Basic Level 1. PSA course for analysts

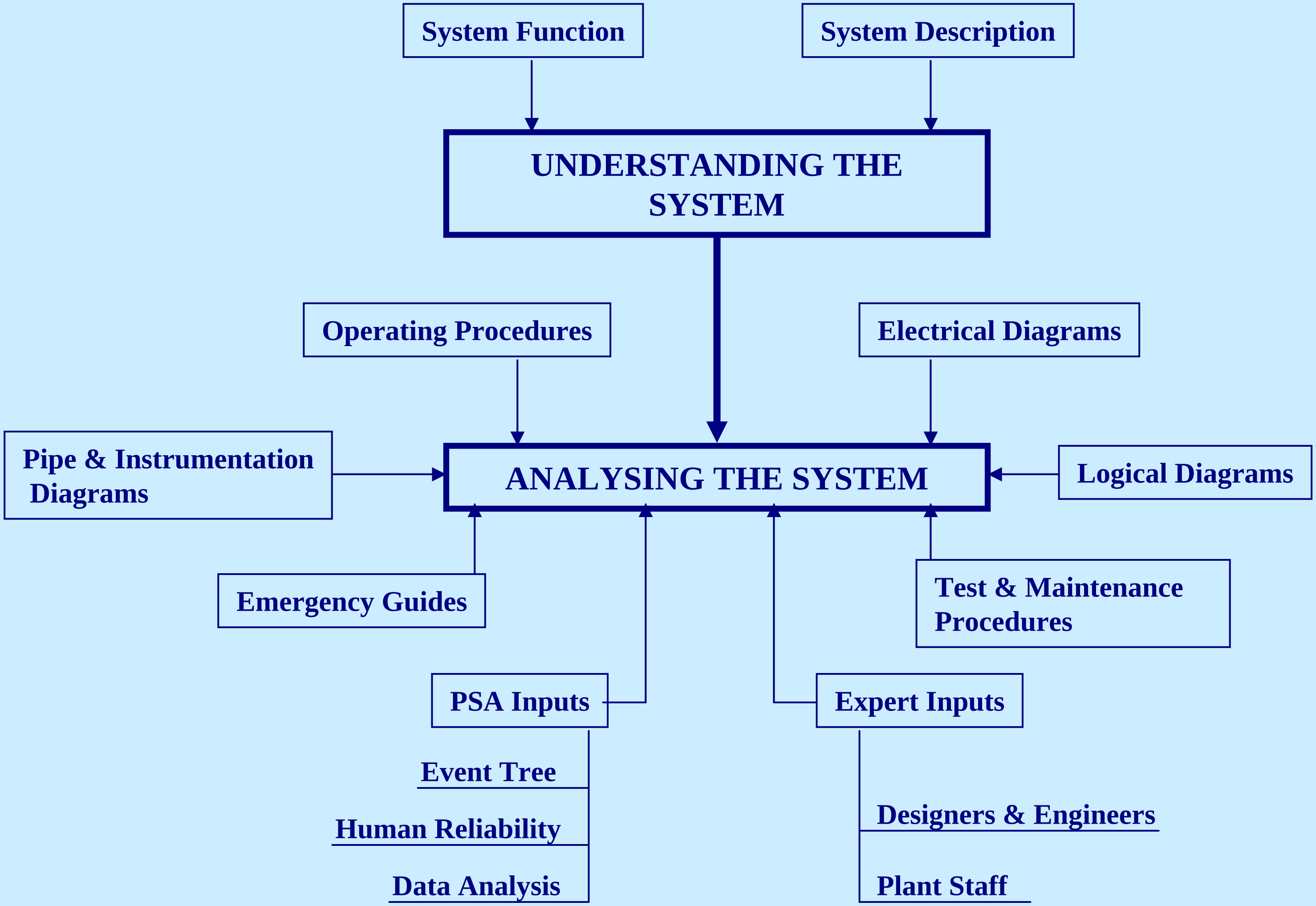
System Analysis in a PSA

part 2

CONTENT

- Information Requirements
- System Boundary and Component Boundary
- System Simplification (internal boundaries)
- Support Systems
- Maintenance and Tests
- Human Errors
- Common Cause Failures
- Success Criteria: Top Events
- Modelling:
- Component failure modes
- A structured approach to modelling
- House events
- Circular logic loops
- Quantification

INFORMATION REQUIREMENTS



SYSTEM BOUNDARY

- The starting point when analysing a system is to define its limits.
- The system boundary for a PSA model can be different from the physical design boundary of the system.
- None of the components outside the boundary will be analysed in detail, although they cannot be ignored:
- Maintenance or tests on those components might affect the analysed system;
- The support systems are outside the boundary.
- The interfaces between the different systems have to be well defined so that the analysis will be complete when all the systems are put together.

COMPONENT BOUNDARY (limit of resolution)

- A boundary for each component has to be defined according to the criteria from the data analysis.
- This boundary depends on the available data.
- No component inside the boundary will be modelled

SYSTEM SIMPLIFICATION

- Simplifying the system means removing:
  - all the items that are not critical to the system function.
  - all the items that are inside the component boundaries.
- Then the simplified diagram of the system can be drawn

SYSTEM SIMPLIFICATION (cont'd)

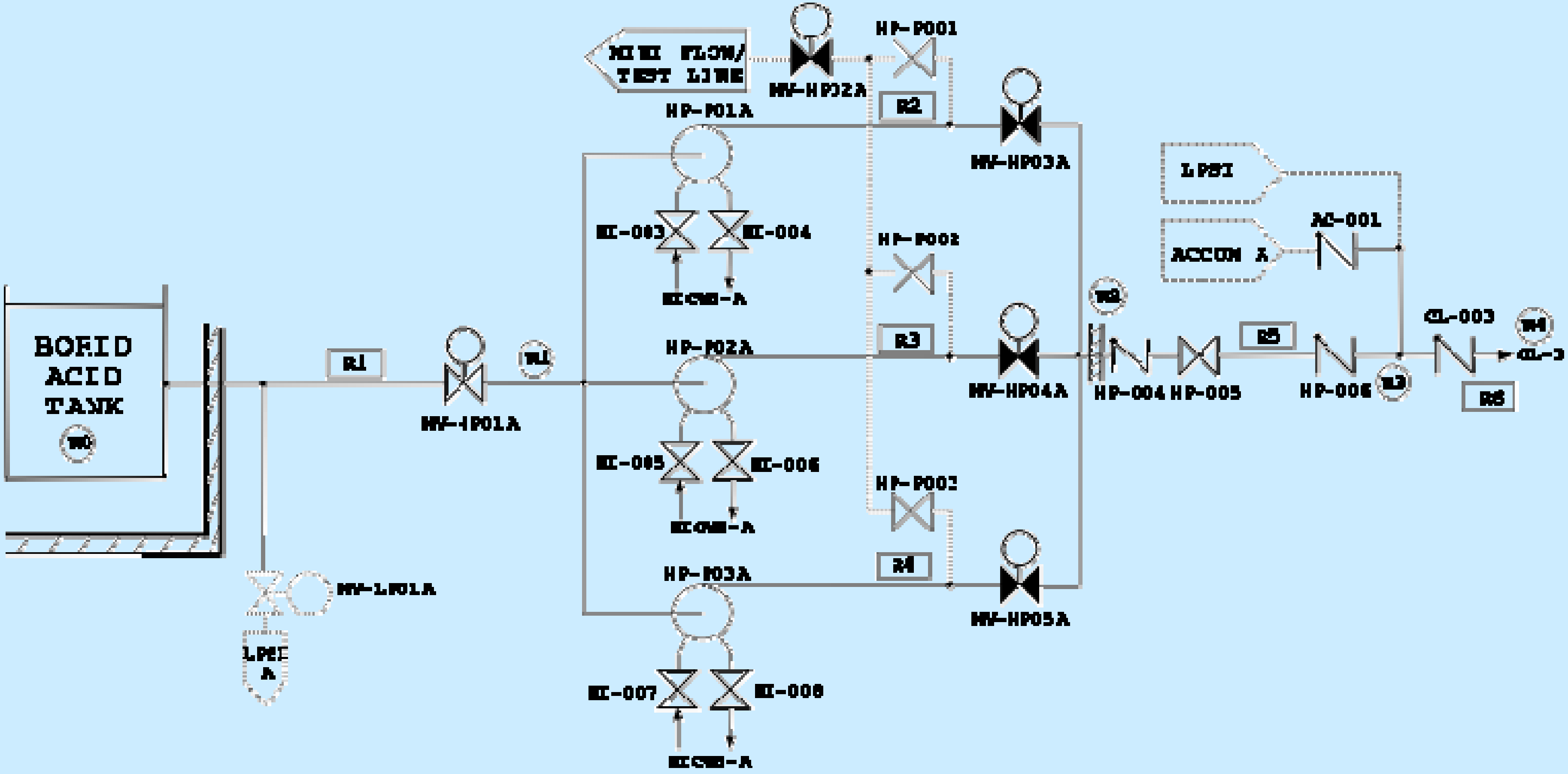
Simplified Mechanical Diagram	Simplified Electrical Diagram
Remove:	Remove:
Small Pipes (< 10% nominal flow)	Items inside component boundaries
Instruments that do not affect the system performance	Components not required for the system performance
Non-required pipes after two closed valves	
All the components that are not going to be modelled	All the components that are not going to be modelled

INTERNAL BOUNDARIES

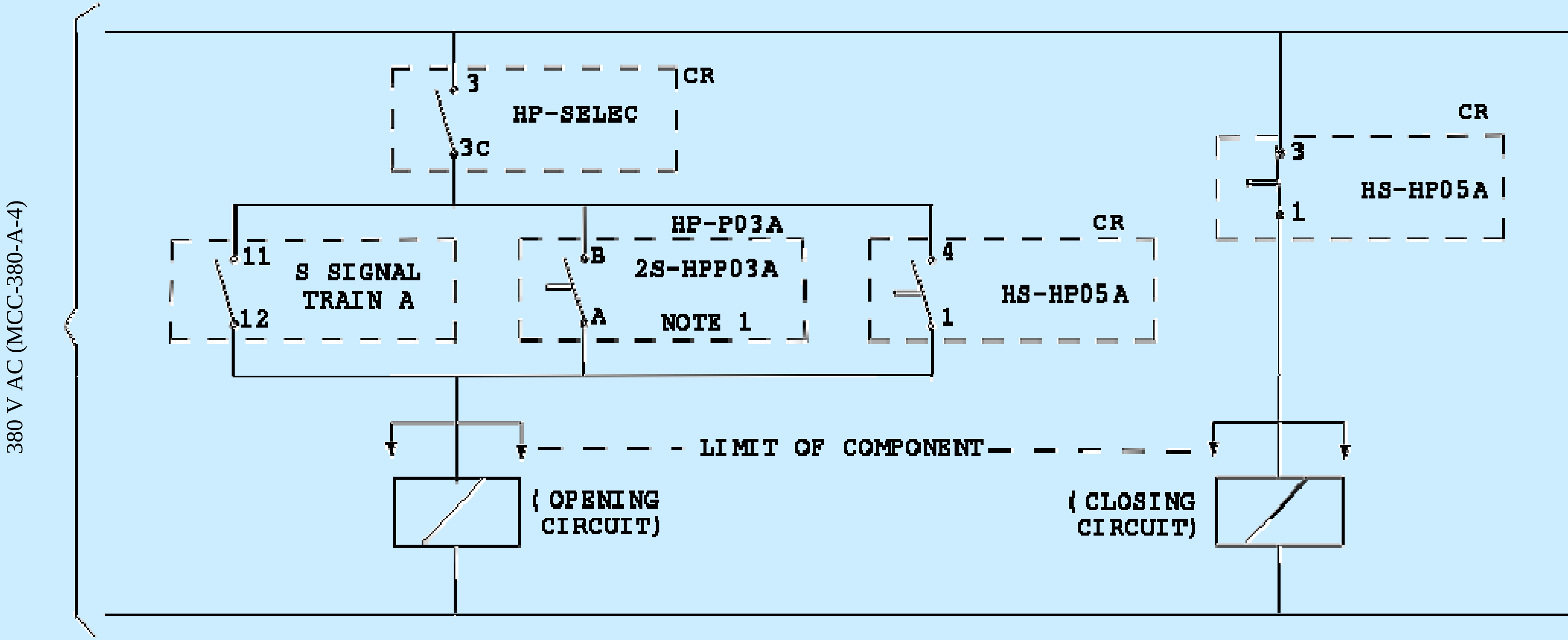
- It is useful for the further modelling, to divide the system into a number of subsystems and sub-subsystems.
- This is the choice of internal boundaries for the system.
- To represent this, the analyst can use 'nodes' and 'runs' (the lengths between two nodes).

INTERNAL BOUNDARIES (cont'd)

HPSI TRAIN-A SIMPLIFIED DIAGRAM



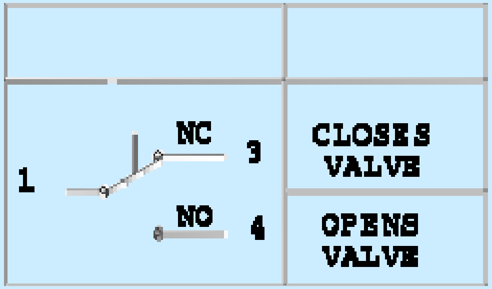
SIMLIFIED ELECTRICAL DIAGRAMS



SIMLIFIED ELECTRICAL DIAGRAMS (cont'd)

VALVE MV-HPO5A SIMPLIFIED CONTROL DIAGRAM

HS-HP05A



1

NC

3

NO

4

CLOSES VALVE

OPENS VALVE

Note 1: Contact closes when Pump HP-P03A starts

HP-SELEC

CONT POS	1 1C	2 2C	3 3C
LOOP A	*		
LOOP B		*	
LOOP C			*

SUPPORT SYSTEMS, DEPENDENCIES

- Most components require the correct function of other systems in order to actuate - these are called support systems.
- For the correct analysis of the system, all the dependencies must be considered.
- The support system modelling depends on the component actuation that is required:

  A valve that fails closed with loss of electric power does not need electric power in order to close, but will need it in order to open.

  A pump does not need room cooling in order to start and run for a short time, but will probably need it in order to run for a longer time.

SUPPORT SYSTEMS, DEPENDENCIES (cont'd)

- The main support systems to be considered are:

  ELECTRICAL SYSTEMS

  INSTRUMENTATION AND CONTROL

  HVAC

  COOLING

  COMPRESSED AIR

- The available information about the system provides most of these inputs, but plant staff and engineering backup might be required.

DEPENDENCY TABLE

- A useful way to store and present all the information about support systems is to draw a dependency table.

SUPPORT SYSTEMS

COMPONENT	DC Power Supply	AC Power Supply	Component Cooling	HVAC	Instrumentation and Control
Pump 1	6.3 KV-train A-MCC-1	Not required	EICWS-A	Fan cooler X	Not required
Pump 2	6.3 KV-train B-MCC-1	220V DC train B (1)	EICWS-B	Fan cooler Y	I and C train B
Valve 3	Not required	Not required	Not required	Not required	Not required
Valve 4	380V-train B-MCC-1	Not required	Not required	Not required	I and C train B

(It has been assumed that pump 1 is normally running and that pump 2 is required to start and run. Also, valve 3 is required to stay open and valve 4 is required to open.)

DEPENDENCY TABLE (cont’d)

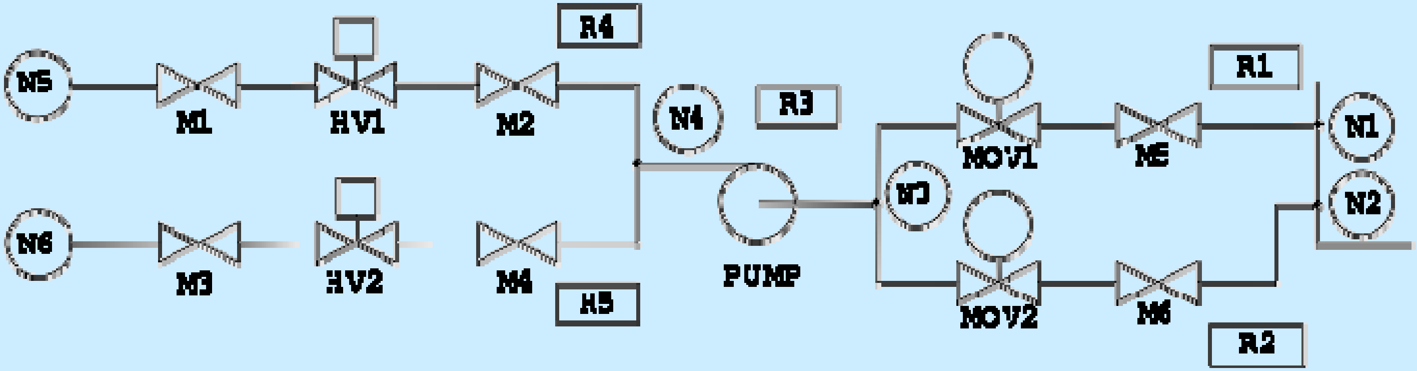
- The dependency table can hold as much information as considered necessary.

  For example:

  - names of link-points between the analysed system and the support systems (relays, fuses, etc)
  - fault tree gate names

SYSTEM MAINTENANCE

- One of the reasons why a component is not available when required is because it is on maintenance, or because it is out of service due to the maintenance work on an adjacent component.
- It is important to define all the maintenance events that can affect the analysed system and in which way the system is affected.
- A practical way to define these events is developing a maintenance table



System analysis in a PSA (part 2)

MAINTENANCE TABLE

AFFECTED COMPONENT

Abbreviations: C – closed, D – de-energised

COMP ON MTE	M1	M2	M3	M4	M5	M6	MOV1	MOV2	PUMP	HV1	HV2	EFFECT ON SYSTEM
HV1 mech. mte.	C	C								D		No flow trough R4
HV1 elec. mte										D		No effect
PUMP mech. mte		C		C			C/D	C/D	D			No flow trough R1, R2, R3, R4, R5 = No flow trough R3
PUMP elec. mte									D			No flow trough R3
MOV1 mech. mte		C		C				C/D	D			No flow trough R1, R2, R3, R4, R5 = No flow trough R3
MOV1 elec. mte							D					No effect

Very important! Plant staff back-up is very important when developing this table.

Supplementary Notes on the Maintenance Table

1. The analysis of the maintenance table shows in what way the analysed system is affected by the maintenance events.

2. All the maintenance events that affect the same RUN of the analysed system can be grouped in a single EVENT that represents UNAVAILABILITY DUE TO MAINTENANCE.

3. How this EVENT has been formed is an important input for the DATA ANALYSIS. That information will be required in order to assess the probabilities of the EVENTS that represent UNAVAILABILITY DUE TO MAINTENANCE.

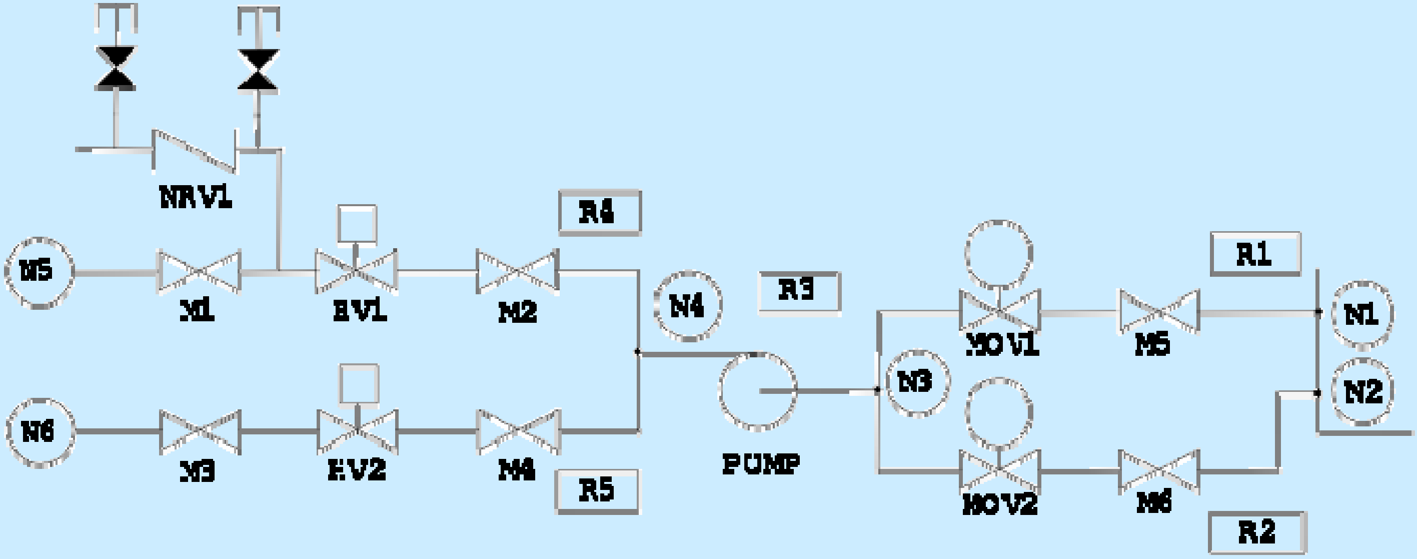
4. These events will be included in the system model.

SYSTEM TESTS

- The study of the tests that are carried out on the analysed system gives the following information:
  - how often the components are tested
  - failure modes that are and are not tested
  - system misalignments due to tests
  - system unavailability due to tests

SYSTEM TESTS (cont’d)

- This information is required for DATA and HUMAN RELIABILITY ANALYSES.



TEST TABLE

A table to analyse the different tests that affect the system can be constructed. (Surveillance and calibration works will also be considered in this analysis).

TEST NAME AND DESCR.	TESTED COMPONENTS		REALIGNED COMPONENTS		Unavailabi-lity	Freq.	Notes
	Component	Tested mode	Component	Position			
TEST T (NRV1)	NRV1 HV1 M1	OPEN CLOSE OPEN CLOSE	HV1 M1	CLOSE CLOSE	RUN R4 UNAVAILABLE	1/year	

Very important! Plant staff back-up is very important for developing this table.

Supplementary Notes for Test Table

1. The analysis of the TEST TABLE shows in what way the analysed system is affected by the test events.

2. The events that represent UNAVAILABILITY DUE TO TESTS are deduced from this table.

3. These events will be included in the system model.

HUMAN ACTIONS

- Some HUMAN ACTIONS before and during the accident can affect the system availability and performance:

1) HUMAN ERRORS BEFORE THE ACCIDENT:
   - MISALIGNMENTS: System components can be left incorrectly aligned after test or maintenance works.
   - MISCALIBRATIONS: These errors affect to Instrumentation & Control components.

2) HUMAN ACTIONS DURING THE ACCIDENT:
   - BACK-UP ACTIONS: Actions to actuate equipment that has failed to do so automatically.
   - DIRECT ACTIONS: Human actions that are necessary for a system or component to actuate.

Supplementary Notes on Human Actions

1. Some HUMAN ACTIONS before and during the accident can have a direct effect on the system.

2. The incorrect performance of those actions leads to the HUMAN ERRORS that have to be considered in the system analysis.

a) HUMAN ERRORS BEFORE THE ACCIDENT

These errors cause the system or component to be unavailable when required.

Supplementary Notes on Human Actions (cont'd)

- MISALIGNMENTS: System components might be left incorrectly aligned after tests, operational alignments or maintenance works.

  Some examples of these errors are:

  Wrong position of valves that do not align automatically, de-energised motors, wrong position of switches that do not return automatically, disconnected cables, etc.

  Every component that is tested, maintained or manipulated, is subject to unavailability due to human error unless it can be proved that the "wrong alignment" is clearly and unambiguously detected by alarms, tests after maintenance, etc., and therefore it can be immediately corrected.

Supplementary Notes on Human Actions (cont’d)

- MISCALIBRATIONS: All the Instrumentation & Control components that are periodically calibrated are subject to wrong calibration.

  These HUMAN ERRORS will be modelled according to the criteria of Human Reliability Analysis.

  The Test & Maintenance Tables will help to find the HUMAN ERRORS that have to be modelled.

Supplementary Notes on Human Actions (cont'd)

b) HUMAN ACTIONS DURING THE ACCIDENT:

- BACK-UP ACTIONS: Actions that are performed by the operator to actuate systems or components that have failed to do so automatically.

Supplementary Notes on Human Actions (cont’d)

- DIRECT ACTIONS: Human actions that are necessary for a system or component to actuate when required.

  These actions are considered according to the criteria of the Human Reliability and Accident Sequence Analyses.

  For "support systems", these human actions depend on the "front line systems" requirements.

  Also, the Emergency Guides provide the way to find out which human actions are important during the accident.

  The human reliability analyst provides the rules to model the human errors, the general naming convention, and the initial values that have to be used for the first quantification of the system.

COMMON CAUSE FAILURES

- The analysis of common cause failures leads to the inclusion of basic events in the fault tree that represent these failures. This is done so that the basic events included in the fault tree may be treated as independent events.

- Common cause failures mean that the probability of failure of several redundant components can be much higher than may be expected from multiplying their independent failure probabilities. Common cause failures must be considered in addition to independent failures.

COMMON CAUSE FAILURES (cont'd)

- Various factors may lead to the failure of two or more redundant components: e.g., environmental factors design factors, component maintenance.
- The failure modes caused by these factors and the components affected will be determined by the data analysis. The data analyst provides the rules to model these events and the naming convention for them.
- Also, there are common cause failures due to human errors before the accident. These are modelled in accordance with the human reliability analysis. The human reliability analyst provides the rules to model these events and the naming convention for them.

SUCCESS CRITERIA AND TOP EVENTS

- Every system modelled in a PSA is required to perform a function successfully. This function might be different in different situations.
- The performance required from the front line systems comes from the event trees/functional fault trees. This required performance is the front line system success criteria.
- The performance required from the support systems comes from the front line systems.
- The event that represents the failure of a system (or sub-system) to comply with its success criteria is the TOP EVENT of its fault tree.

Supplementary Notes on Top Events and Success Criteria

1. The front line system top events are defined in the event tree/- functional trees (see description of event tree and functional fault tree analysis).

2. The support system top events are defined in the front line system trees.

MODELLING

COMPONENT FAILURE MODES

- The different component failure modes have to be defined before starting modelling.
- This task is normally performed by the data analyst who provides every system analyst with a list of all the component failure modes that are to be considered and the naming convention.

MODELLING (cont’d)

NAMING CONVENTION

< a >   < b >   < c >   < d >

a - 2 characters for system code

b - 2 characters for component code

c - 8 characters for event description

d - 1 character for failure mode code

EXAMPLE TABLE OF COMPONENT FAILURE MODES

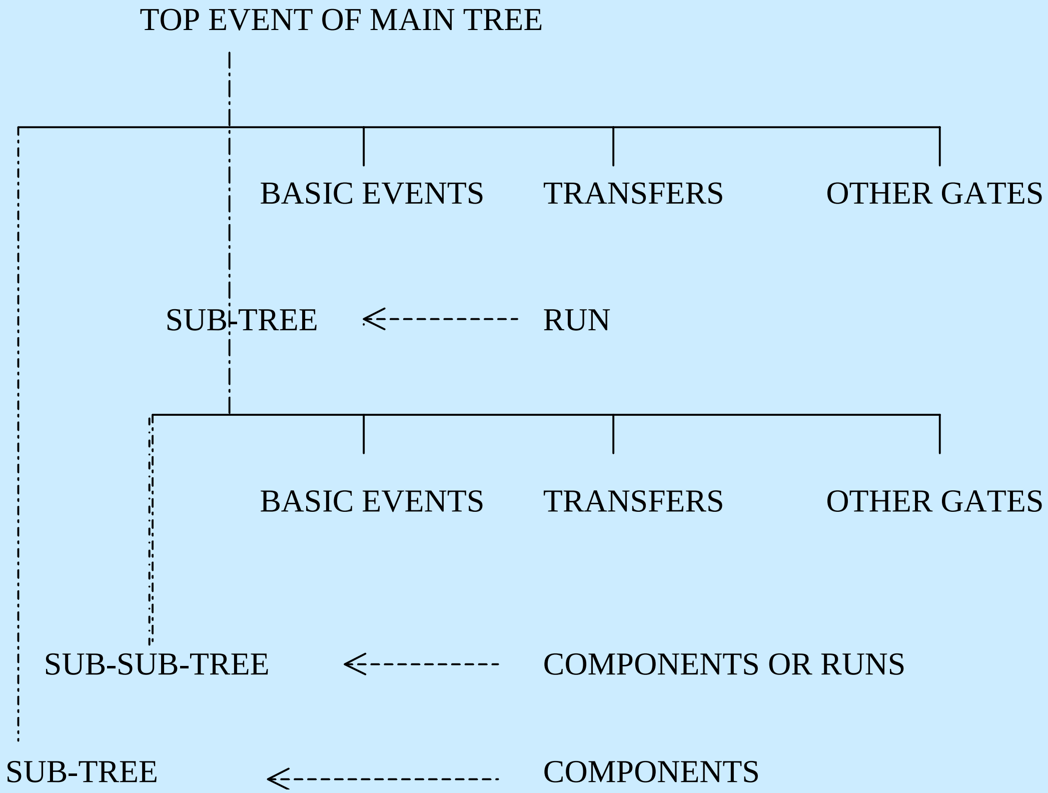
COMPONENT	FAILURE MODE	b	d
Motorised pump	Failure to start	MP	S
	Failure to run	MP	R
Pneumatic Valve	Failure to open	PV	O
	Failure to close	PV	C
	Failure to stay open	PV	X
	Failure to stay closed	PV	Y
Motorised Valve	Failure to open	MV	O
	Failure to close	MV	C
	Failure to stay open	MV	X
	Failure to stay closed	MV	Y
Control Valve	Loss of function	CV	F

System analysis in a PSA (part 2)

EXAMPLE TABLE OF COMPONENT FAILURE MODES (cont'd)

Non-return Valve	Failure to open	NV	O
	Failure to close (against flow)	NV	P
	Failure to stay closed	NV	Y
Filter	Blocked	FI	F
Manual switch	Loss of function	SW	F
Battery	Loss of function	BA	F
Bus Bar	Loss of function	BB	F
Fuse	Spurious opening	FU	T
Relay	Failure to energise	RE	E
	Failure to de-energise	RE	D
	De-energise spuriously	RE	T
Pressure Instruments	Loss of function	PT	F

A STRUCTURED APPROACH TO MODELLING



A STRUCTURED APPROACH TO MODELLING (cont'd)

- A simple structure that models the failure of the success criterion under the top event can be drawn.
- This first model calls the different sub-trees. These sub-trees represent failures of the runs (modules) that have been defined in the simplified diagrams.
- The components can be modelled as independent sub-trees. There can be as many levels as are considered necessary.

A STRUCTURED APPROACH TO MODELLING (cont'd)

- The advantage of this structure is that the sub-trees are modelled only once, but are used as many times as required by the higher level trees.
- Every gate that represents the failure of another system is modelled as a transfer gate.
- Every gate that represents the failure of part of the system that has been modelled as an independent sub-tree is represented by a transfer gate.
- Every gate that represents a failure already modelled in the same tree can be represented as an internal transfer gate.

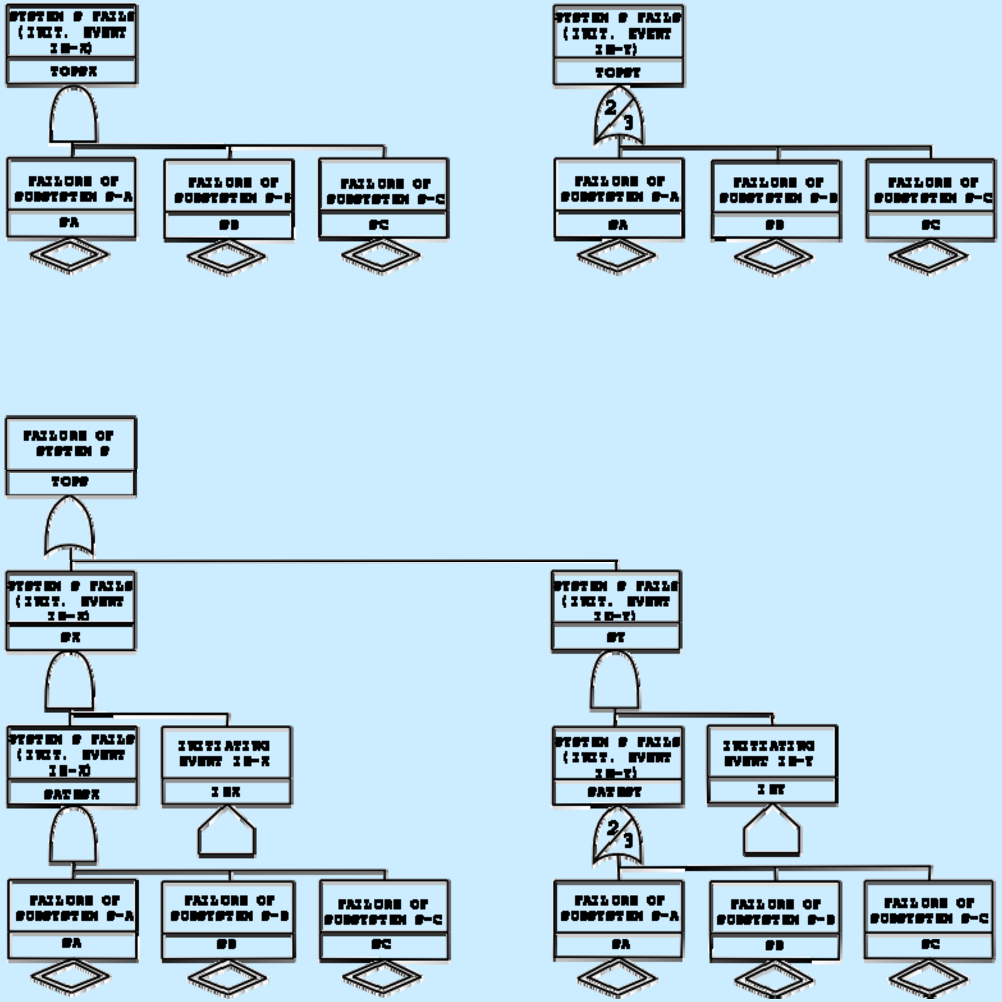
HOUSE EVENTS

- House events are useful in system modelling to avoid having to draw several system trees for different initiating events.

Initiating Event	Success Criteria
IE-X	1 sub-system required
IE-Y	2 sub-systems required

System analysis in a PSA (part 2)

HOUSE EVENTS (cont’d)



OTHER EXAMPLE (House Events)

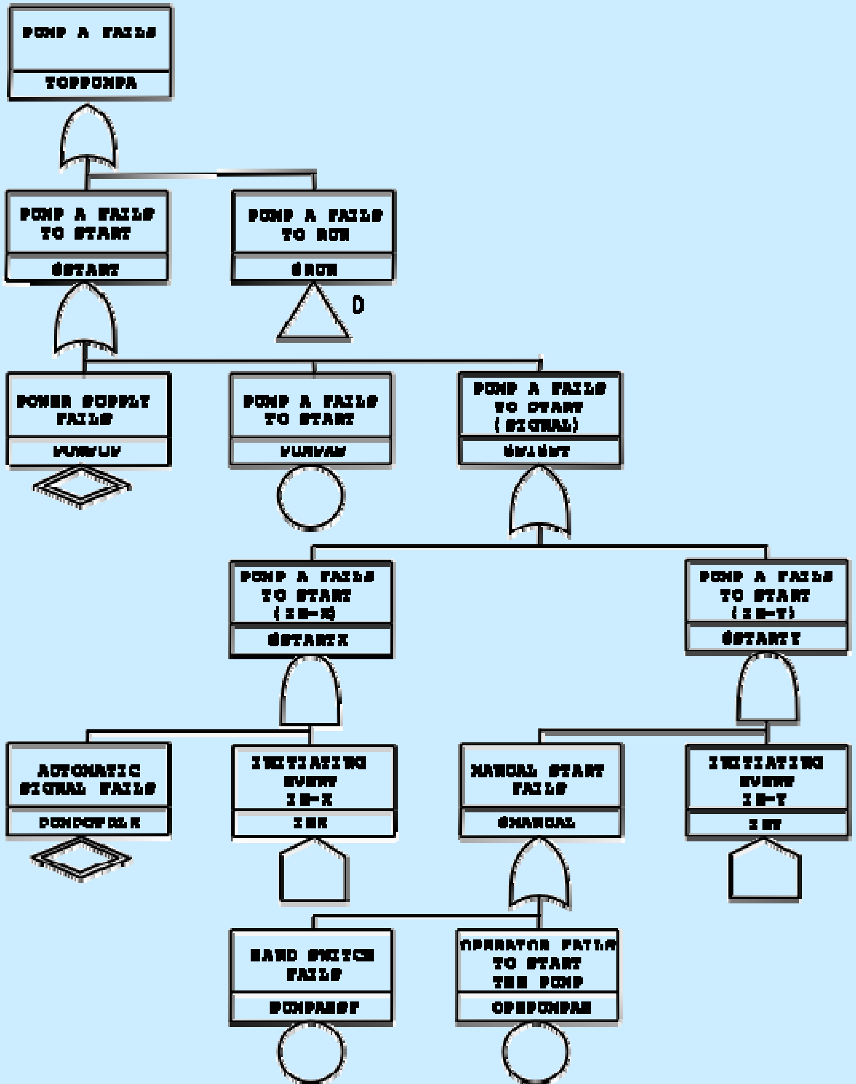
IE-X

Pump A starts automatically and there is no time for an operator backup action

IE-Y

Pump A has to be started by the operator

OTHER EXAMPLE (House Events) (cont'd)



CIRCULAR LOGIC LOOPS

- Circular logic loops can occur when two systems support each other.

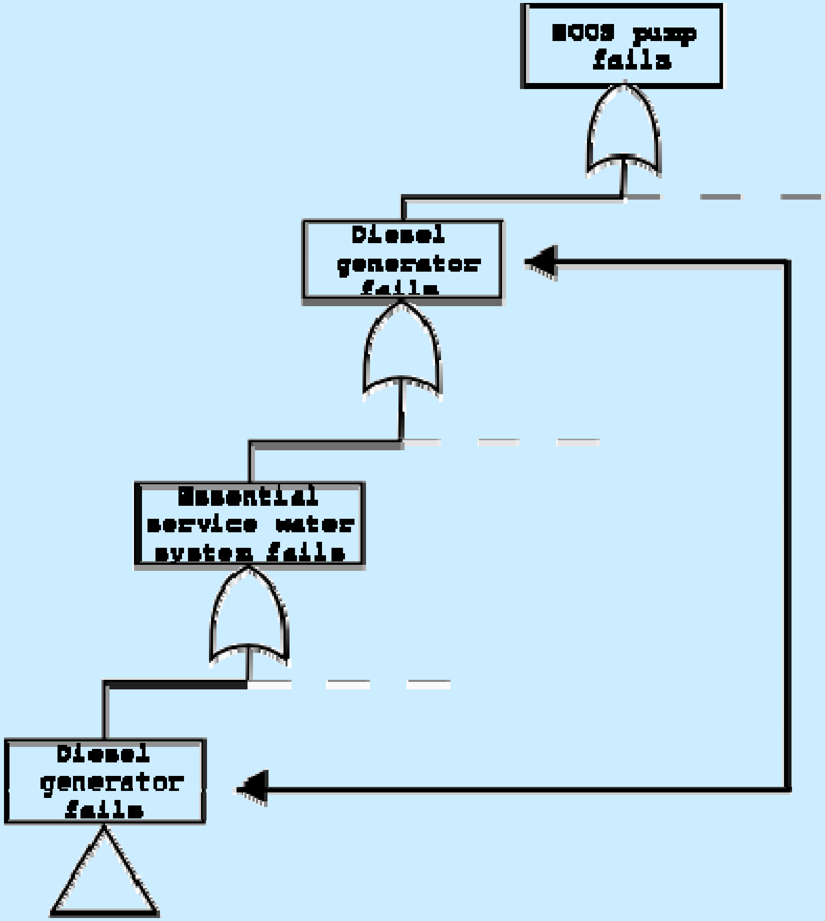
- For example:

  A diesel generator needs the essential service water system for cooling when operating.

  The essential service water system needs the diesel generator to start and run in the event of a loss of offsite power.

System analysis in a PSA (part 2)

CIRCULAR LOGIC LOOPS (cont’d)



ECCS pump fails

Diesel generator fails

Essential service water system fails

Diesel generator fails

SOLUTION TO CIRCULAR LOGIC LOOP

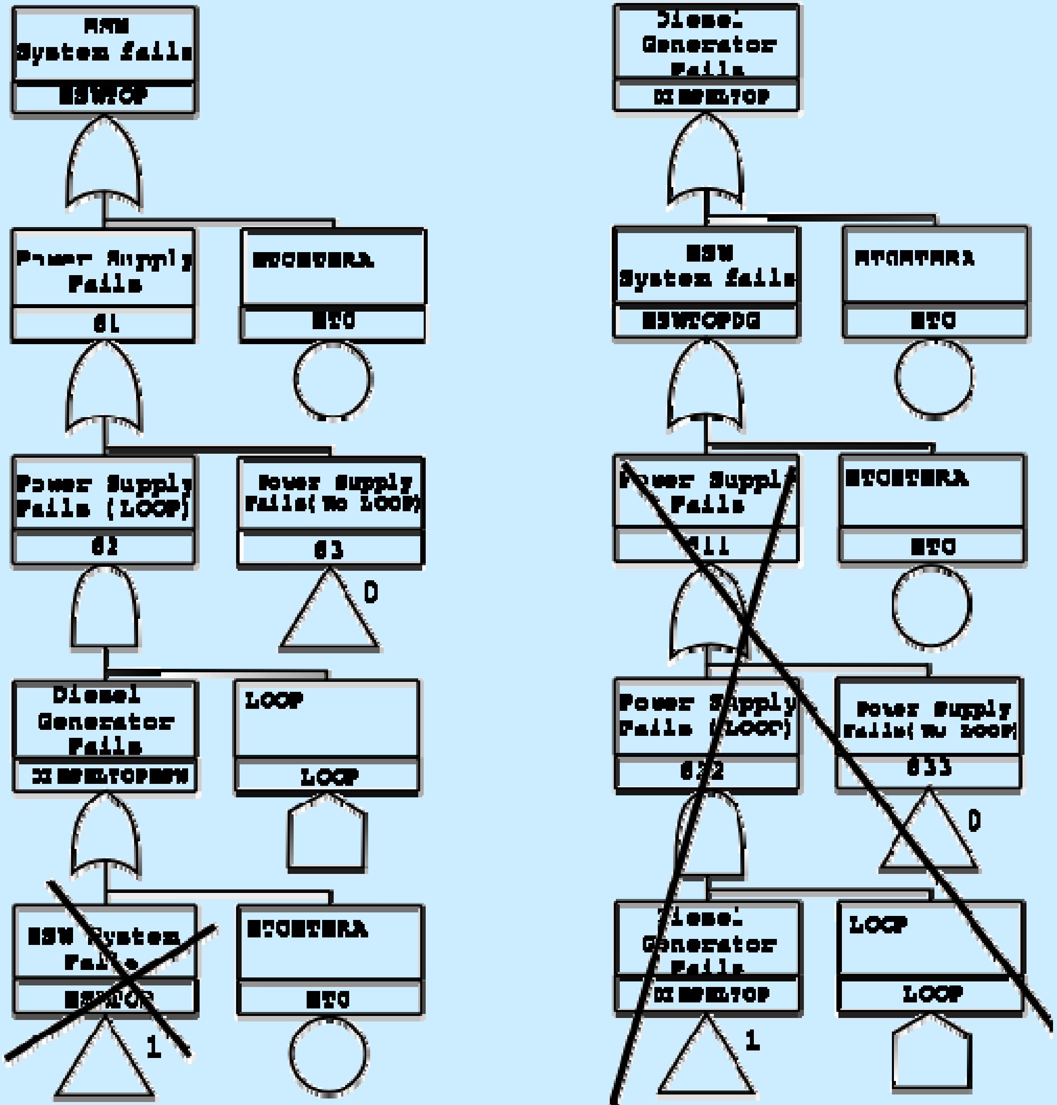
- This problem can be solved with two different models for each system.

- A tree for the diesel generator as a support system for the ESW is required. This tree does not have cooling in it. (If the ESW fails so will the diesel generator, but there is no need to include this - the ESW is failed whether or not the diesel generator fails!)

- A tree of the ESW system as a support system for the diesel generator is required. This tree does not have the power supply in it.

System analysis in a PSA (part 2)

SOLUTION TO CIRCULAR LOGIC LOOP (cont'd)



QUANTIFICATION

A preliminary quantification of the system is required to:

- Check that there are no circular logics in the trees
- Check if the system model can be simplified further
- Remove impossible cutsets (e.g., cutsets involving unavailability due to maintenance of both trains of the same system)
- Find possible common cause failures that have been missed

Where to get more information?

- References
  - The Fault Tree Handbook (NUREG-0492 Jan 1981)
  - IAEA-Safety Series 50-P-4 Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1) (1992)