Reliability and Availability Assessment Methods

Fault tree method

Event Tree Method

FAULT TREE METHOD (FT)

- A graphical risk analysis method for modeling how basic events (equipment failures, human actions, etc.) cause a complex, adverse outcome – system fault

Fault tree analysis methodology

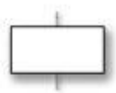
- System definition (subject of analysis)
- Defining the analyzed top event
- Step by step fault tree construction across all branches of the system
- Creating a qualitative solution
- Quantifying the results

FAULT TREE METHOD (FT)

The FT method is a **deductive** logical method that answers the question how something happened or how something could have happened?

- systematically linking an adverse event (the so-called top event) to the underlying basic events (failures and other)
- Connecting multiple events using logical functions (AND, OR)

SOME FAULT TREE SYMBOLS

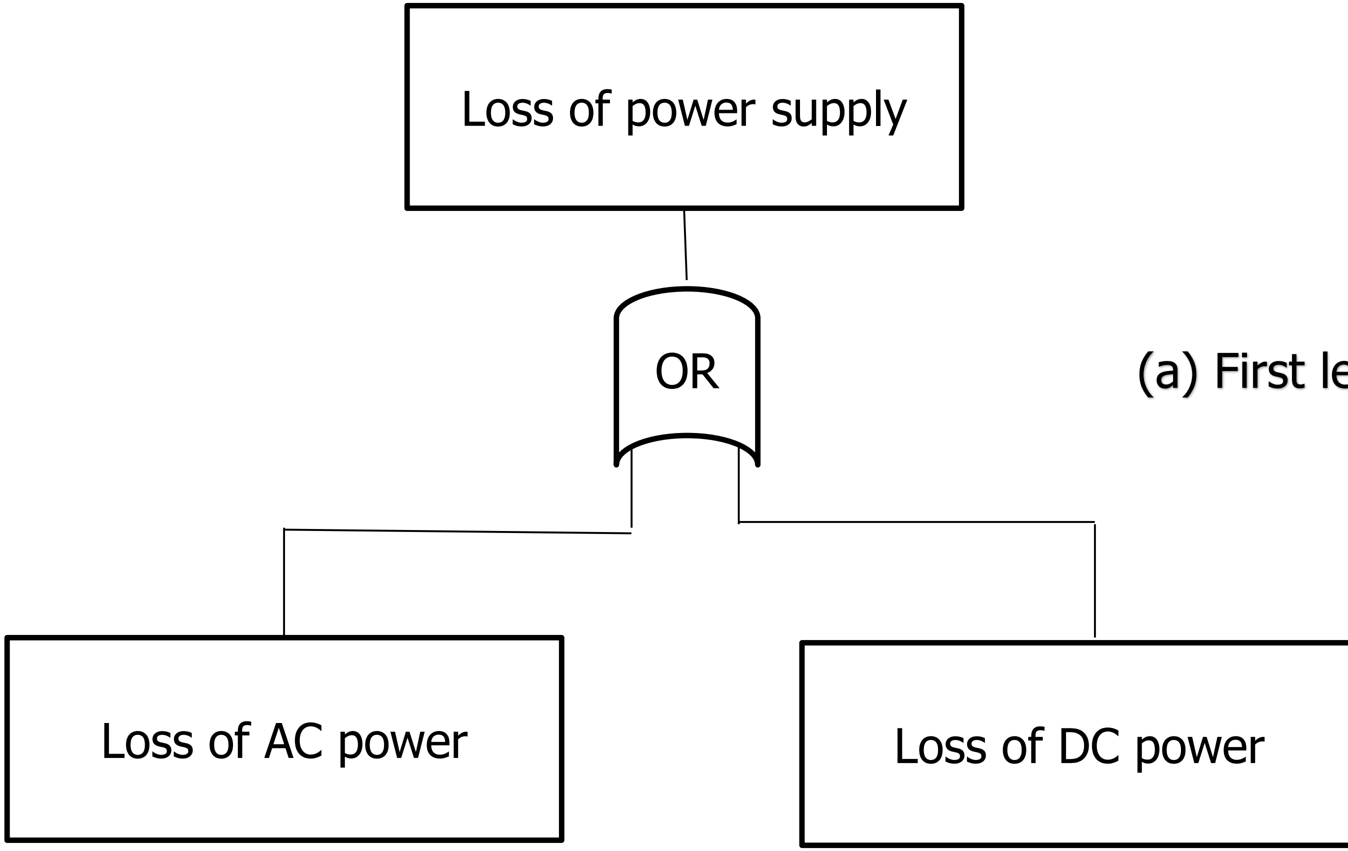
Symbol	Name	Description
		Primary Event Symbols
	Circle	**Basic Event** – a basic initiating fault requiring no further development
	Oval	**Conditioning Event** – specific conditions or restrictions that apply to any logic gate (used with INHIBIT gate)
	Diamond	**Undeveloped Event** – an event that is not developed further because it is of insufficient consequence or because information is unavailable
	House	**External Event** – an event which is normally expected to occur (not a fault event)
		Intermediate Event Symbols
	Rectangle	A fault event that occurs as a result of the logical **combination** of other events
		Gate Symbols
	OR Gate	The **union** operation of events, i.e. the output event occurs if (at least) one or more of the inputs occur
	AND Gate	The **intersection** operation of events, i.e. the output event occurs if and only if all the inputs occur
	INHIBIT Gate	The output event occurs if the (single) input event occurs in the presence of an enabling condition (i.e. Conditioning Event (oval) drawn to the right of the gate)
		Transfer Symbols
	Triangle-in	Indicates that the tree is developed further someplace else (e.g. another page)
	Triangle-out	Indicates that this portion of the tree is a sub-tree connected to the corresponding Triangle-In (appears at the top of the tree)

FAULT TREE METHOD

The structure of a FT is the following: an adverse (top) event, which can be a facility failure or other accident under investigation, is placed on top of the tree and then linked, by logical functions to other events (failures) that are by nature "more basic”

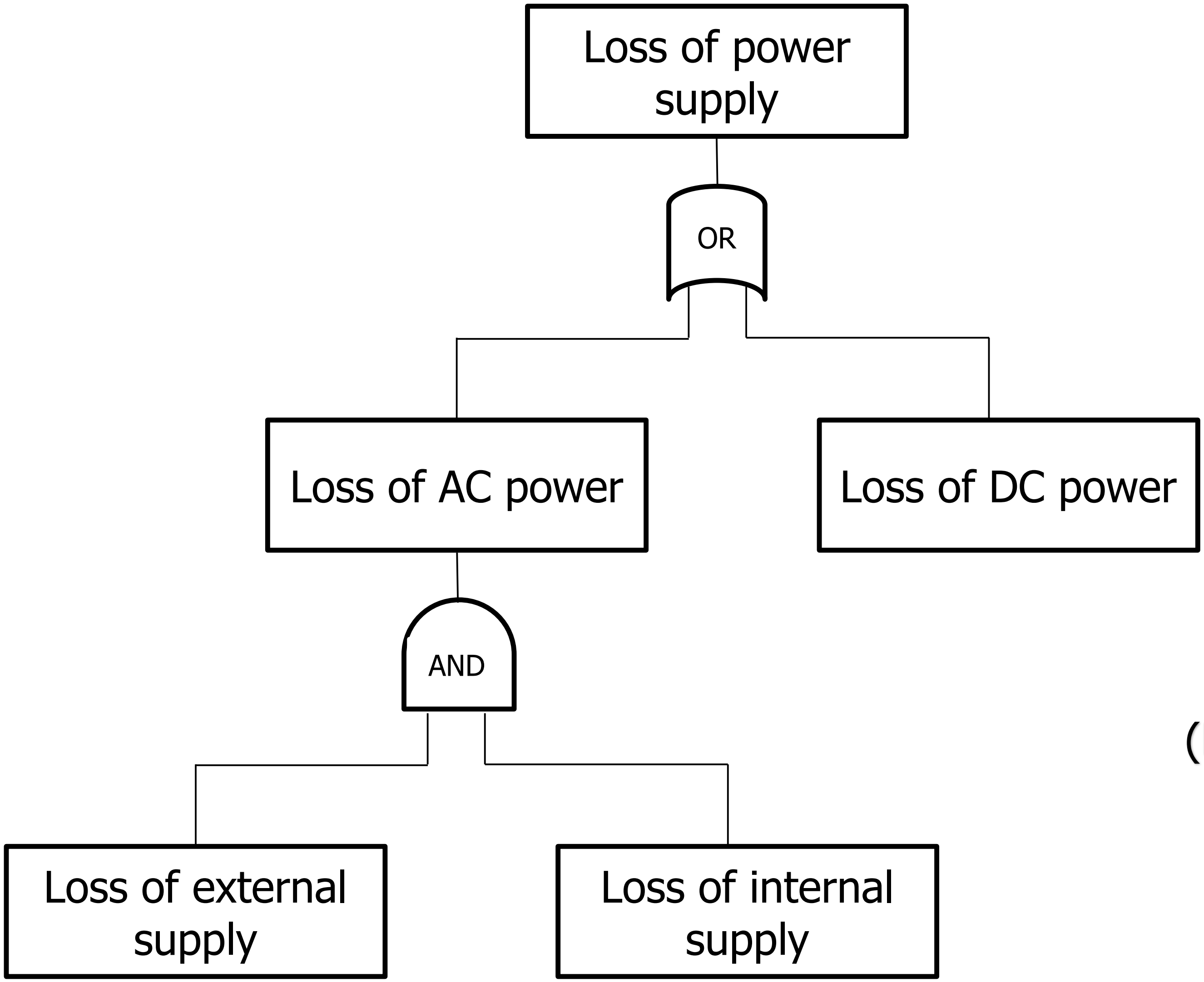
- other events are arranged below each other in levels that depend on the degree of their complexity

FT – loss of power supply



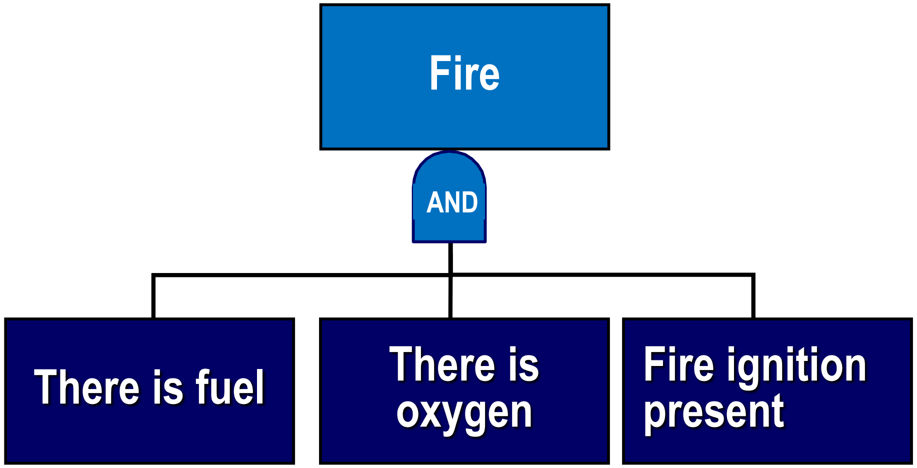
(a) First level

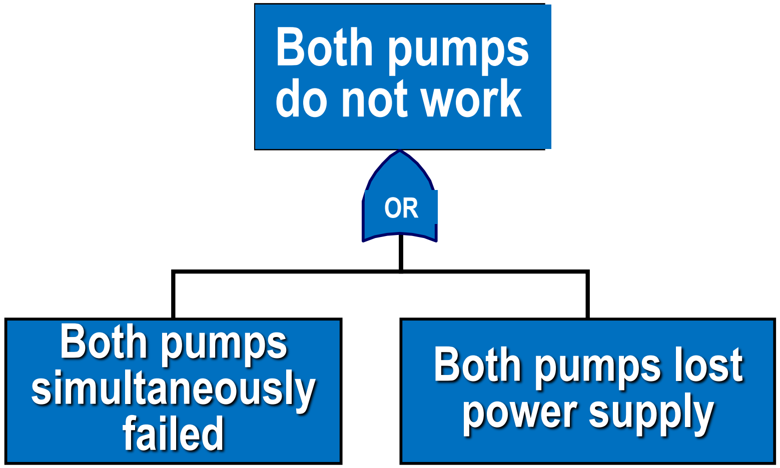
FT – loss of power supply



(b) Second level

“AND” and “OR” gate





FAULT TREE METHOD

The fault tree ends with the fundamental (basic) events representing the primary, basic faults of the facility, the component faults.

The process involves moving backwards in time searching for the possible root causes of an adverse event (failure). In doing so, the fault tree can be developed to an arbitrary level of detail, and the recommended approach is to develop the fault tree to a level (component) for which there are adequate data.

For example, a fault tree of an electronic system will end up with an amplifier instead of the transistors and resistors from which the amplifier is built, if there is a (satisfactory) failure information for such devices (amplifiers).

FAULT TREE METHOD– qualitative and quantitative analysis

- The method requires full knowledge of a system operation (creation of graphical reliability model and physical model of the system)
- By forming the structure of the fault tree, further qualitative and then quantitative analysis is carried out. The goal of the qualitative analysis is to reduce the fault tree to a logically equivalent but simpler form using Boolean algebra.

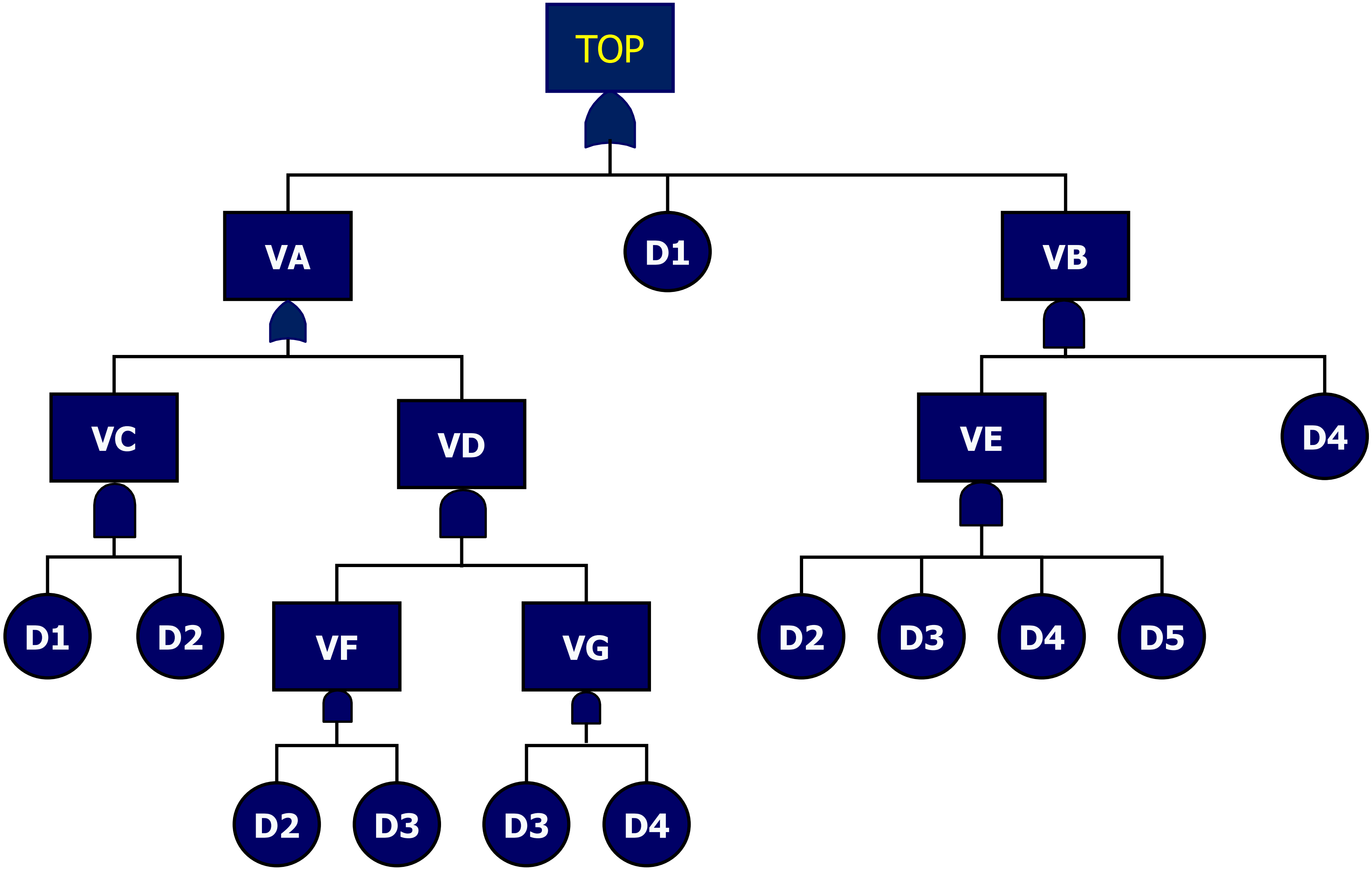
Knowledge of the probability of occurrence of underlying events enables a quantitative analysis of the fault tree

- numerical calculation of the probability of failure (adverse event), ie. unreliability or unavailability of the system.

Boolean algebra laws

Law/Theorem	Law of Addition	Law of Multiplication
Identity Law	$x + 0 = x$	$x \cdot 1 = x$
Complement Law	$x + x' = 1$	$x \cdot x' = 0$
Idempotent Law	$x + x = x$	$x \cdot x = x$
Dominant Law	$x + 1 = 1$	$x \cdot 0 = 0$
Involution Law	$(x')' = x$	
Commutative Law	$x + y = y + x$	$x \cdot y = y \cdot x$
Associative Law	$x+(y+z) = (x+y)+z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
Distributive Law	$x \cdot (y+z) = x \cdot y+x \cdot z$	$x+y\cdot z = (x+y) \cdot (x+z)$
Demorgan's Law	$(x+y)' = x' \cdot y'$	$(x \cdot y)' = x' + y'$
Absorption Law	$x + (x \cdot y) = x$	$x \cdot (x + y) = x$

Fault tree example



$$TOP = VA + D1 + VB$$

$$= (VC + VD) + D1 + VE \cdot D4$$

$$= D1 \cdot D2 + VF \cdot D6 + D1 + D2 \cdot D3 \cdot D4 \cdot D5 \cdot D4$$

$$= D1 \cdot D2 + D2 \cdot D3 \cdot D3 \cdot D4 + D1 + D2 \cdot D3 \cdot D4 \cdot D5 \cdot D4$$

$$= D1 \cdot D2 + D2 \cdot D3 \cdot D3 \cdot D4 + D1 + D2 \cdot D3 \cdot D4 \cdot D4 \cdot D5$$

Repeated event

$$= D1 \cdot D2 + D2 \cdot D3 \cdot D4 + D1 + D2 \cdot D3 \cdot D4 \cdot D5$$

$$TOP = D1 + D2 \cdot D3 \cdot D4$$

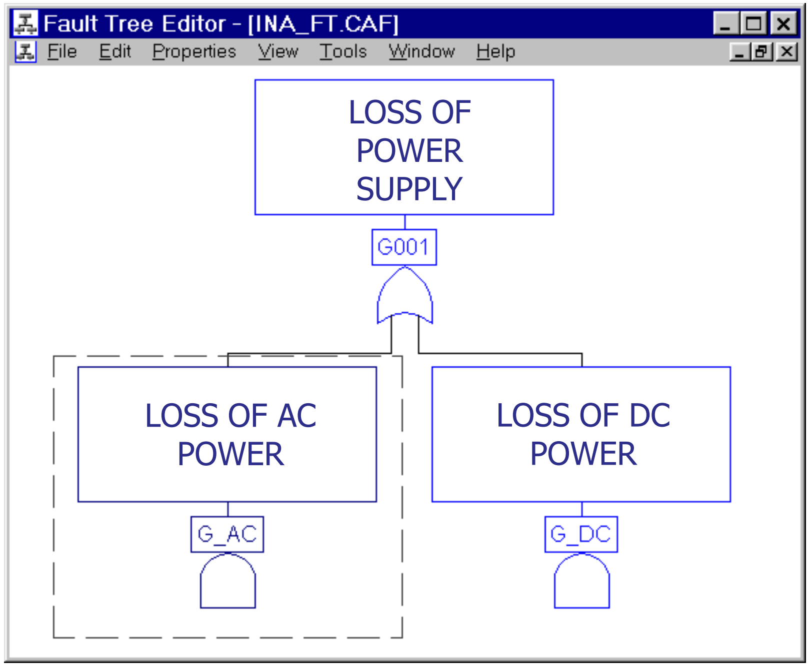
supersets

Minimal cut sets

FT for loss of power supply (example)

Model background and assumptions:

- the system is dependent on AC and DC power
- for the DC power there are two redundant sources (batteries and alternating source)
- the AC power also comes from two redundant sources (external grid and diesel generator)
- the model stops at the level of individual subsystems (control and physical part) for which we know the failure probabilities



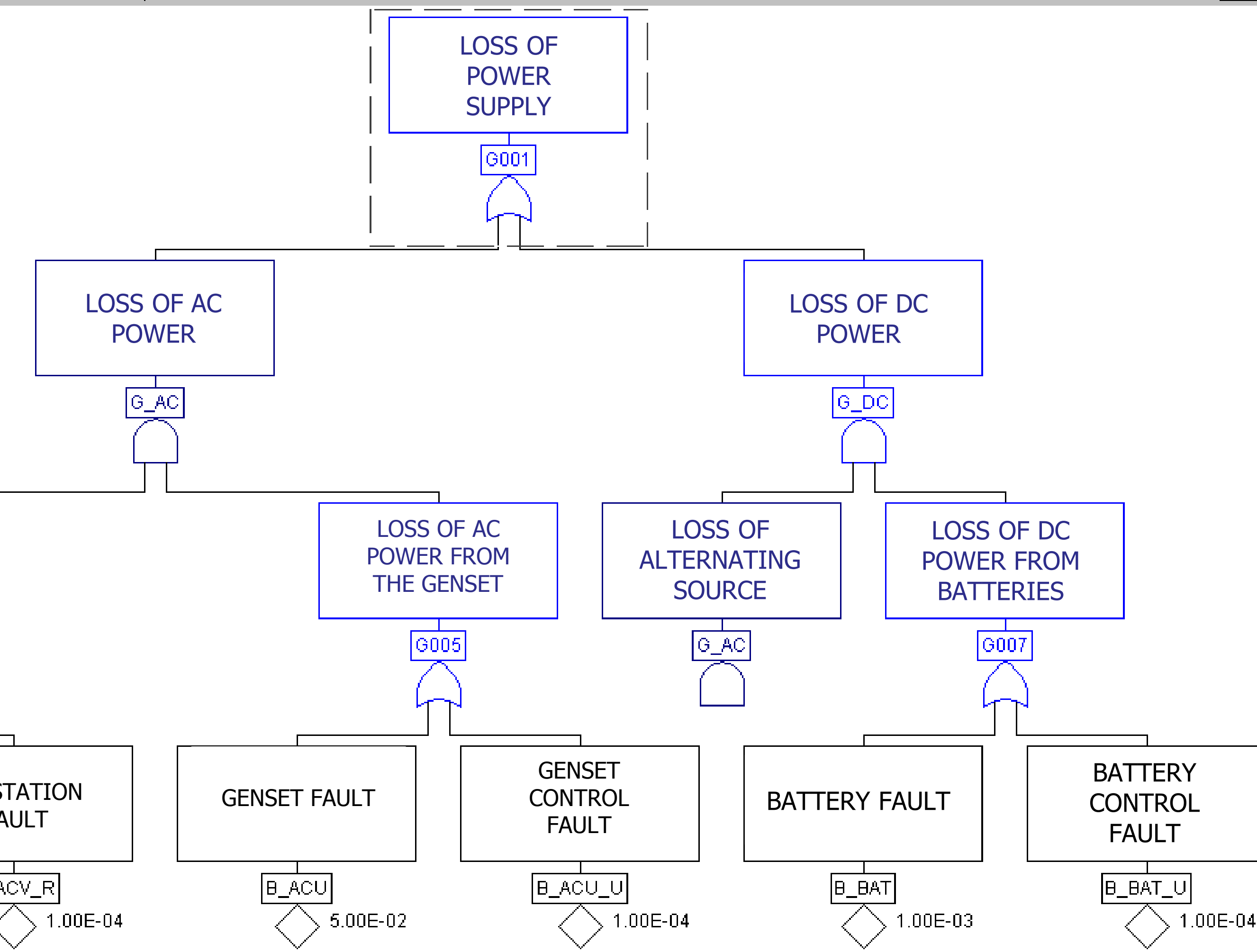
Example of FT (AC/DC)

Fault Tree Editor - [INA_FT.CAF]

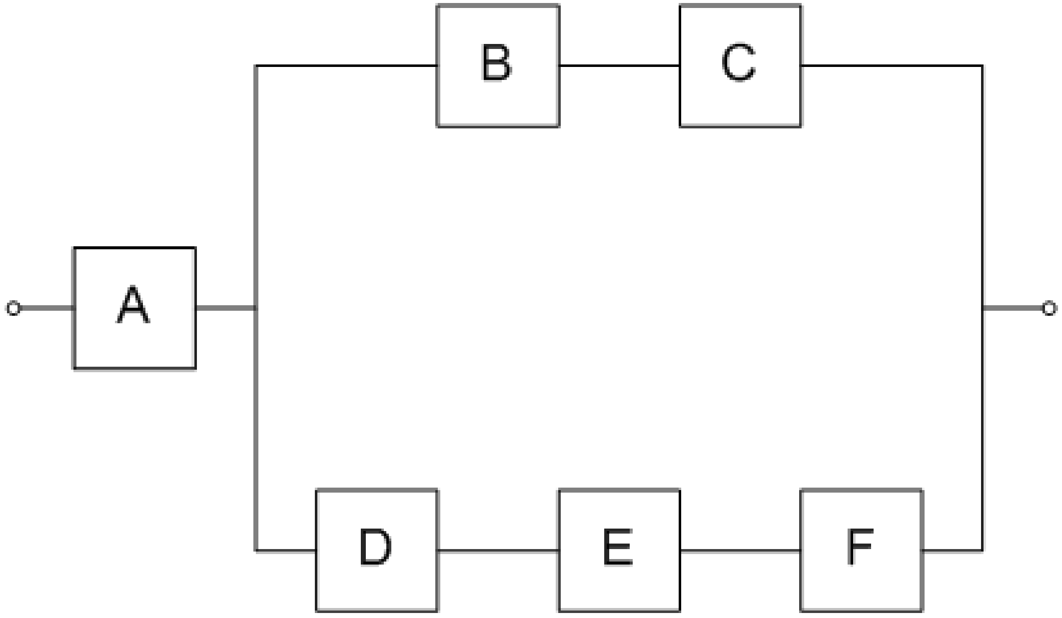
File Edit Properties View Tools Window Help

Model background and assumptions:

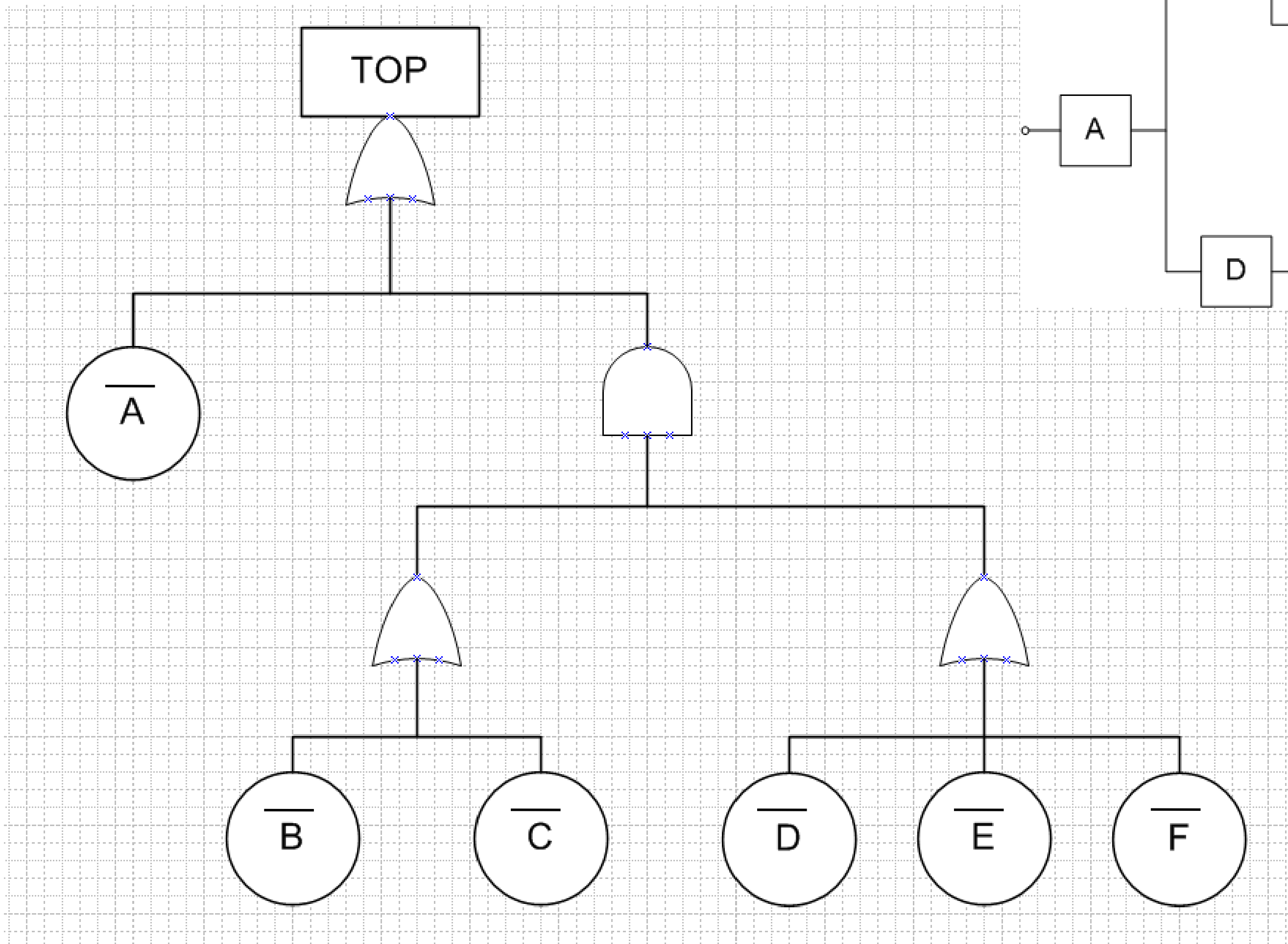
- the system is dependent on AC and DC power
- for the DC power there are two redundant sources (batteries and alternating source)
- the AC power also comes from two redundant sources (external grid and diesel generator)
- the model stops at the level of individual subsystems (control and physical part) for which we know the failure probabilities

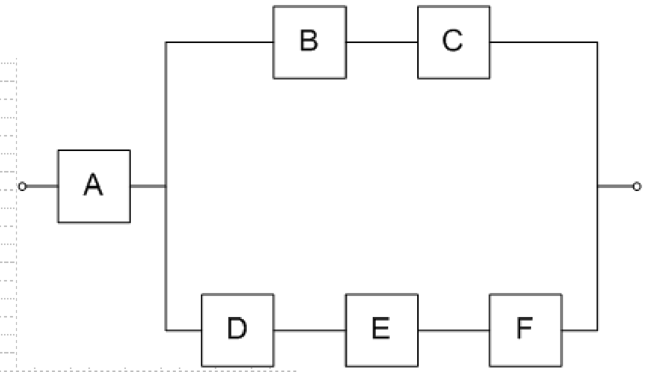


Example – reliability model



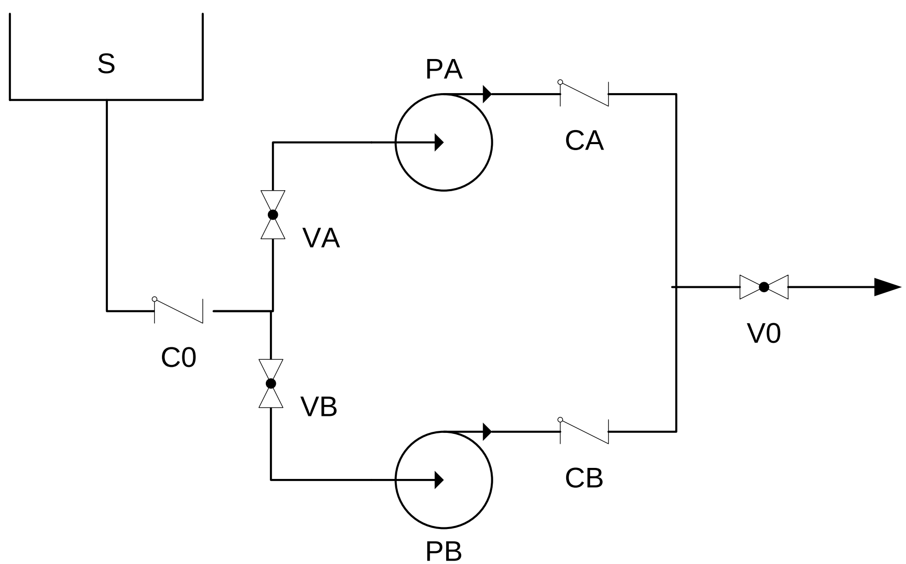
Example – fault tree



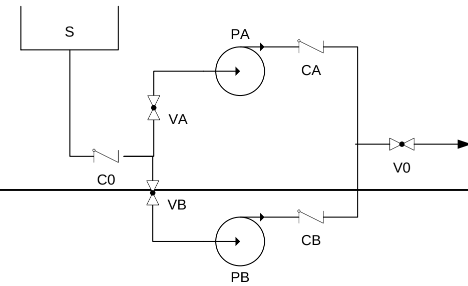


Event – water supply from the tank disabled

The goal of the system is to enable the water supply from the tank to the arrow on the right side of the figure.
Success criteria: one pump is sufficient
Power supply (pumps, valves, instrumentation and control):
L1 and corresponding instrumentation have their own source – E1
L2 and corresponding instrumentation have their own source – E2
Valve V0 is supplied from both sources.



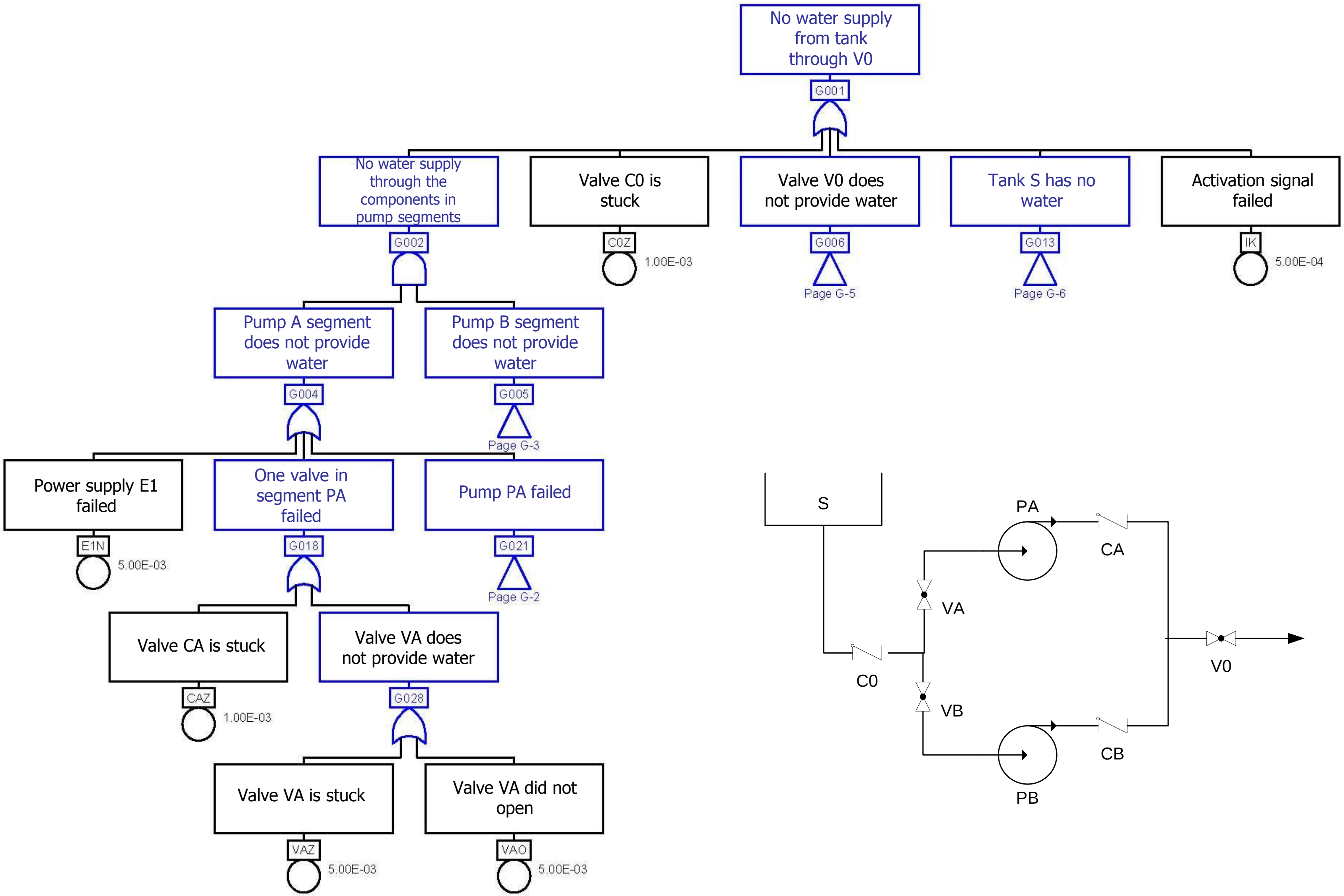
Conditions



Component	Symbol	Faults	Probability/Frequency
Tank	Sx	- There is no water in the tank - Water is leaking out of the tank	0.005 0.005
Control valve	Vx	- Valve is not open - Valve is stuck	0.005 0.005
Check valve	Cx	- Valve is stuck	0.001
Pump	Px	- Pump cannot start - Pump fails during operation - Pump is in maintenance	0.001 0.0005 h^{-1} 0.005
Pipes		- Pipes are assumed sufficiently reliable and are not modeled	-
Activation signal		- Signal has not activated the system	0.0005
Power supply		- Power supply is incorrect	0.005

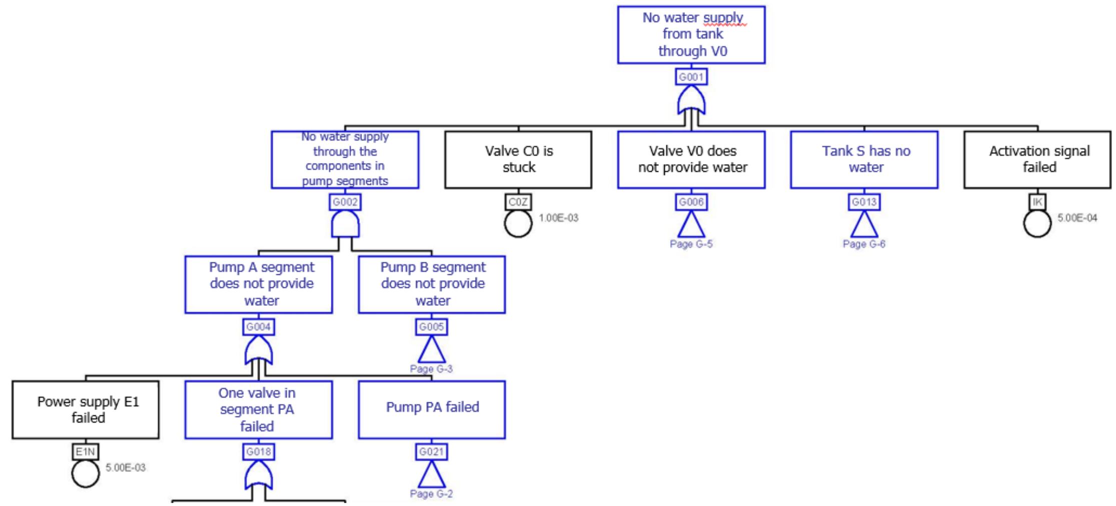
- The system has to work 20 hours.
- At most one pump can be in maintenance at once.
- There is one signal that activates the system when required.

Solution

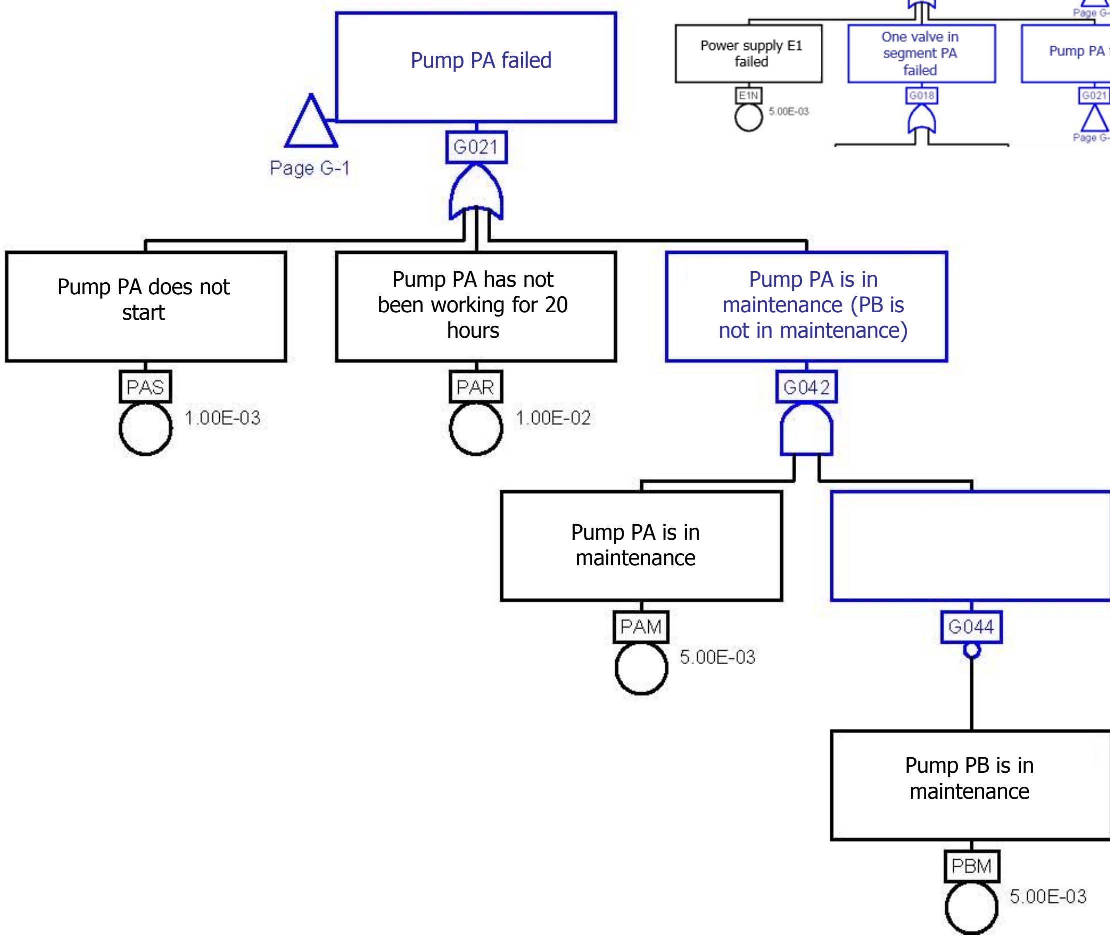


No water supply from tank through V0
G001
No water supply through the components in pump segments
G002
Valve C0 is stuck
C0Z
1.00E-03
Valve V0 does not provide water
G006
Page G-5
Tank S has no water
G013
Page G-6
Activation signal failed
IK
5.00E-04
Pump A segment does not provide water
G004
Pump B segment does not provide water
G005
Page G-3
Power supply E1 failed
E1N
5.00E-03
One valve in segment PA failed
G018
Pump PA failed
G021
Page G-2
Valve CA is stuck
CAZ
1.00E-03
Valve VA does not provide water
G028
Valve VA is stuck
VAZ
5.00E-03
Valve VA did not open
VAO
5.00E-03
S
PA
CA
VA
C0
V0
VB
CB
PB

Solution

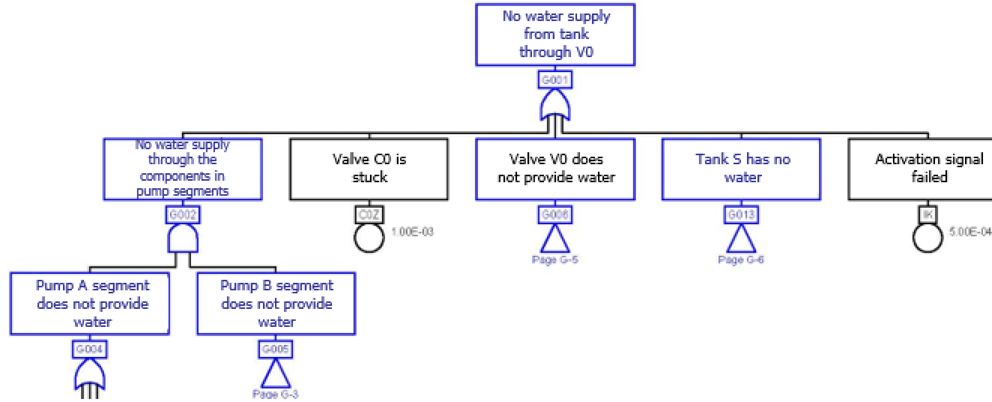


No water supply from tank through V0
G001
No water supply through the components in pump segments
G002
Valve C0 is stuck
COZ
1.00E-03
Valve V0 does not provide water
G006
Page G-5
Tank S has no water
G013
Page G-6
Activation signal failed
IK
5.00E-04
Pump A segment does not provide water
G004
Pump B segment does not provide water
G005
Page G-3
Power supply E1 failed
E1N
5.00E-03
One valve in segment PA failed
G018
Pump PA failed
G021
Page G-2

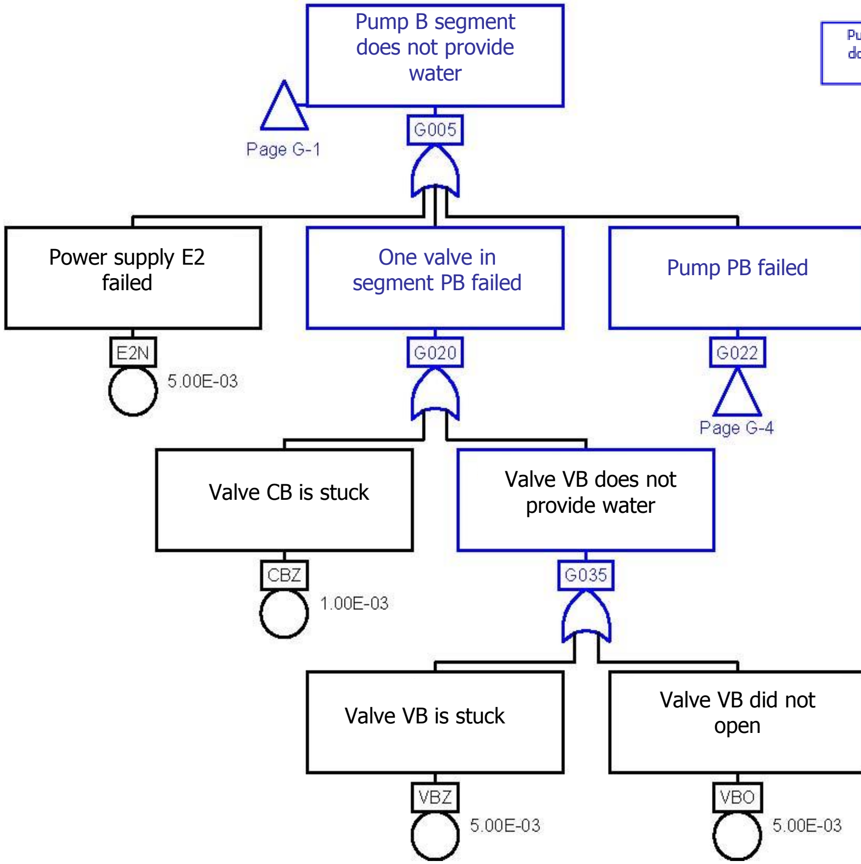


Pump PA failed
Page G-1
G021
Pump PA does not start
PAS
1.00E-03
Pump PA has not been working for 20 hours
PAR
1.00E-02
Pump PA is in maintenance (PB is not in maintenance)
G042
Pump PA is in maintenance
PAM
5.00E-03
G044
Pump PB is in maintenance
PBM
5.00E-03

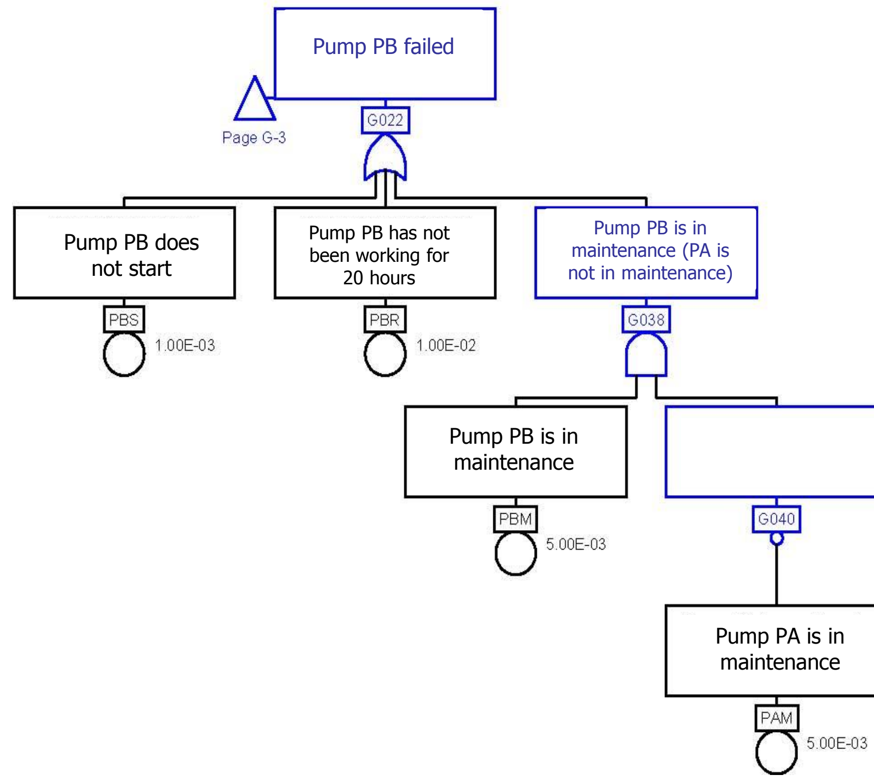
Solution



No water supply from tank through V0
G001
No water supply through the components in pump segments
G002
Valve C0 is stuck
C0Z
1.00E-03
Valve V0 does not provide water
G006
Page G-5
Tank S has no water
G013
Page G-6
Activation signal failed
IK
5.00E-04
Pump A segment does not provide water
G004
Pump B segment does not provide water
G005
Page G-3

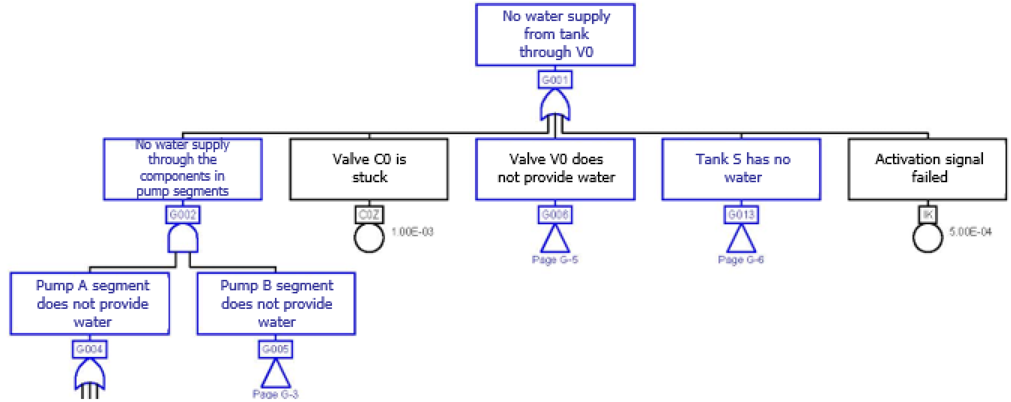


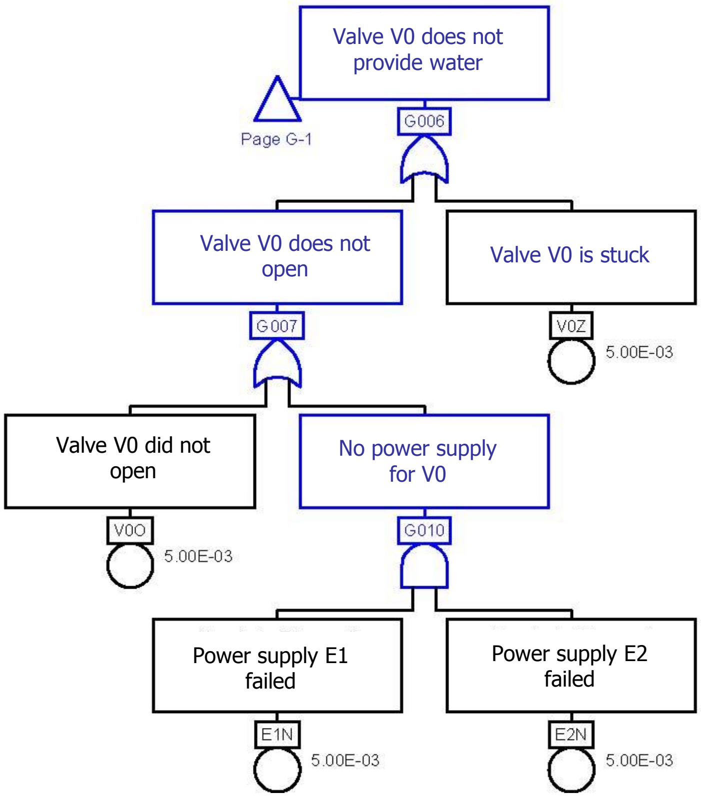
Pump B segment does not provide water
Page G-1
G005
Power supply E2 failed
E2N
5.00E-03
One valve in segment PB failed
G020
Pump PB failed
G022
Page G-4
Valve CB is stuck
CBZ
1.00E-03
Valve VB does not provide water
G035
Valve VB is stuck
VBZ
5.00E-03
Valve VB did not open
VBO
5.00E-03

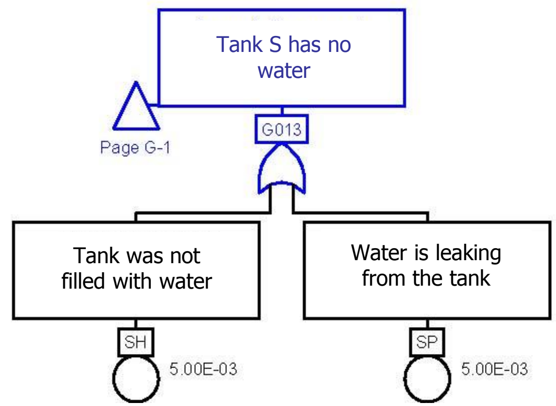


Pump PB failed
Page G-3
G022
Pump PB does not start
PBS
1.00E-03
Pump PB has not been working for 20 hours
PBR
1.00E-02
Pump PB is in maintenance (PA is not in maintenance)
G038
Pump PB is in maintenance
PBM
5.00E-03
G040
Pump PA is in maintenance
PAM
5.00E-03

Solution







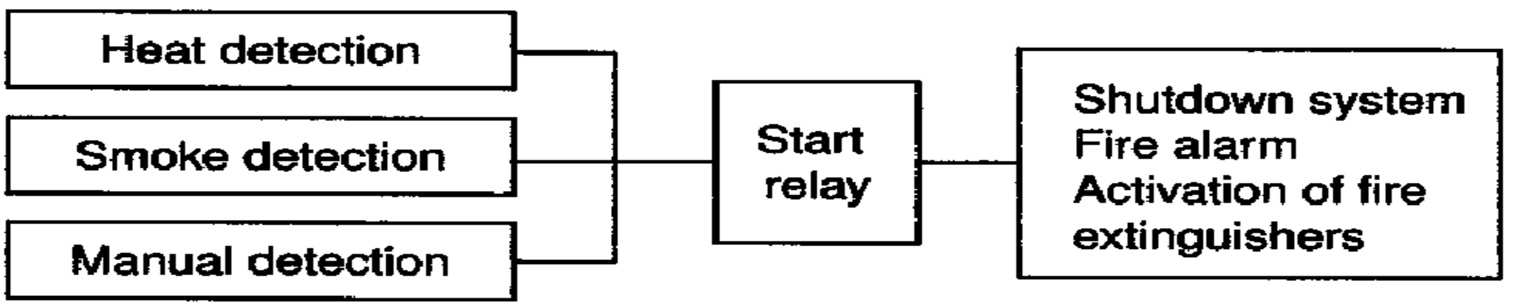
Result: 0.0225

Fire protection system

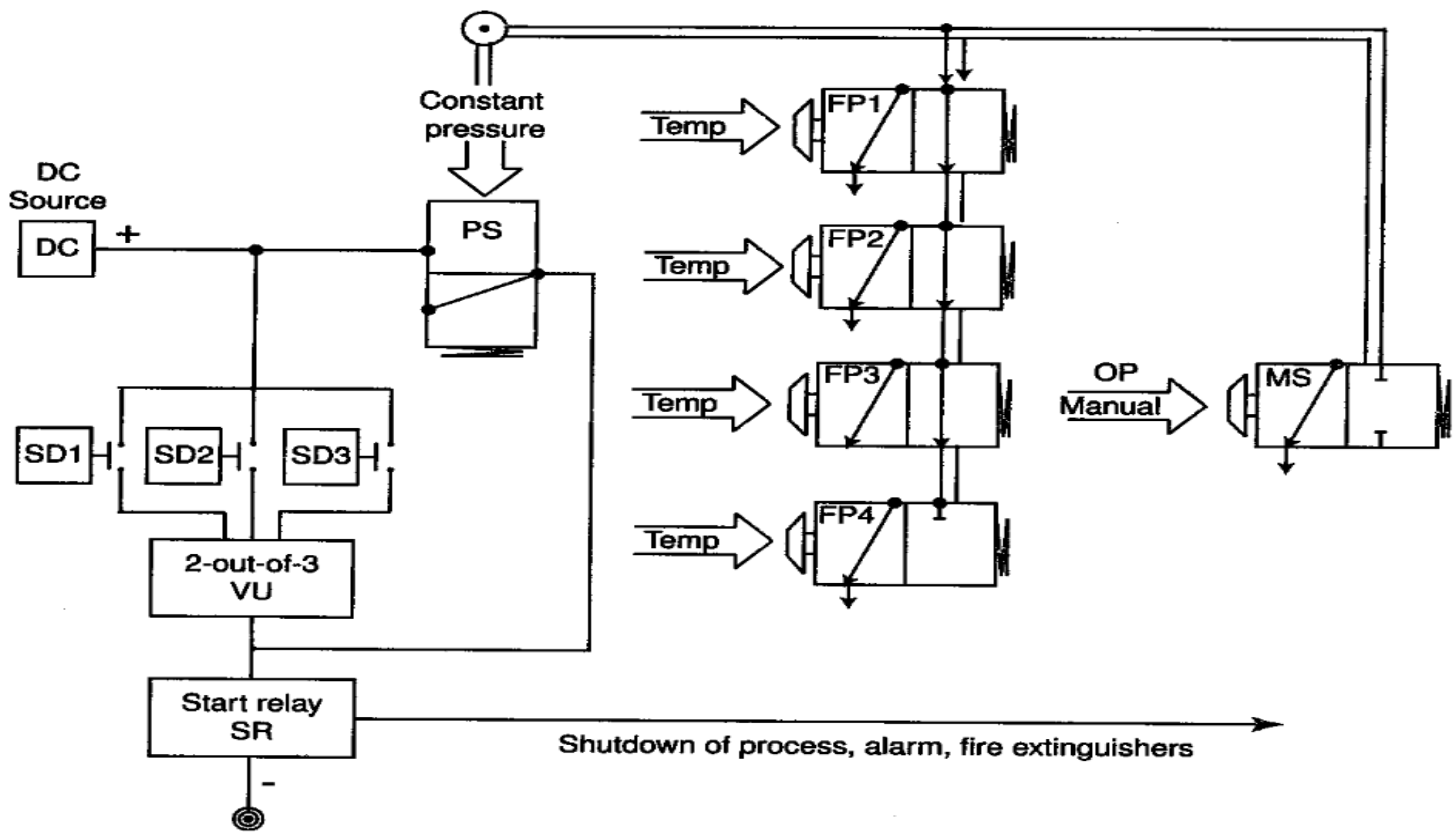
- Draw a fire protection system fault tree.
- The system is divided in three parts: heat detector, smoke detector and manual activation. One DC power system is used for all three systems.
- The heat detector consists of 4 thermal fuses (FP1 – FP4) which fail when the temperature achieves 72 °C. The system pressure is 3 bar. If any of thermal fuses fails, the air will be released and the pressure drop will actuate a switch that connects a DC energy source with a relay that starts the fire extinguishing system.
- The smoke detector consists of 3 optical smoke detectors SD1 – SD3. The detectors are very sensitive so in order to avoid the potential wrong command, the 2/3 logic is embedded, which means that two out of three detectors have to actuate for the system to actuate. A special voting unit checks the detector signals and finally actuates the relay by closing the contacts towards the energy source.
- Additionally, there is a possibility of a manual activation through the special switch in the compressed air system, which is also triggered by the pressure drop as are the heat detectors.

Fire protection system

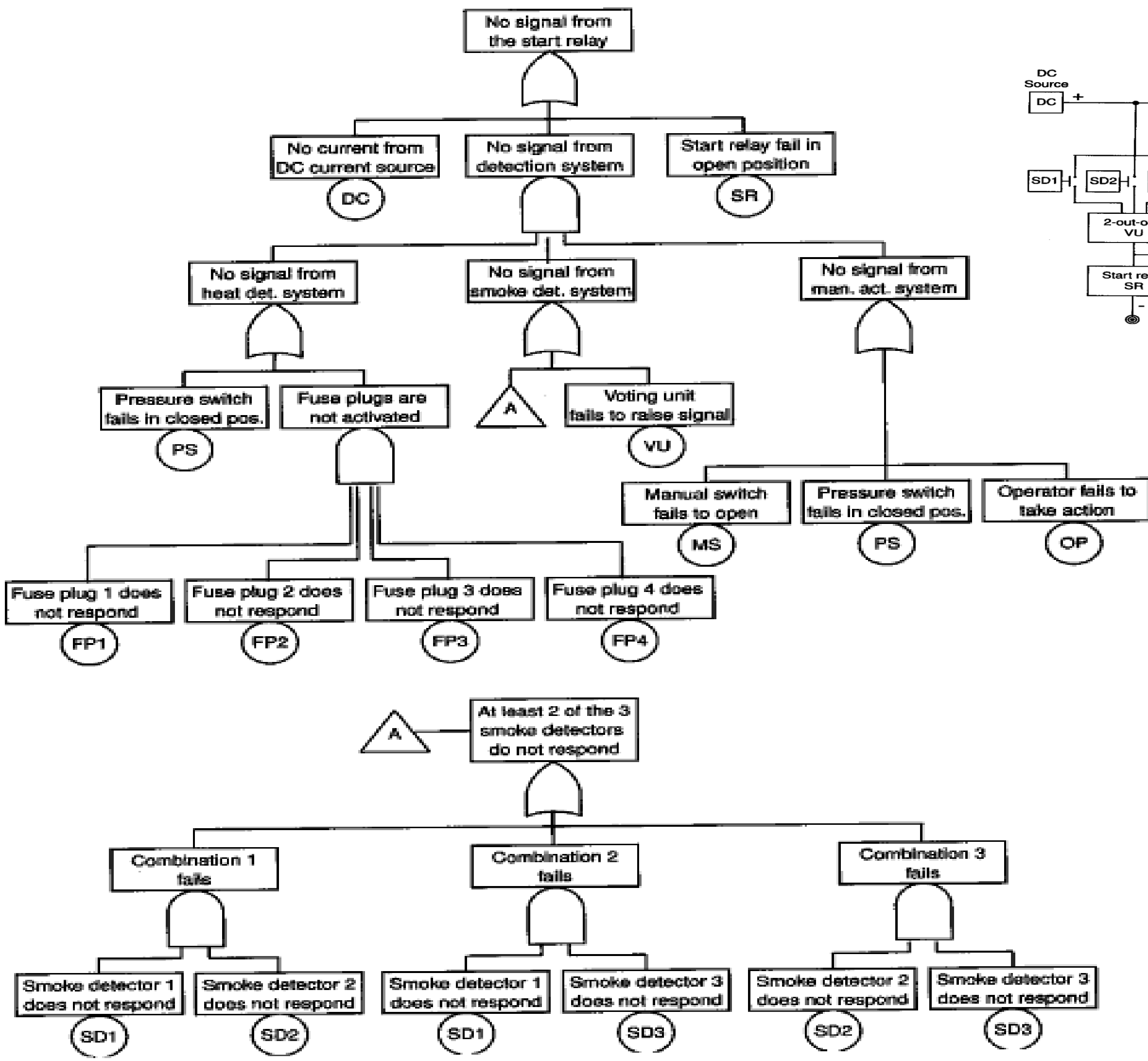
- Simplified system scheme

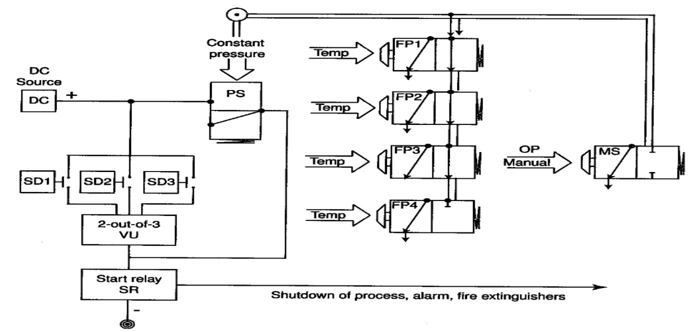


Fire protection system



Fire protection system





EVENT TREE (ET)

- <u>graphical</u> representation of all events in the system
- an inductive method of identifying different possible outcomes of a postulated initial (initiating) event

INITIAL EVENTS IN ET SYSTEM WITH A SEQUENTIAL LOGIC

- **initial events in technical systems are usually different failure events, system failures, but also transient events such as sudden changes in load or loss of load**
- **these may be events occurring outside the system, but they always represent high requirements for the safe operation of the system**

EVENT TREE METHOD

- **The selected initial event is decisive for the course of the analysis: considered are its consequences which are limited by the actions of the safety systems**

EVENT TREE METHOD – application to a system protected by the safety systems

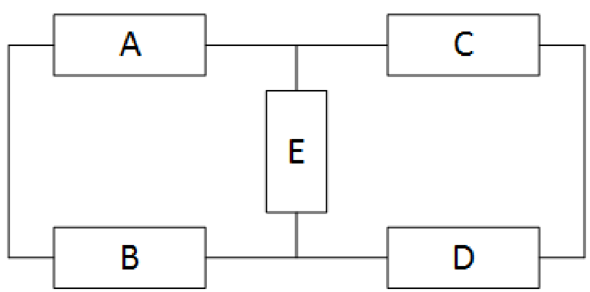
- at the moment of defining the initial event, all <u>safety systems</u> that need to act <u>must be identified</u>; these systems thus become part of the event tree structure
- the <u>probability</u> of possible <u>failures of the safety systems</u> is determined by means of the <u>fault tree analysis</u>

ET APPLICATION TO A SYSTEM THAT WORKS CONTINUOUSLY (CONSTANTLY)

The components can be observed in an arbitrary order since their operation is not chronological with respect to each other.

In the illustrative example, we will observe the components in the following order: A, B, C, D and E (notation of the correct work of the components and $\bar{A}, \bar{B}, \bar{C}, \bar{D}$ *and* $\bar{E}$ is the notation of the component failures).

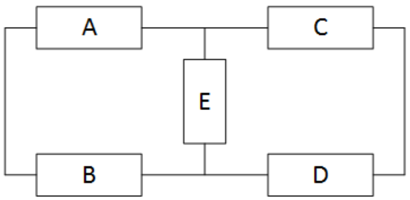
Initially, all components work correctly, we want to determine the reliability of the system after one year.

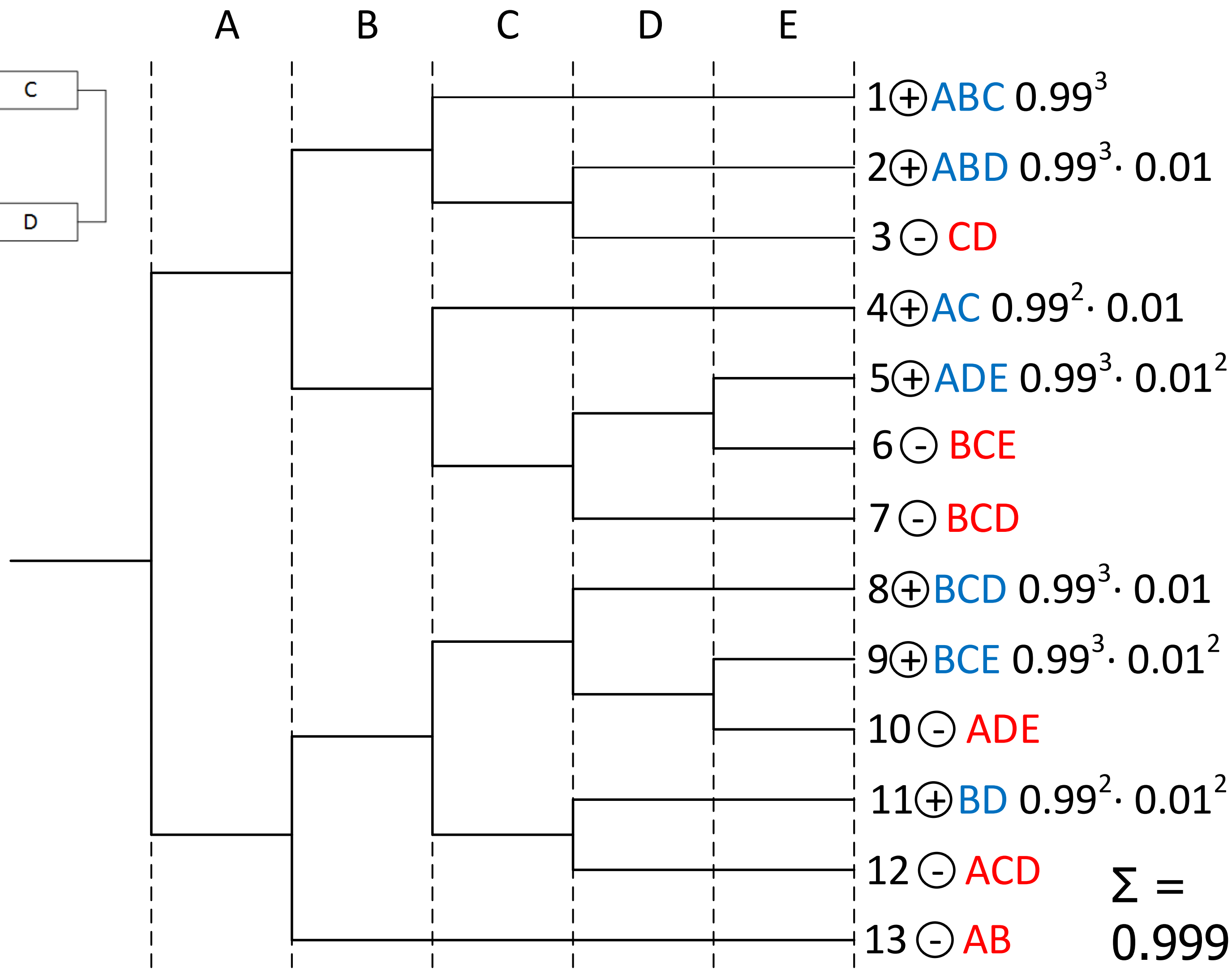


REDUCED EVENT TREE

- Reduced extent of the event tree
- It is used when we can conclude about the final state (path) without observing all the components included in the event tree

REDUCED EVENT TREE





$\Sigma = 0.999798$

REDUCED EVENT TREE

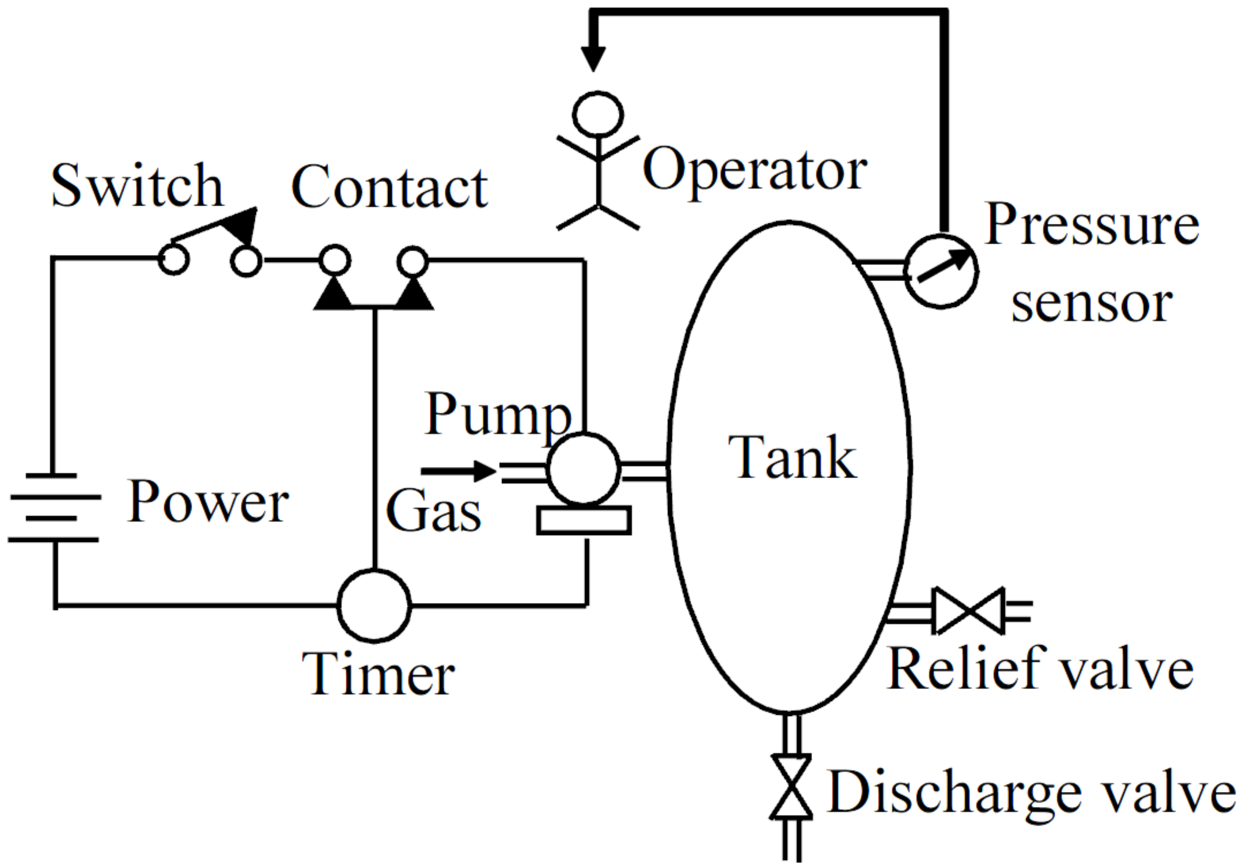
The calculation of reliability (unreliability) or steady state availability (unavailability) becomes less extensive as well:

$$R_S(1\ \text{year}) = R_A R_B R_C + R_A R_B Q_C R_D + R_A Q_B R_C + R_A Q_B Q_C R_D R_E + Q_A R_B R_C R_D + Q_A R_B R_C Q_D R_E + Q_A R_B Q_C R_D = 0{,}999798.$$

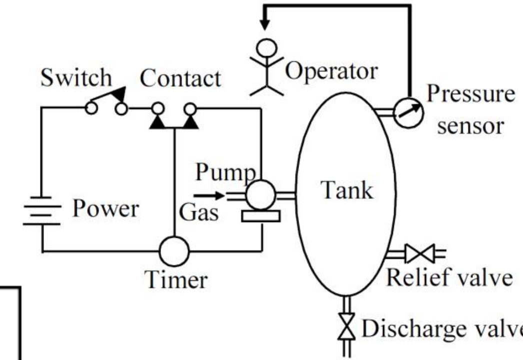
Similarly:

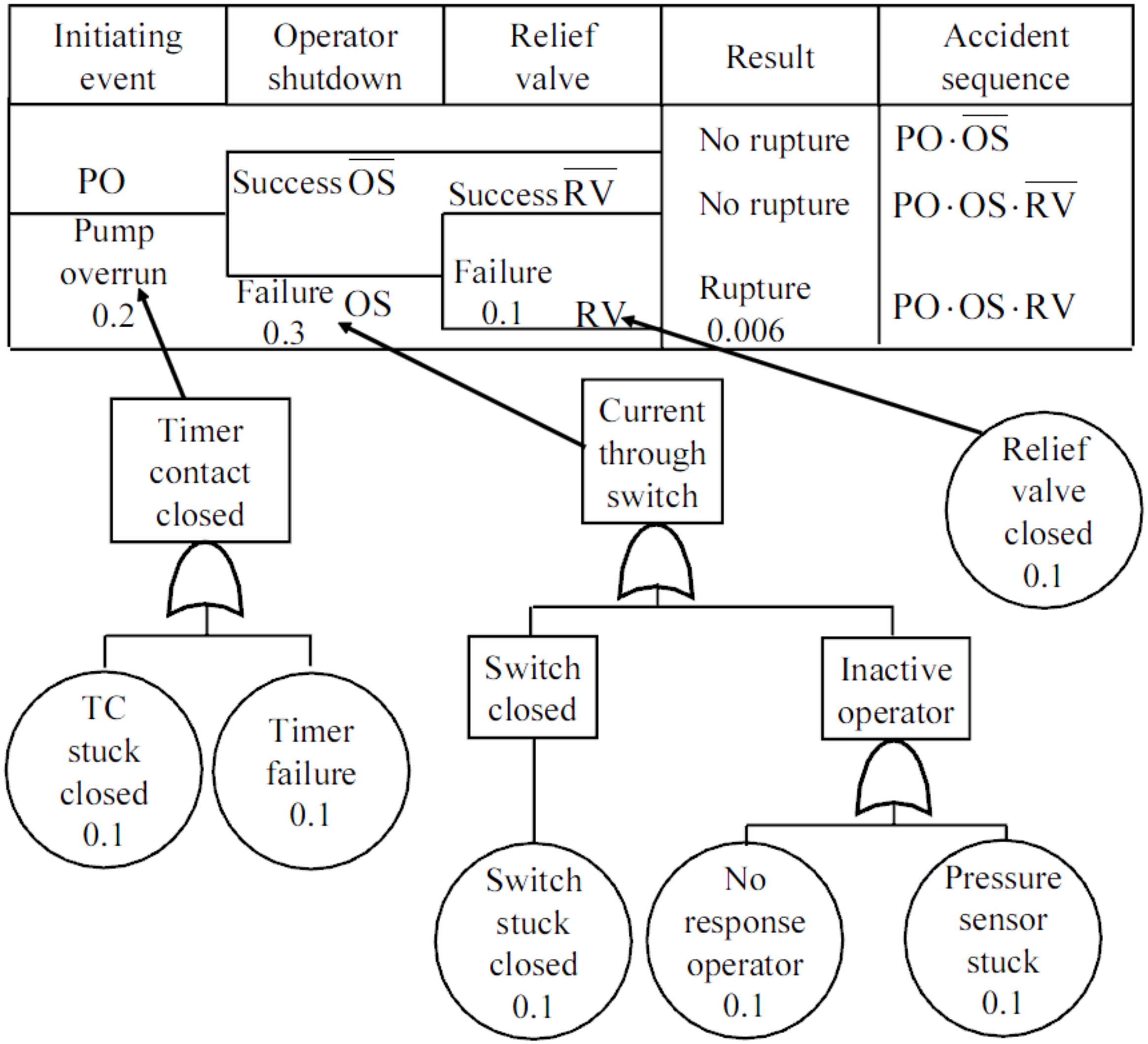
$$Q_S(1\ \text{year}) = R_A R_B Q_C Q_D + R_A Q_B Q_C R_D Q_E + R_A Q_B Q_C Q_D + Q_A R_B R_C Q_D Q_E + Q_A R_B Q_C Q_D + Q_A Q_B = 0{,}000202 = 1 - R_S(1\ \text{year})$$

Example


Operator
Switch
Contact
Pressure
sensor
Pump
Tank
Power
Gas
Relief valve
Timer
Discharge valve

Example





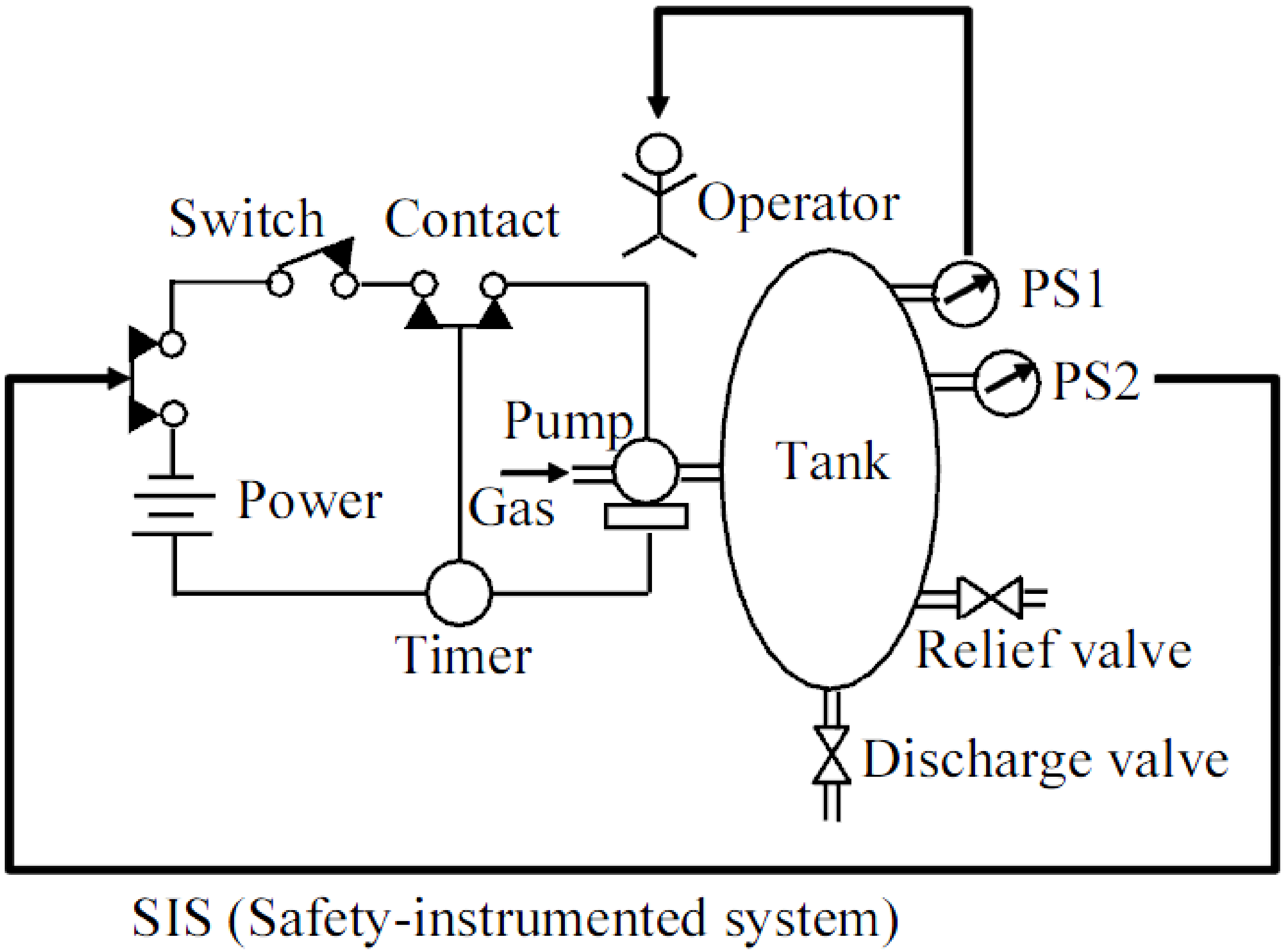
$0.2 \cdot 0.7 = 0.14$

$0.2 \cdot 0.3 \cdot 0.9 = 0.054$

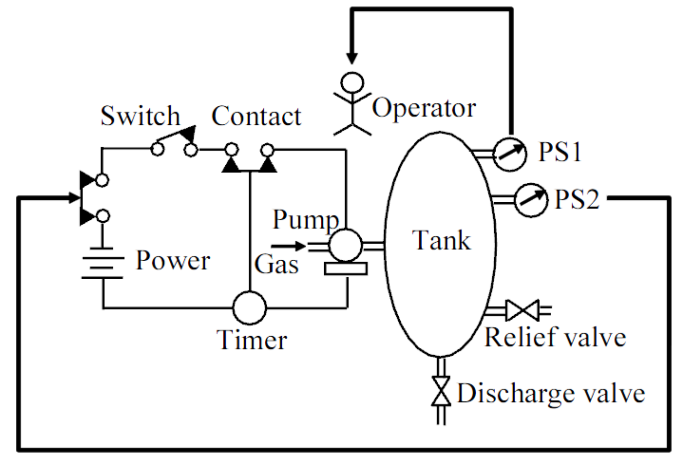
$0.2 \cdot 0.3 \cdot 0.1 = 0.006$

$$\sum = 0.2$$

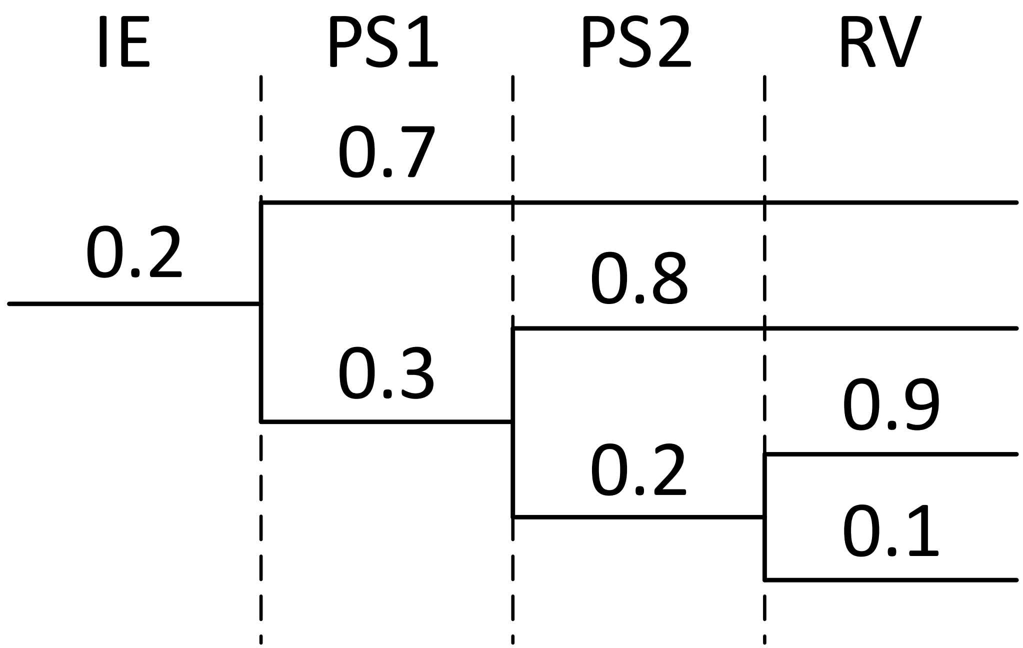
Improvement



Improvement



SIS (Safety-instrumented system)



$$0.2 \cdot 0.7 = 0.14$$

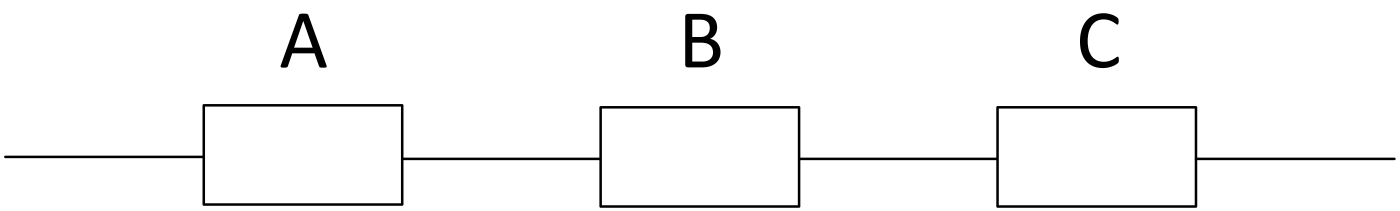
$$0.2 \cdot 0.3 \cdot 0.8 = 0.048$$

$$0.2 \cdot 0.3 \cdot 0.2 \cdot 0.9 = 0.0108$$

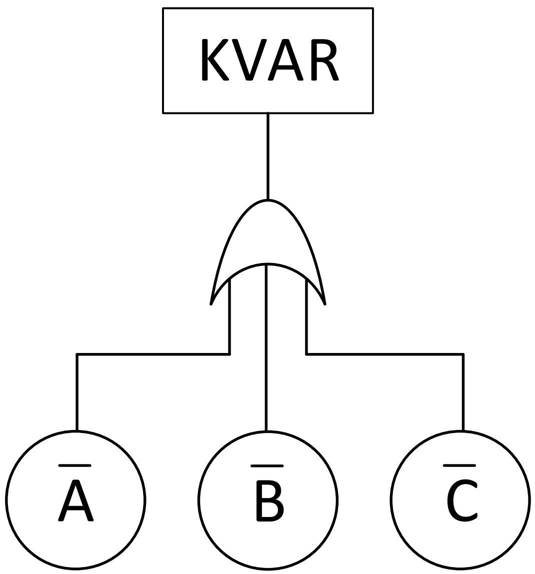
$$0.2 \cdot 0.3 \cdot 0.2 \cdot 0.1 = 0.0012$$

$$\sum = 0.2$$

Reliability of series system

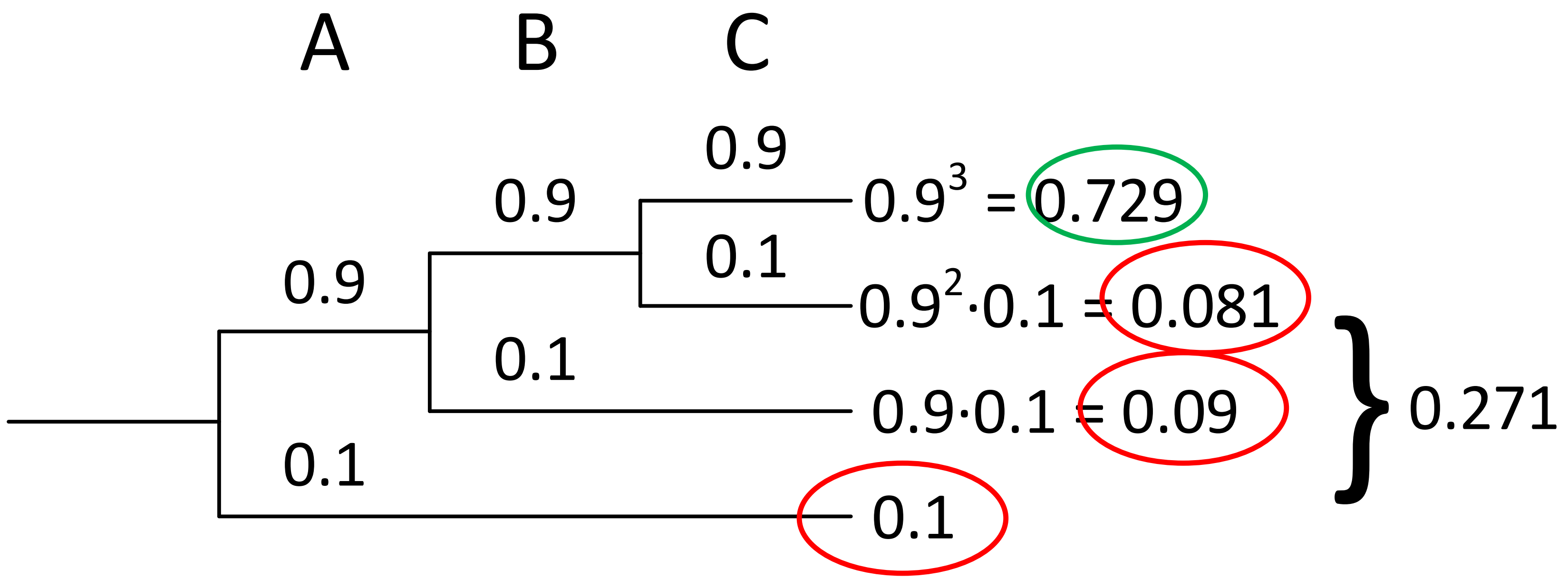


$$R(t) = P(A)P(B)P(C) = 0.9^3 = 0.729$$

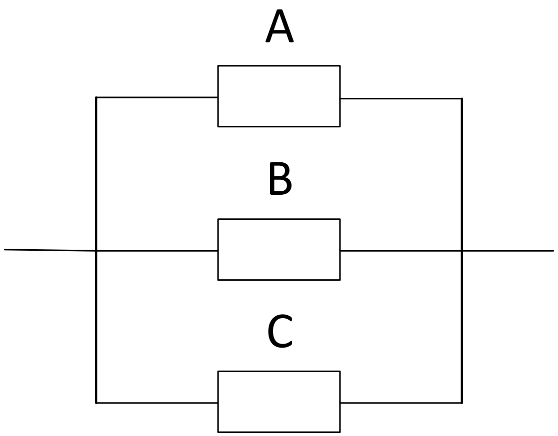


$$Q(t) = P(\overline{A}+\overline{B}+\overline{C}) = P(\overline{A}) + P(\overline{B}) + P(\overline{C}) - P(\overline{A})P(\overline{B}) -$$
$$-P(\overline{A})P(\overline{C}) - P(\overline{B})P(\overline{C}) + P(\overline{A})P(\overline{B})P(\overline{C}) =$$
$$= 3\cdot 0.1 - 3\cdot 0.1^2 + 0.1^3 = 0.271 = 1 - R(t)$$

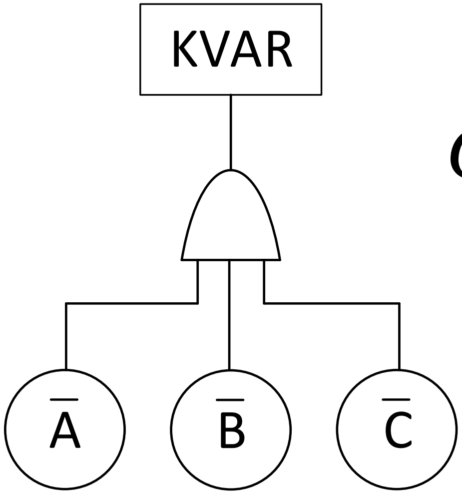
Reliability of series system



Reliability of parallel system



$$R(t) = P(A+B+C) = P(A)+P(B)+P(C)-P(A)P(B)-$$
$$-P(A)P(C)-P(B)P(C)+P(A)P(B)P(C)=$$
$$=3\cdot 0.9-3\cdot 0.9^2+0.9^3=0.999=1-Q(t)$$



$$Q(t)=P(\bar{A})P(\bar{B})P(\bar{C})=0.1^3=0.001$$

Reliability of parallel system