something in function of its end, purpose or goal.
  - Engineered system is build in such a way that the physical system is used to realize some functions in order to reach a certain goal.

- Causality perspective
  - The selected means to realize the end has to have the capability to cause the effect that specified by the end.

What is a failure?

Deviation from normal behavior, deviation from achieving the goal.



System Development Life Cycle

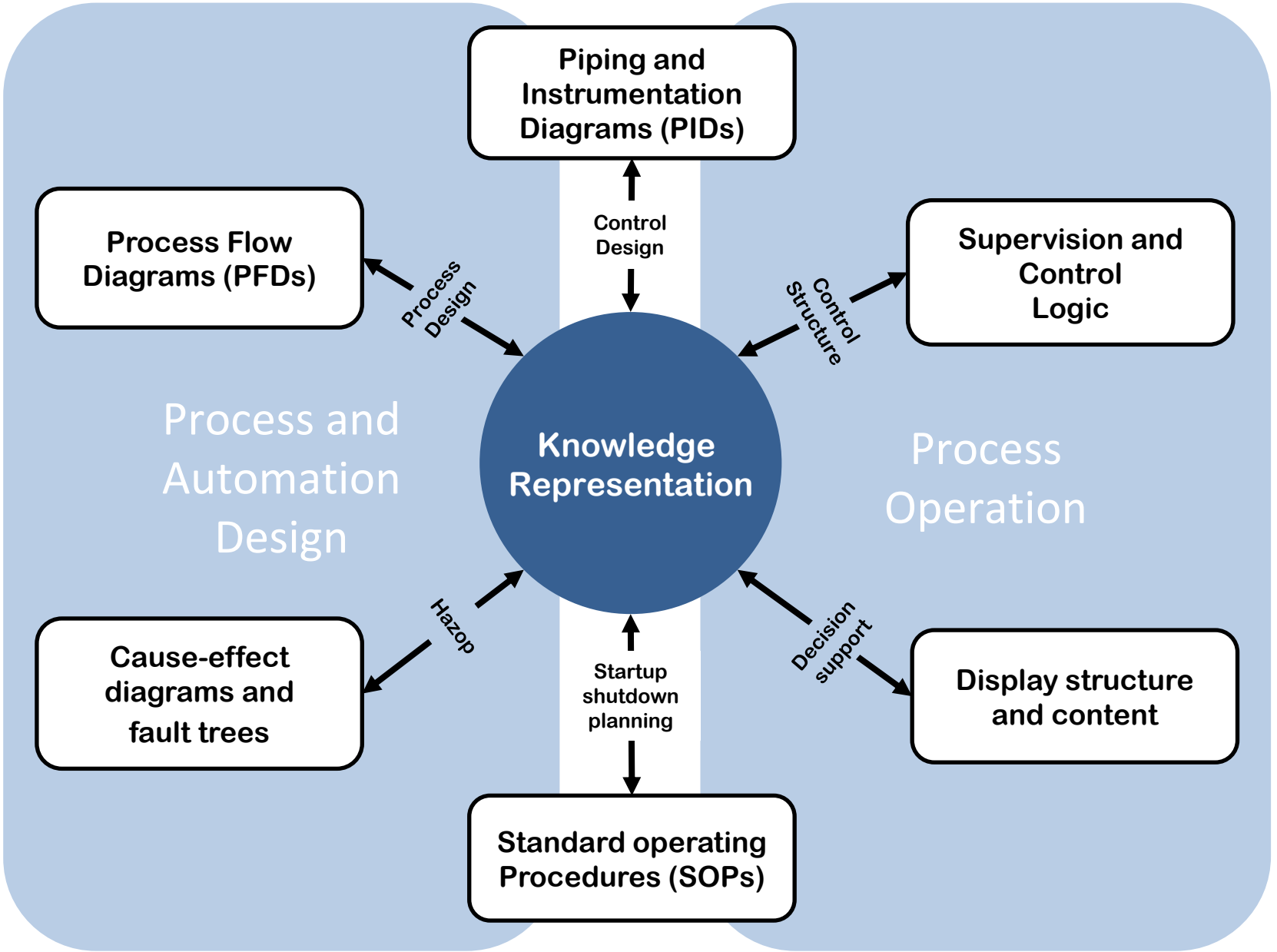
- The system development life cycle framework provides a sequence of activities for system designers and developers to follow. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.

- There are different SDLC models available for different industrial domains.

  – Preliminary analysis
  – Conceptual design
  – Requirement analysis
  – Detailed design
  – Commissioning and Testing
  – Operation and Maintenance
  – Decommissioning

- Process design, automation design, display design, procedure design etc.
- Process knowledge passing from the design phases to the operation phases is important for safety and realiability
- Cause-effect of plant deviation is evaluated in the design phase of the system development.

This knowledge is not explicitly presented in the control room



Hazard Identification & Risk Analysis

- Hazard Identification and Risk Analysis is often used collectively. It encompasses all activities involved in identifying hazards and evaluating risk at industrial plant, throughout their life cycle.

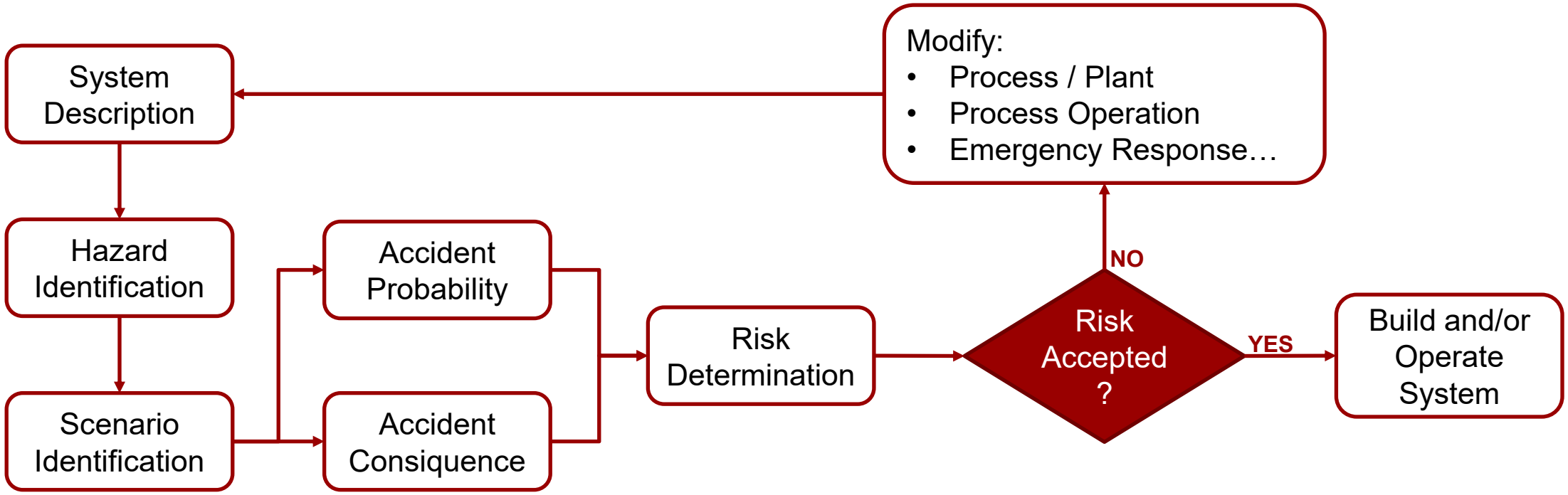


Diagram from the book ”Chemical Process Safety”

Hazard Identification & Risk Analysis

- Hazard – What can go wrong?
- Consequences – How bad could it be?
- Likelihood – How often might it happen?

- Tools:
  - qualitative risk analysis
    - Hazard survey or checklist
    - hazard and operability analysis (HAZOP)
    - failure modes and effects analysis (FMEA)
    - layer of protection analysis (LOPA)
  - Quantitative risk analysis (probability)
    - fault trees and event trees

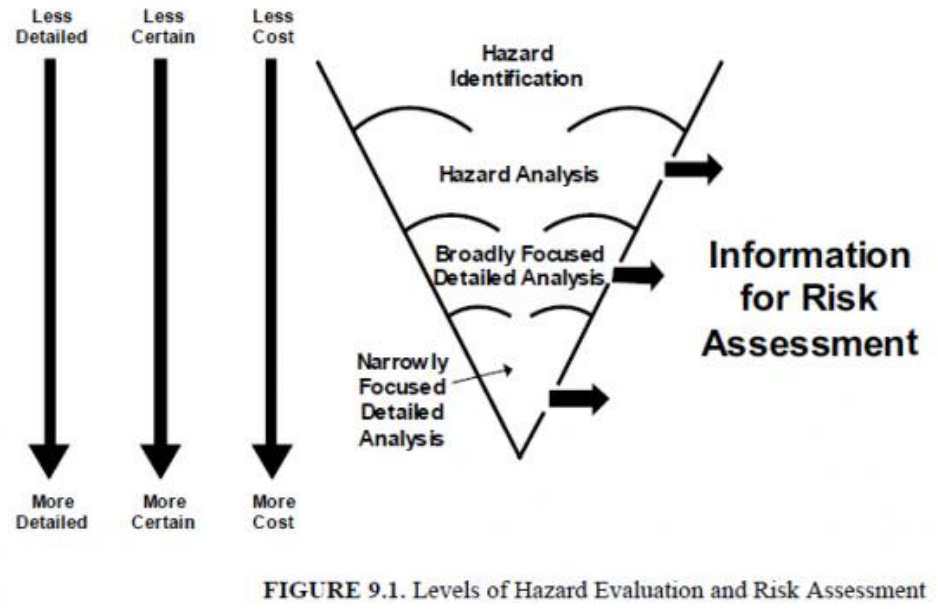


FIGURE 9.1. Levels of Hazard Evaluation and Risk Assessment

Figure from AICHE website

- Hazard and risk reviews may be performed at any stage in a project's life cycle

Hazard and Operability Study (HAZOP)

- HAZOP is a structured and systematic examination of a complex planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment.

- Normally performed
  - When applied to new plants at the point where the design is nearly firm and documented
  - Or to existing plants where a major redesign is planned

- Initially developed in the chemical process plant systems but has since been extended to other areas, including other complex systems such as nuclear power plant operation.

Hazard and Operability Study (HAZOP)

- Result of HAZOP study
  - HAZOP tables that contains:
    - identification of hazards and operating problems;
    - recommended changes in design, procedure, etc. to improve safety; and
    - recommendations for follow-on studies where no conclusion was possible due to lack of information.

  - It is a qualitative analysis

  - HAZOP meeting requires
    - detailed plant descriptions, such as drawings, procedures, and flow charts.
    - considerable knowledge of the process, instrumentation, and operation, (this information is usually provided by the meeting participants who are experts in these areas)

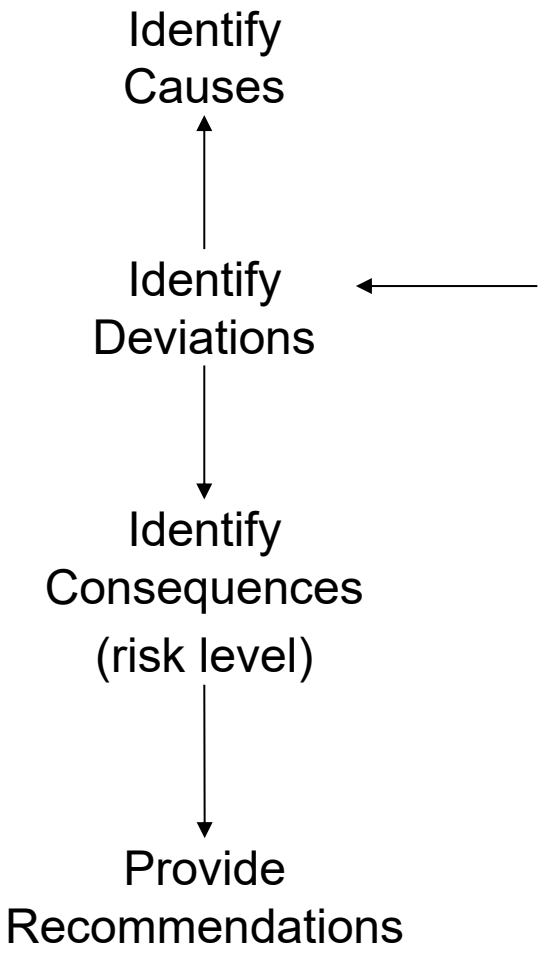
Hazard and Operability Study (HAZOP)

- HAZOP Meeting and team
  - Normally 5-7 people (depending on the size of the plant)
  - Time consuming process
    - Systems shall be divided into different nodes (sub-systems)
    - each node requires several hours for discussion and analysis
    - additional time must be allowed for coordination and documentation
  - Participants
    - Team-leader (expert in HAZOP)
    - Domain experts
      - For new plant: project engineer, process engineer, safety engineer, commissioning manager, IC design engineer
      - For existing plant: plant superintendent, process supervisor, maintenance engineer, technician

Hazard and Operability Study (HAZOP)

- Concepts
  - Systems shall operate under design conditions
  - Problems arise when deviations from design conditions occur
- Basis
  - Plant documents such as PFDs and P&IDs
- Procedure
  - Use “**Guide Words**” to question every node of process to discover what deviations from the intention of design can occur and what are their causes and consequences may be.

Hazard and Operability Study (HAZOP)

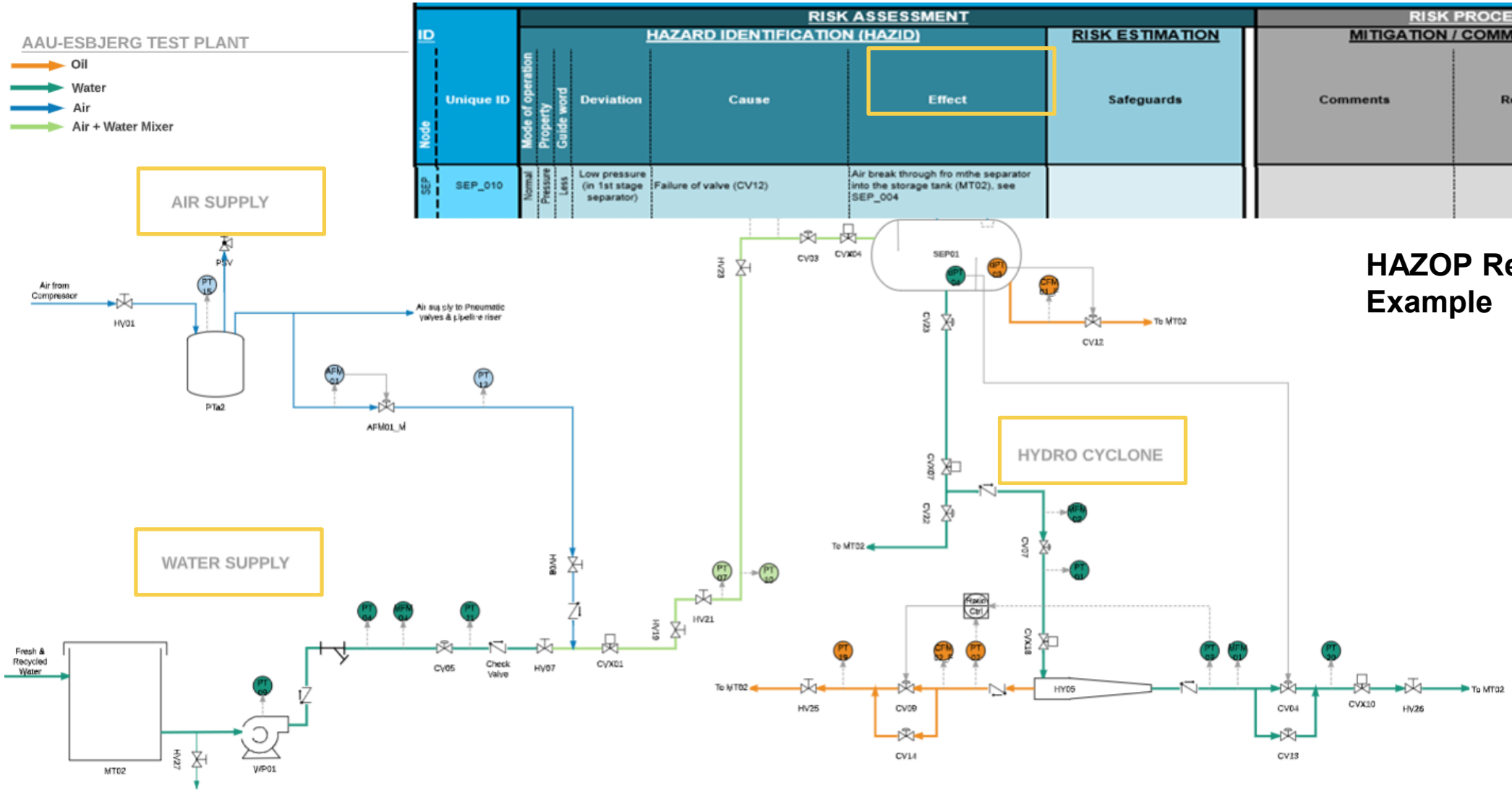


Guide Word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN / INSTEAD	Complete substitution
EARLY	Relative to the clock time
LATE	Relative to the clock time
BEFORE	Relating to order or sequence
AFTER	Relating to order or sequence

Covering every parameter relevant to the system under review: i.e. flow rate. flow quantity, pressure, temperature, etc.

Hazard and Operability Study (HAZOP)

ID				RISK ASSESSMENT				RISK PROCESSING	
				HAZARD IDENTIFICATION (HAZID)			RISK ESTIMATION	MITIGATION / COMMENTS	
Node	Unique ID	Mode of operation	Property	Guide word	Deviation	Cause	Effect	Safeguards	Comments	Required action
SEP	SEP_010	Normal	Pressure	Less	Low pressure (in 1st stage separator)	Failure of valve (CV12)	Air break through fro mthe separator into the storage tank (MT02), see SEP_004			

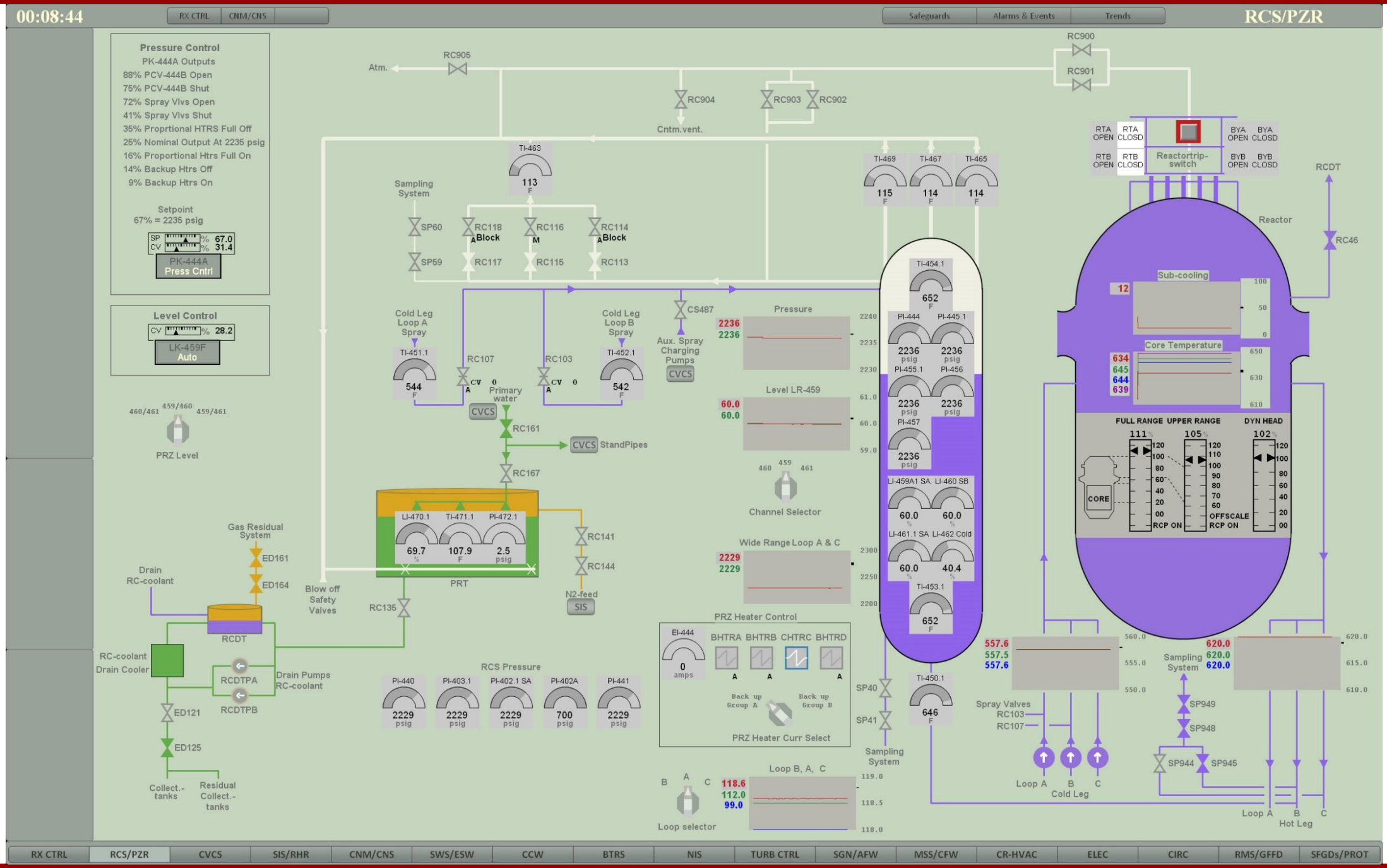


HAZOP Report Example

Group Discussion

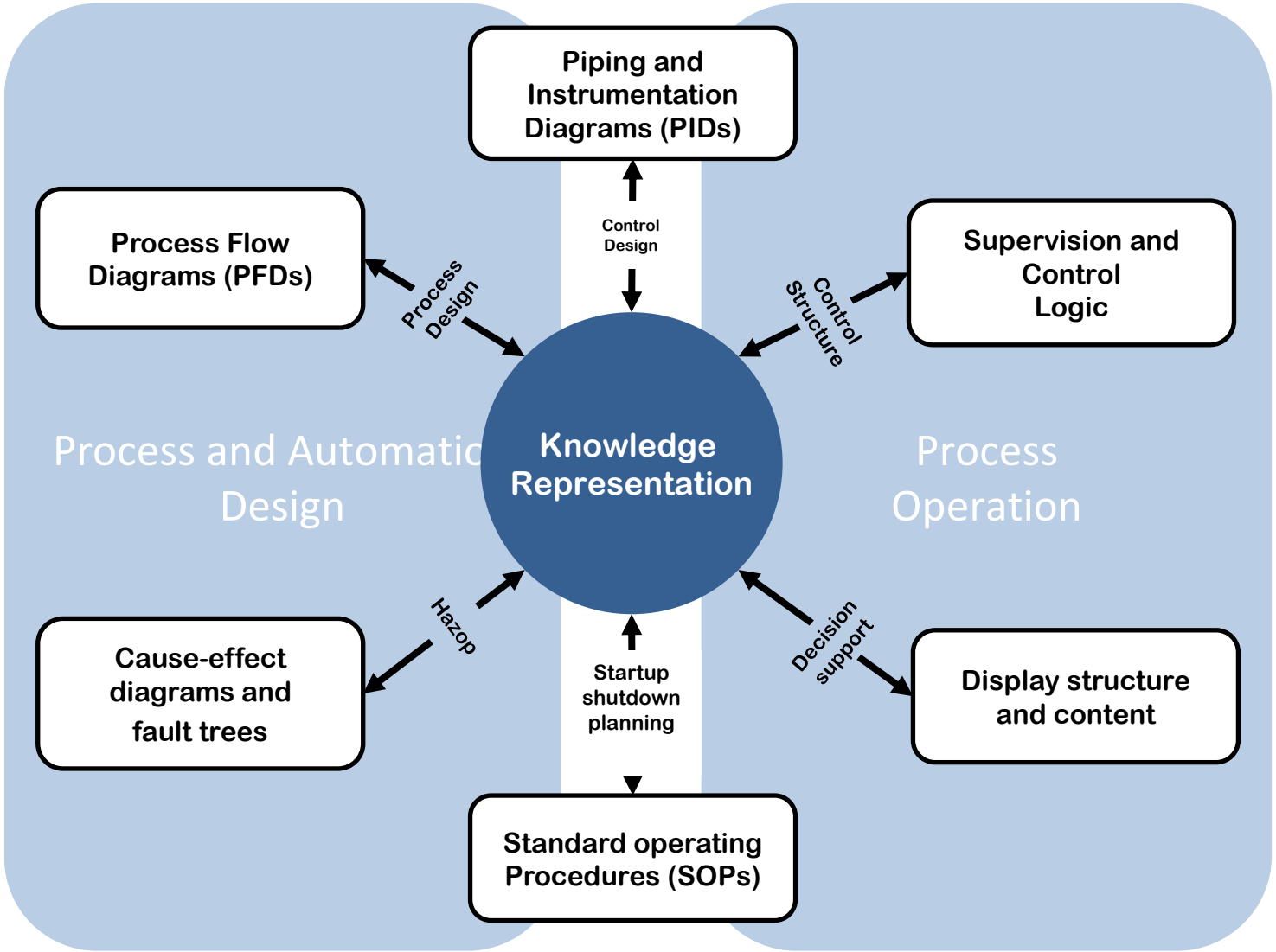
- Perform HAZOP analysis for the PWR pressurizer
  - List 2-3 potential deviations for the pressurizer
  - Try to formulate in a HAZOP table

Node	ID	Property	Guide Word	Deviation	Cause	Effect	Safeguards
RCS-PRZ	1						
RCS-PRZ	2						


00:08:44
RX CTRL
CNM/CNS
Safeguards
Alarms & Events
Trends
RCS/PZR
Pressure Control
PK-444A Outputs
88% PCV-444B Open
75% PCV-444B Shut
72% Spray Vlvs Open
41% Spray Vlvs Shut
35% Proprtional HTRS Full Off
25% Nominal Output At 2235 psig
16% Proportional Htrs Full On
14% Backup Htrs Off
9% Backup Htrs On
Setpoint
67% = 2235 psig
PK-444A
Press Cntrl
Level Control
LK-459F
Auto
PRZ Level
RC905
Atm.
RC904
Cntm.vent.
RC903
RC902
RC900
RC901
Sampling System
SP60
SP59
RC118
RC117
RC116
RC115
RC114
RC113
TI-463
113
TI-469
115
TI-467
114
TI-465
114
RTA OPEN
RTA CLOSD
RTB OPEN
RTB CLOSD
Reactortrip-switch
BYA OPEN
BYA CLOSD
BYB OPEN
BYB CLOSD
RCDT
RC46
Reactor
Sub-cooling
Core Temperature
FULL RANGE
UPPER RANGE
DYN HEAD
CORE
OFFSCALE
RCP ON
Cold Leg Loop A Spray
TI-451.1
544
RC107
RC103
Cold Leg Loop B Spray
TI-452.1
542
CS487
Aux. Spray Charging Pumps
CVCS
Primary water
RC161
CVCS StandPipes
RC167
LI-470.1
LI-471.1
PI-472.1
69.7
107.9
2.5
PRT
RC141
RC144
N2-feed
SIS
RC135
Blow off Safety Valves
Gas Residual System
ED161
ED164
Drain RC-coolant
RCDT
RC-coolant Drain Cooler
RCDTPA
RCDTPB
Drain Pumps RC-coolant
ED121
ED125
Collect.-tanks
Residual Collect.-tanks
RCS Pressure
PI-440
PI-403.1
PI-402.1 SA
PI-402A
PI-441
2229
700
Pressure
Level LR-459
Channel Selector
Wide Range Loop A & C
PRZ Heater Control
EI-444
BHTRA
BHTRB
CHTRC
BHTRD
Back up Group A
Back up Group B
PRZ Heater Curr Select
Loop B, A, C
Loop selector
TI-454.1
652
PI-444
PI-445.1
PI-455.1
PI-456
PI-457
2236
LI-459A1 SA
LI-460 SB
LI-461.1 SA
LI-462 Cold
60.0
40.4
TI-453.1
TI-450.1
646
SP40
SP41
Sampling System
Spray Valves
RC103
RC107
Loop A
Loop B
Loop C
Cold Leg
SP949
SP948
SP944
SP945
Hot Leg
RX CTRL
RCS/PZR
CVCS
SIS/RHR
CNM/CNS
SWS/ESW
CCW
BTRS
NIS
TURB CTRL
SGN/AFW
MSS/CFW
CR-HVAC
ELEC
CIRC
RMS/GFFD
SFGDs/PROT

Hazard and Operability Study (HAZOP)

- Summary and reflection
  - Is the HAZOP documentation useful to operation?
  - How to use the HAZOP knowledge in the control room?



Plant-wide fault diagnosis

- Diagnosis
  – determining or analysis of the cause or nature of a problem or a (abnormal) situation.

- In the context of complex industrial plant operation
  – To find the root causes for abnormal plant states
  – Cognitive tasks for control room operators
    - Observe and recognize the abnormal state
    - Understand the causal dependencies in the system
    - Perform **causal reasoning** to identify the causes based on observation

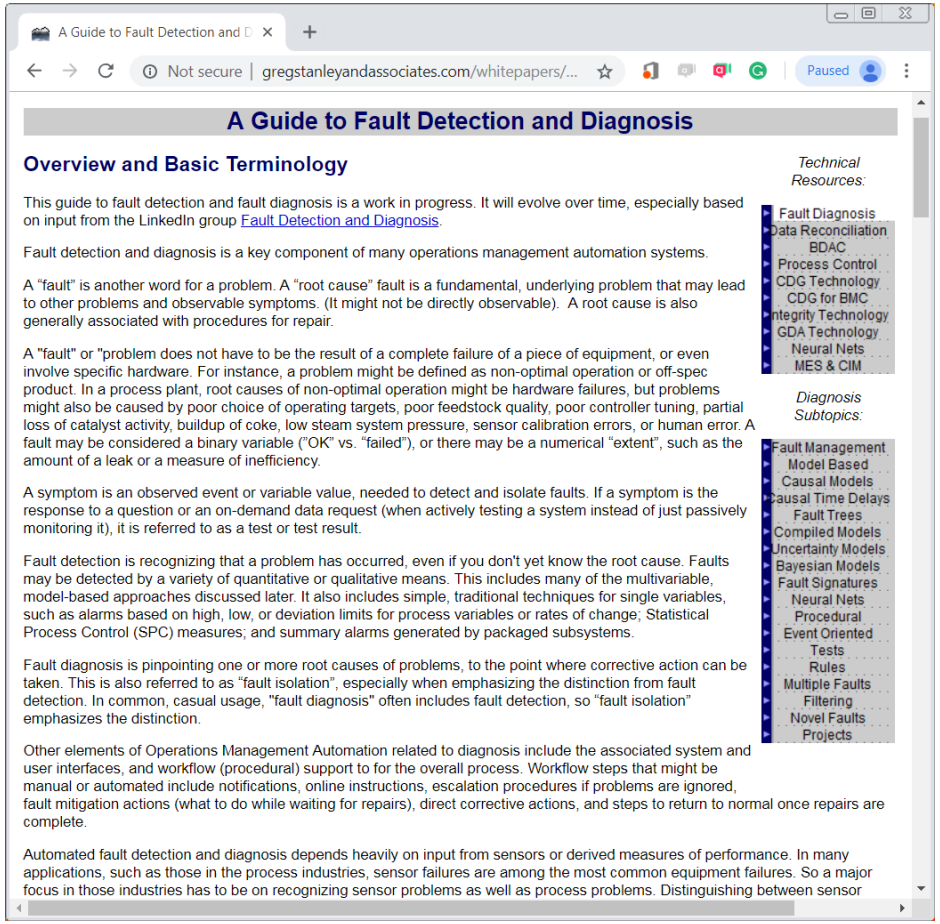
- It has been done during the design of the system, how can we reuse the existing knowledge to to support this process during operation?
- Can we reconstruct the problem solving process to mimic the operator so any of the solutions provided can be easily explained?

Fault detection and diagnosis

- Extended reading:
  - http://gregstanleyandassociates.com/whitepapers/FaultDiagnosis/faultdiagnosis.htm

- Model-based approach vs. data driven approach
- Causal models
- Fault trees

- Rule-based system – implementing other fault diagnosis approaches.



Fault tree analysis (FTA)

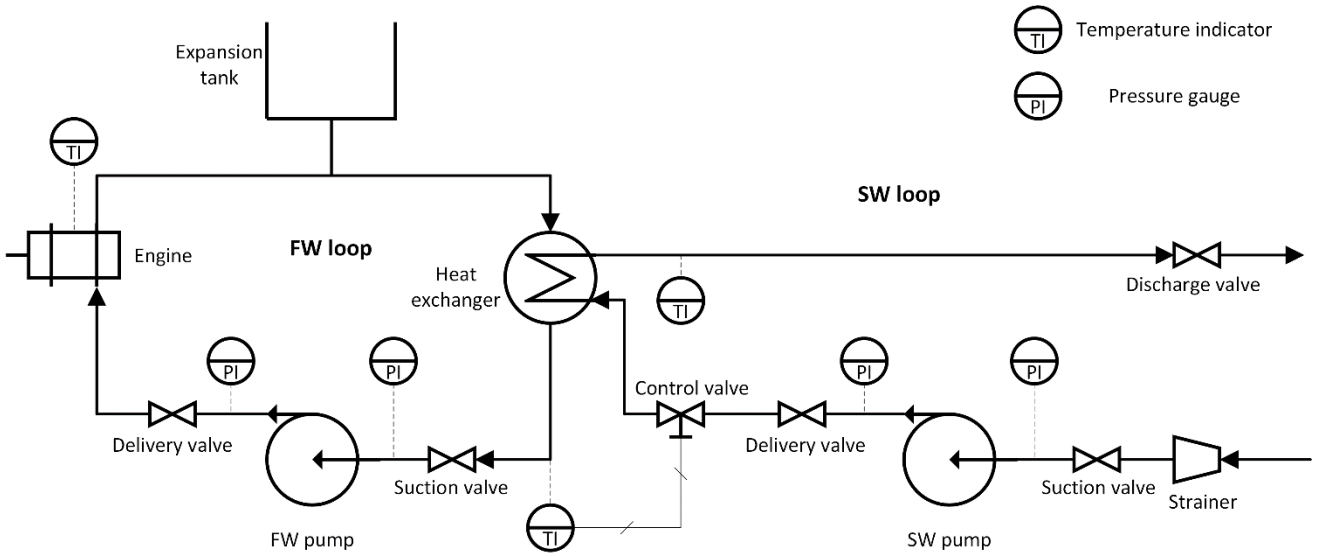
- FTA is a deductive reasoning technique that focuses on one particular failure event.
- The fault tree itself is a graphic model that displays the various combinations of equipment faults and failures that can result in the top event.
- The solution (calculated by using Boolean algebra) of the fault tree is a list of the sets of equipment failures and human/operator errors that are sufficient to result in the accident event of interest (minimal cut-set).
- Requirements for constructing a fault tree:
  - A “complete” understanding of how the plant functions.
  - Knowledge of the plant equipment failure modes and their effects on the plant.

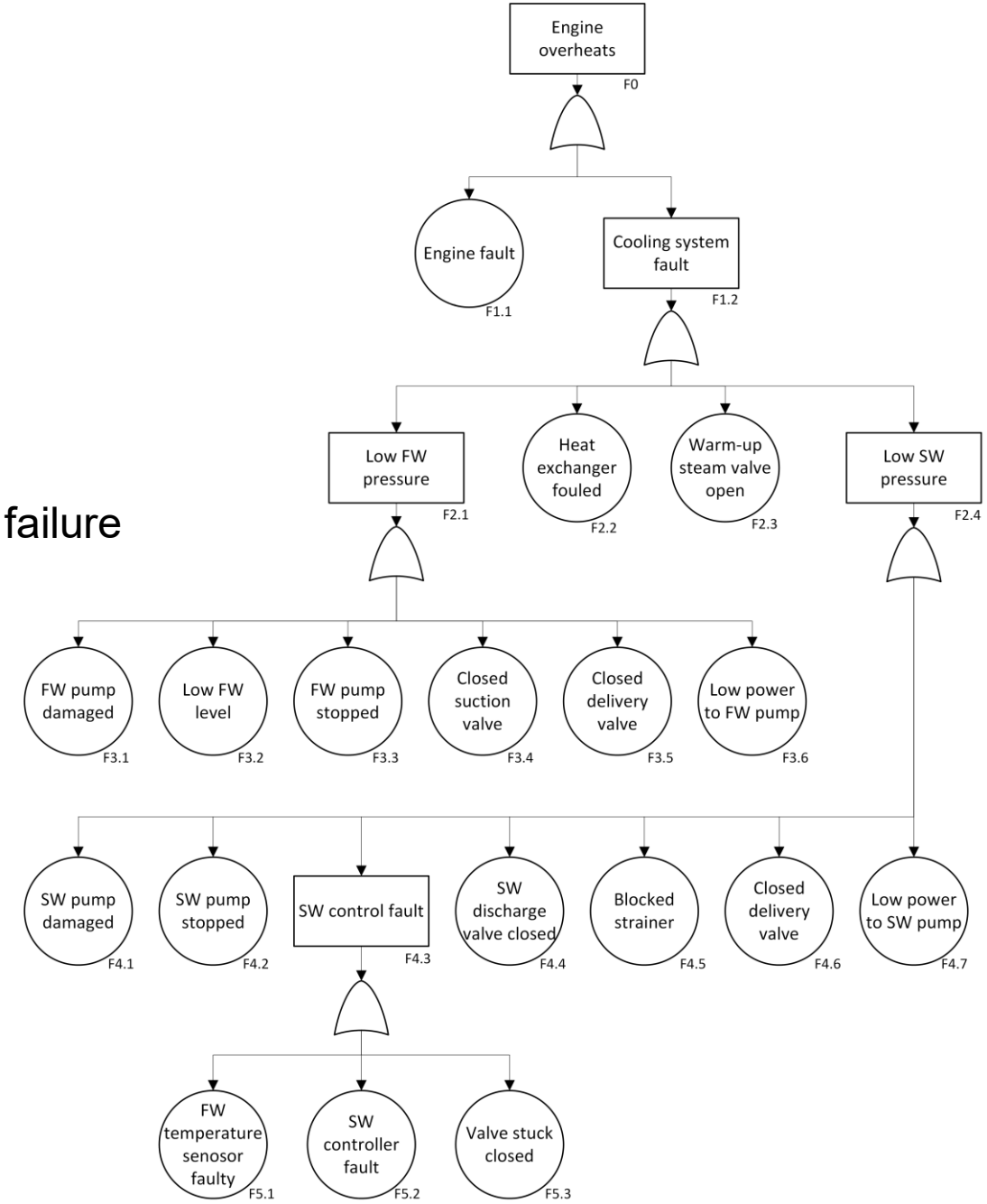
Intermediate Event	A fault event that occurs because of one or more antecedent causes acting through logic gates have occured.
And	The AND-gate is used to show that the output event occurs only if all the input events occur.
Or	The OR-gate is used to show that the output event occurs only if one or more of the input events occur.
Base Event	A base event or also called a basic event that requires no further development because the appropriate limit of resolution has been reached.
Transfer	A transfer symbol indicates that the tree is developed further at th occurrence of the corresponding transfer symbol (in another diagram).
Undeveloped Event	Undeveloped Event is used to define an event which is not further developed either because it is of insufficient consequence or because information is unavailable.

Fault tree analysis (FTA)

- Example: ship engine cooling system
- Top event: Engine Overheats

- engine overheats: engine failure, cooling failure
- cooling failure: FW loop failure, HEX failure, SW loop failure
- …





Fault tree analysis (FTA)

$P + M_A \cdot M_B$

- Pumping in a process plant
  - Two pumps one in use, one in stand by (redundant), in case of one pump fails, the other pump takes over.
  - The two pumps use a common power source
  - The pumps can fail because of either mechanical failure or lose of power.

- Build a Fault tree
  - Top event: PUMPING FAIL

- Fault tree as one type of causal models can be used to implement a rule-based diagnosis system.

Next Time

- How to build a rule-based system based on FTA
- Exercise 1