Hazard Analysis

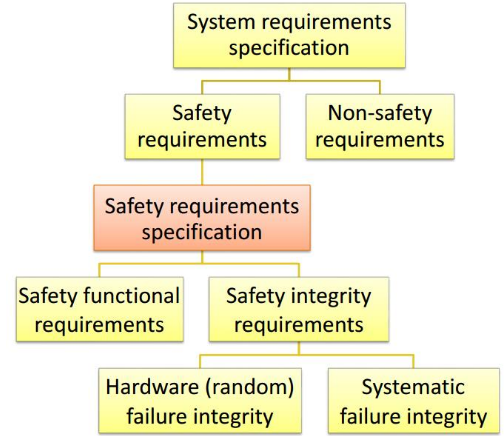
Design and Integration of Embedded Systems

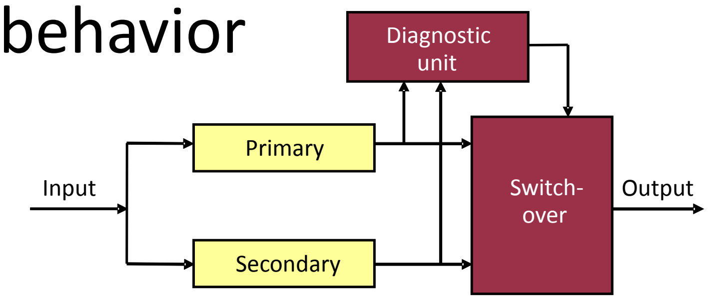
István Majzik

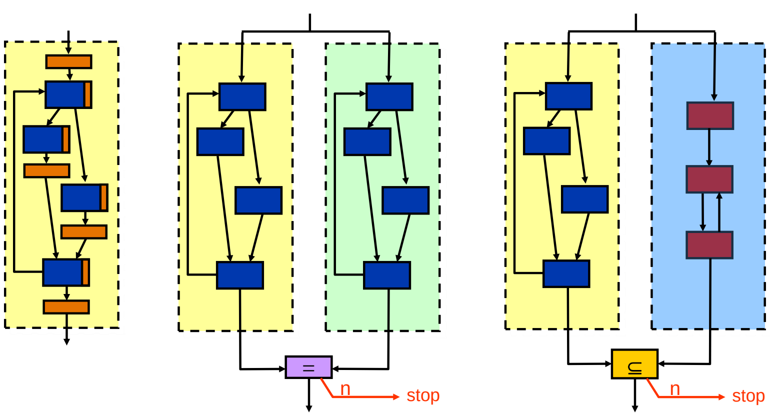
Department of Measurement and Information Systems

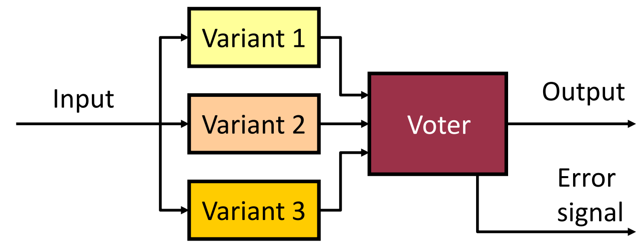
Previous topics

- Specification in safety-critical systems
  - Safety function requirements
  - Safety integrity requirements
  - Dependability requirements
- Architecture design solutions
  - Error detection for fail-stop behavior
  - Fault tolerance for fail-operational behavior







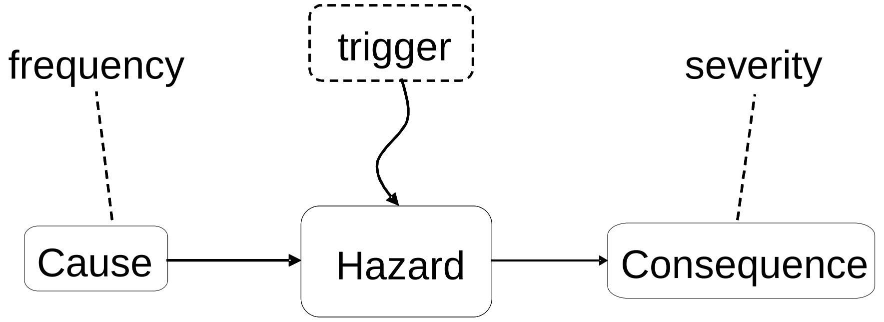


Goals of this presentation

- Focus: Evaluation of the system architecture to ...
  - Analyze the causes of potential hazards
  - Analyze the effects of component faults
- Learning objectives
  - Understand the role of architecture evaluation
  - Know the typical techniques for the analysis
  - Understand the method of risk estimation
  - Perform evaluation of a concrete architecture

Hazard analysis

- Goal: Analysis of the fault effects and the evolution of hazards (hazardous states)
  - What are the causes of a hazard?
  - What are the consequences of a component fault?
- Results:
  - Hazard catalogue
  - Categorization of hazards
    - Frequency of occurrence
    - Severity of consequences
    - → Risk matrix



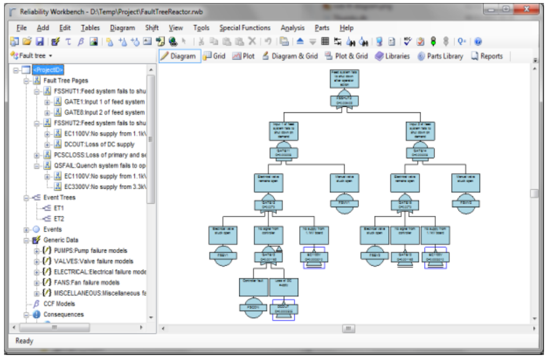
- These results form the basis for risk reduction

Categorization of the techniques

- On the basis of the development phase (tasks):
  - Design phase: Identification and analysis of hazards
  - Delivery phase: Demonstration of safety
  - Operation phase: Checking the effects of modifications
- On the basis of the analysis approach:
  - Cause-consequence view:
    - Forward (inductive): Analysis of the effects of faults/events
    - Backward (deductive): Analysis of the causes of hazards
  - System hierarchy view:
    - Bottom-up: From the components up to system level
    - Top-down: From the system level down to the components
- Systematic techniques are needed

Overview: Analysis techniques

- Informal analysis
  - Checklists
- Systematic analysis of hazard causes and fault effects with risk estimation:
  - Fault tree analysis (FTA)
  - Event tree analysis (ETA)
  - Cause-consequence analysis
  - Failure modes and effects analysis (FMEA)



Checklists

Checklists

- Basic approach
  - Collection of experiences about typical faults and hazards
  - Used as guidelines and as ”rule of thumb” to avoid hazards
- Advantages
  - Known sources of hazards are included
  - Well-proven ideas and solutions can be applied
- Disadvantages
  - Completeness is hard to achieve (checklist is incomplete)
  - False confidence about safety
  - Applicability in different domains than the original domain of the checklist is questionable

Example: Checklist to examine a design

- Completeness
  - Complete list of functions, components, tools
- Consistency
  - Internal and external consistency (e.g., with standards)
  - Traceability of requirements to components
- Realizability
  - Resources are sufficient
  - Usability is satisfied
  - Maintainability is considered
  - Risks handled: cost, technical, environmental
- Testability
  - Properties are specific, measurable, unambiguous
  - Quantitative statements (if possible)

Motivations to check the specification

- Experience: Hazards are often caused by incomplete or inconsistent specification
  - Example: Statistics of failures detected during the software testing of the Voyager and Galileo spacecraft

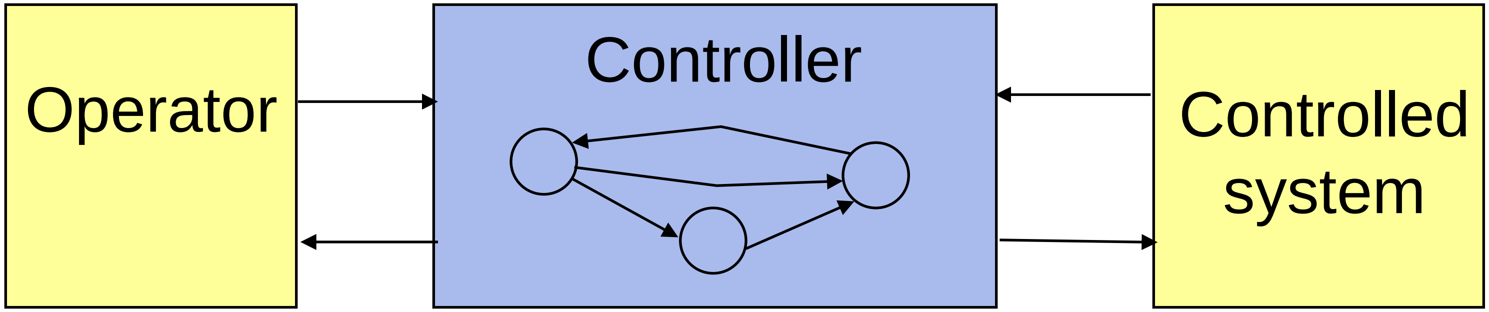
    78% (149/192) specification related failures, from which

    - 23% stuck in dangerous state (without exit)
    - 16% lack of timing constraints
    - 12% lack of reaction to input event
    - 10% lack of checking input values
- Potential solutions to avoid such problems
  - Using a strict specification language
  - Applying well-proven design patterns
  - Checking the specification

Example: Checklist for state machine design

Completeness and consistency:

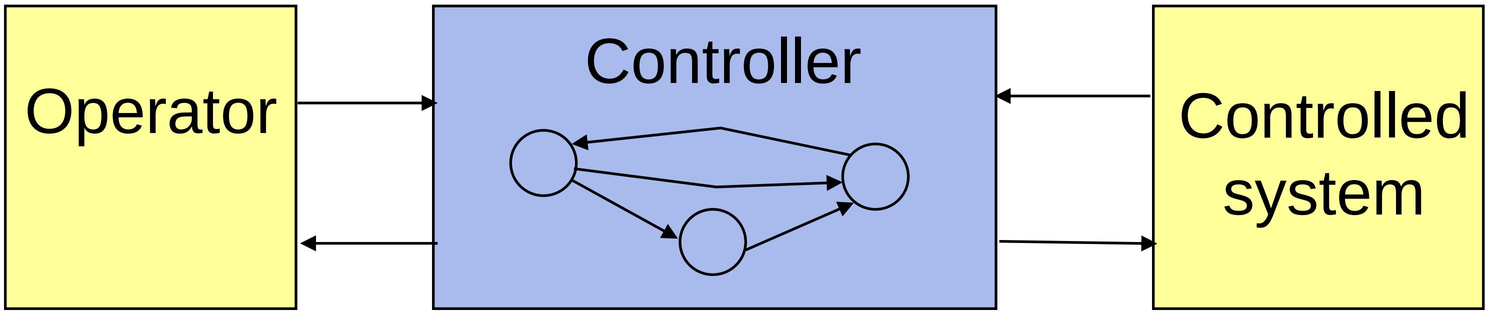
- State definition
- Inputs (trigger events)
- Outputs
- Relation of inputs (triggers) and outputs
- State transitions
- Human-machine interface



Example: Checklist for state machine design

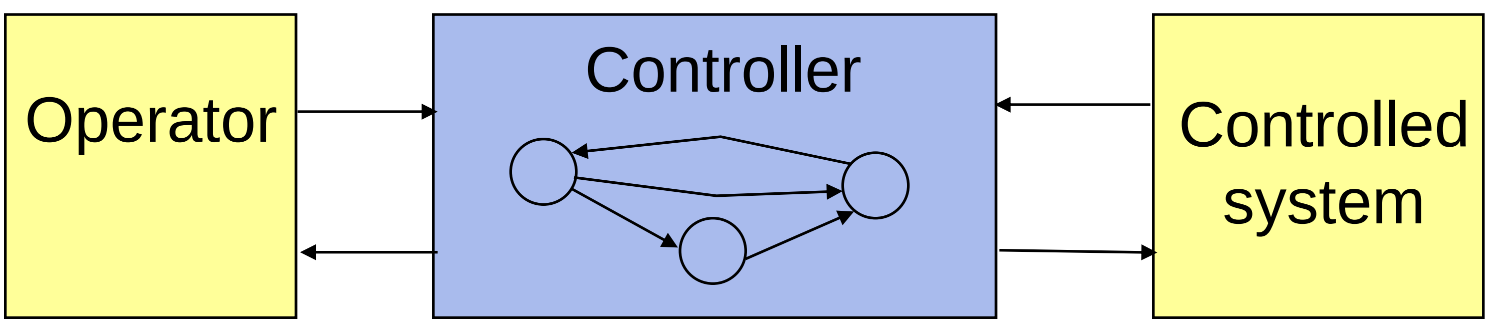
- State definition
- Inputs /
- Outpu
- Relatio
- State transitions
- Human-machine interface

- Safe initial state
- Actualization of the internal model: if input events are missing then timeout and transition to “invalid” state is required; output is not allowed in this state



Example: Checklist for state machine design

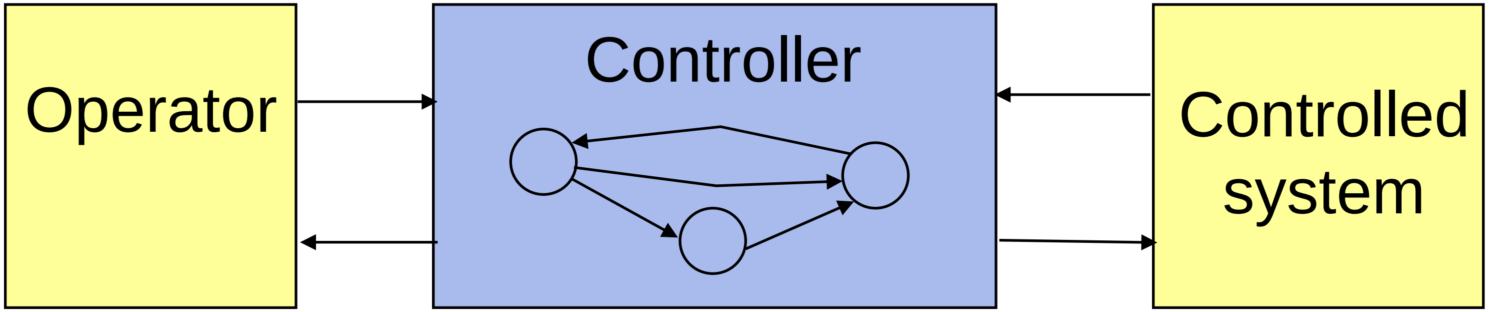
- State definition
- Inputs (trigger events)
  - Reaction to each potential input event
  - Deterministic reactions
  - Input checking (value, timing)
  - Handling of invalid inputs
  - Limited rate of interrupts (to avoid overload)
- Outpu
- Relati
- State t
- Huma



Example: Checklist for state machine design

- State definition
- Inputs (trigger events)
- Outputs
- Relatio
- State t
- Huma

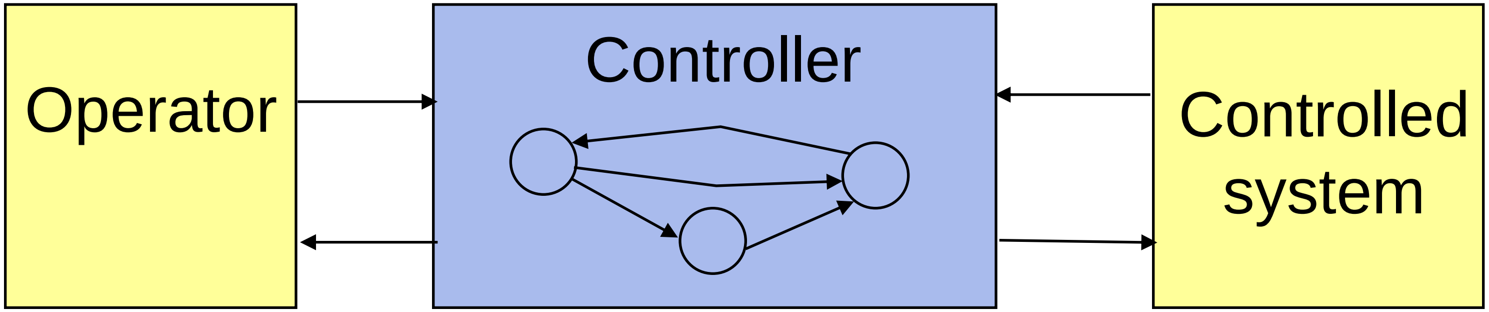
- Acceptance checking on the output
- There are no unused outputs
- Compliance with the limitations of the environment



Example: Checklist for state machine design

- State defi
- Inputs (tri
- Outputs
- Relation of inputs (triggers) and outputs
- State transitions
- Human-machine interface

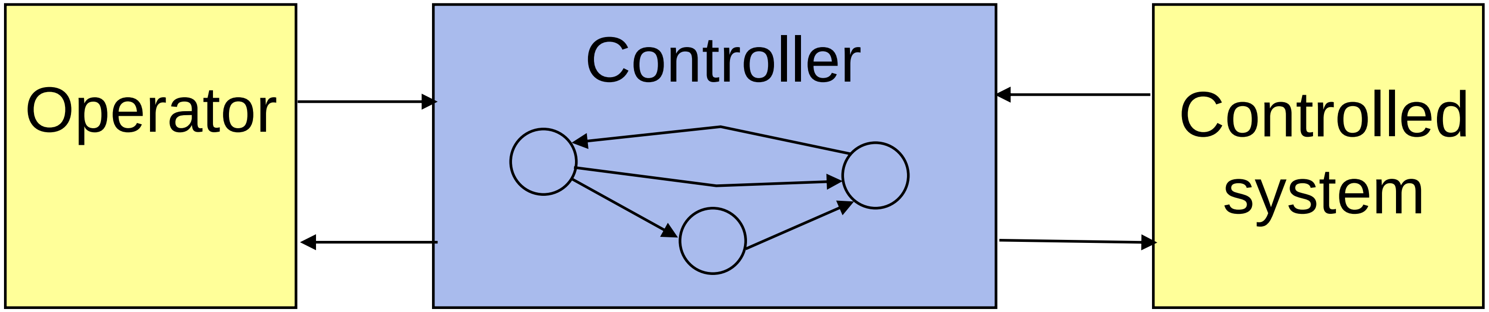
- The effects of outputs are checked through processing the induced inputs
- Stability of the control loop is guaranteed



Example: Checklist for state machine design

- Each state is reachable (static reachability)
- Transitions are reversible (reverse path exists)
- Multiple transitions from dangerous state to safe state
- Confirmed transitions from safe state to dangerous state

- Stat
- Inp
- Out
- Rel
- State transitions
- Human-machine interface

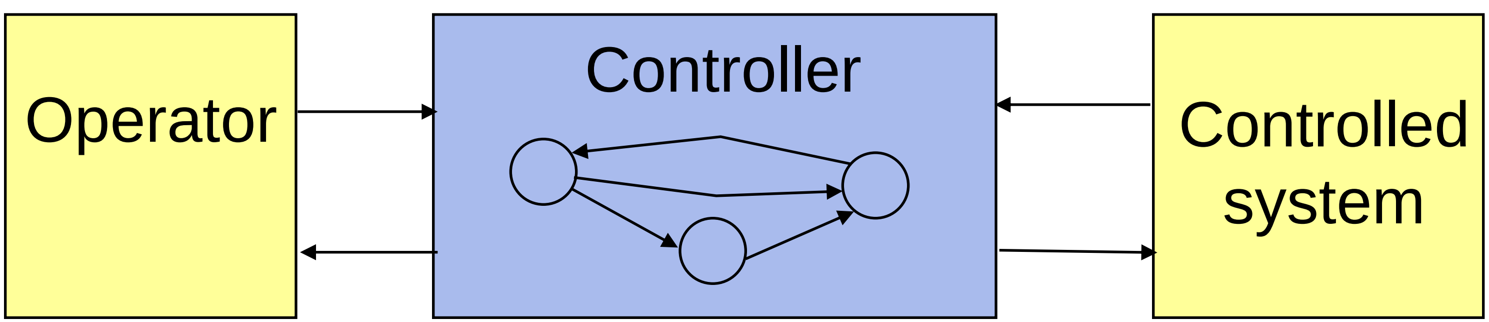


Example: Checklist for state machine design

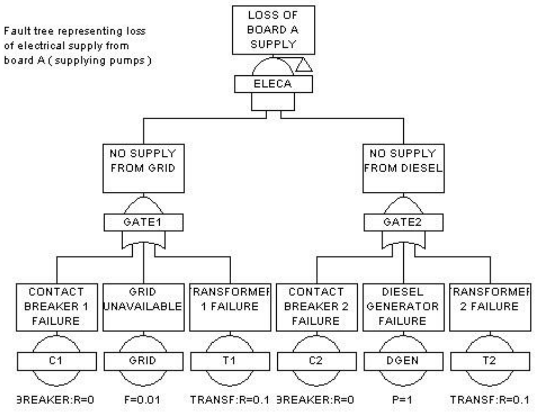
- State definition
- Inpu
- Out
- Rela
- State trans ons
- Human-machine interface

Well-specified outputs towards the operator:

- Ordering of events (with priorities)
- Limited frequency of updates
- Obsolete outputs are removed (timeliness is considered)



Fault tree analysis



Fault tree analysis

Analysis of the causes of system level hazards

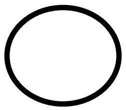
- Top-down analysis
- Identifying the component level combinations of faults/events that may lead to system level hazard

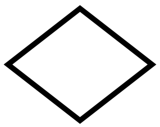
Construction of the fault tree

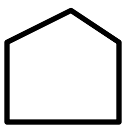
1. Identification of the foreseen system level hazard: on the basis of environment risks, standards, etc.
2. Identification of intermediate events (pseudo-events): Boolean (AND, OR) combinations of lower level events that may cause upper level events
3. Identification of primary (basic) events: no further refinement is needed/possible

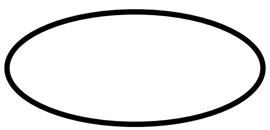
Set of elements in a fault tree

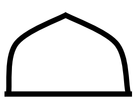

Top level or intermediate event

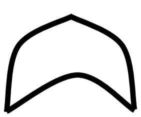

Primary (basic) event


Event without further analysis

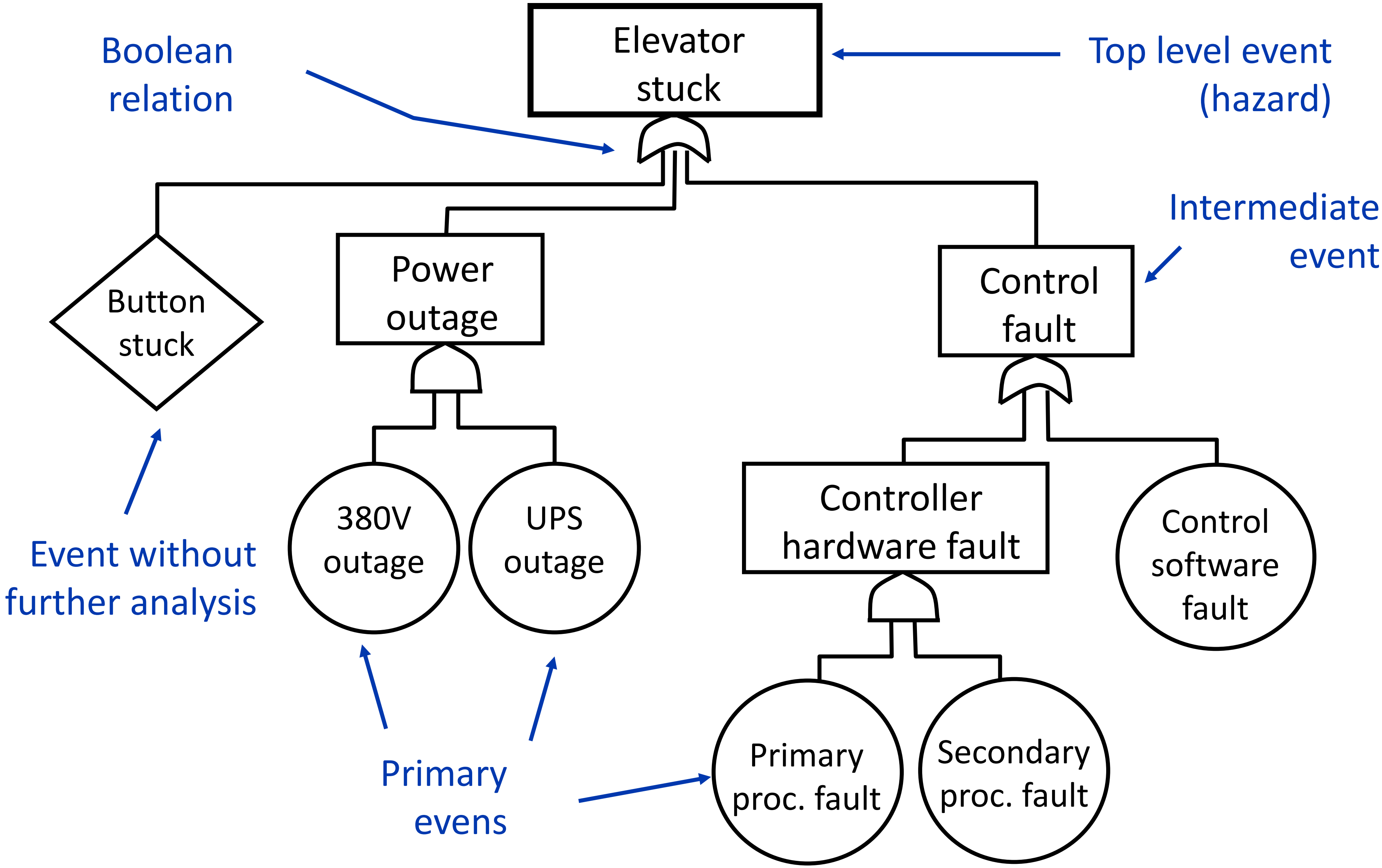

Normal event (i.e., not a fault)


Conditional event

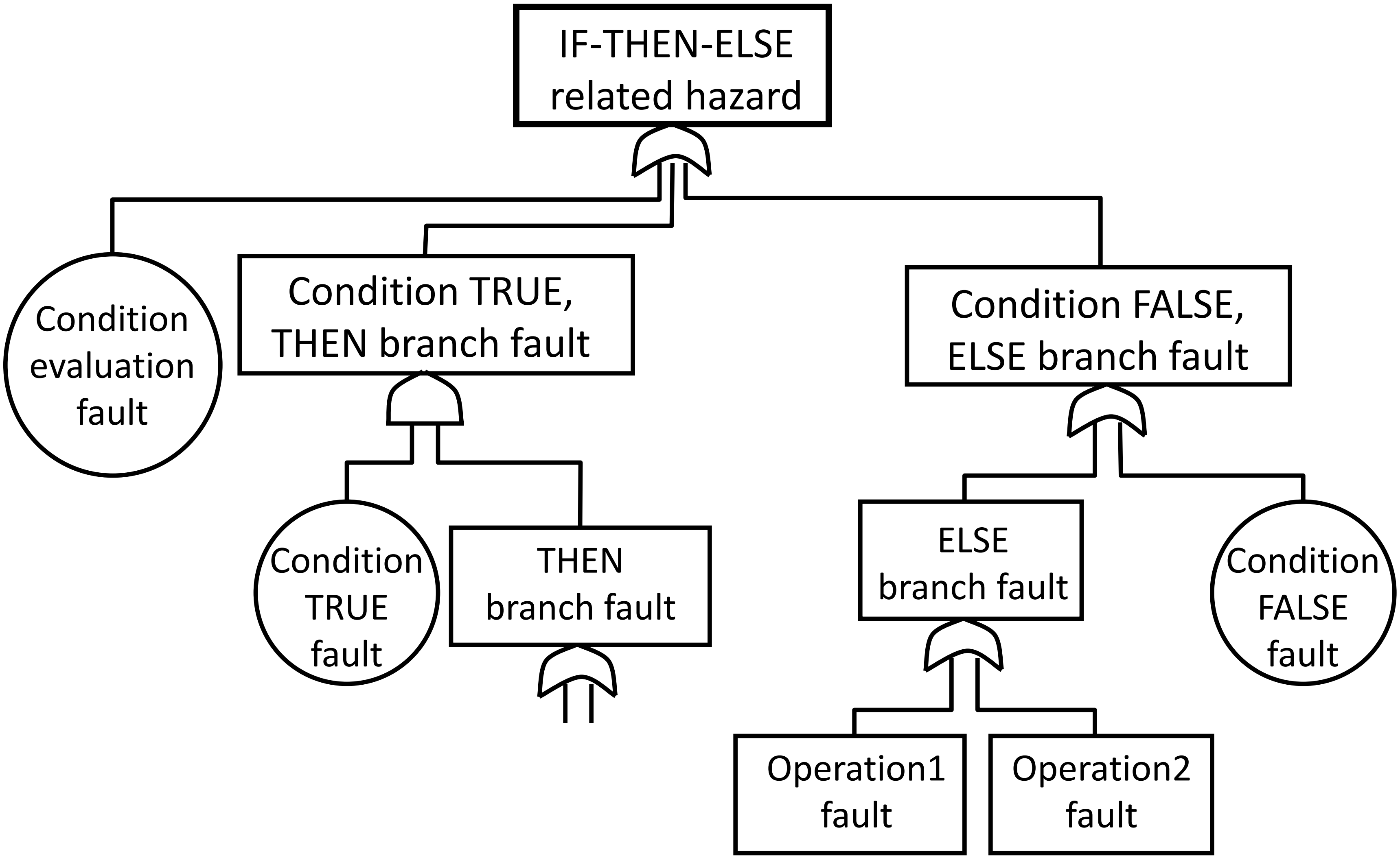

AND combination of events


OR combination of events

Fault tree example: Elevator



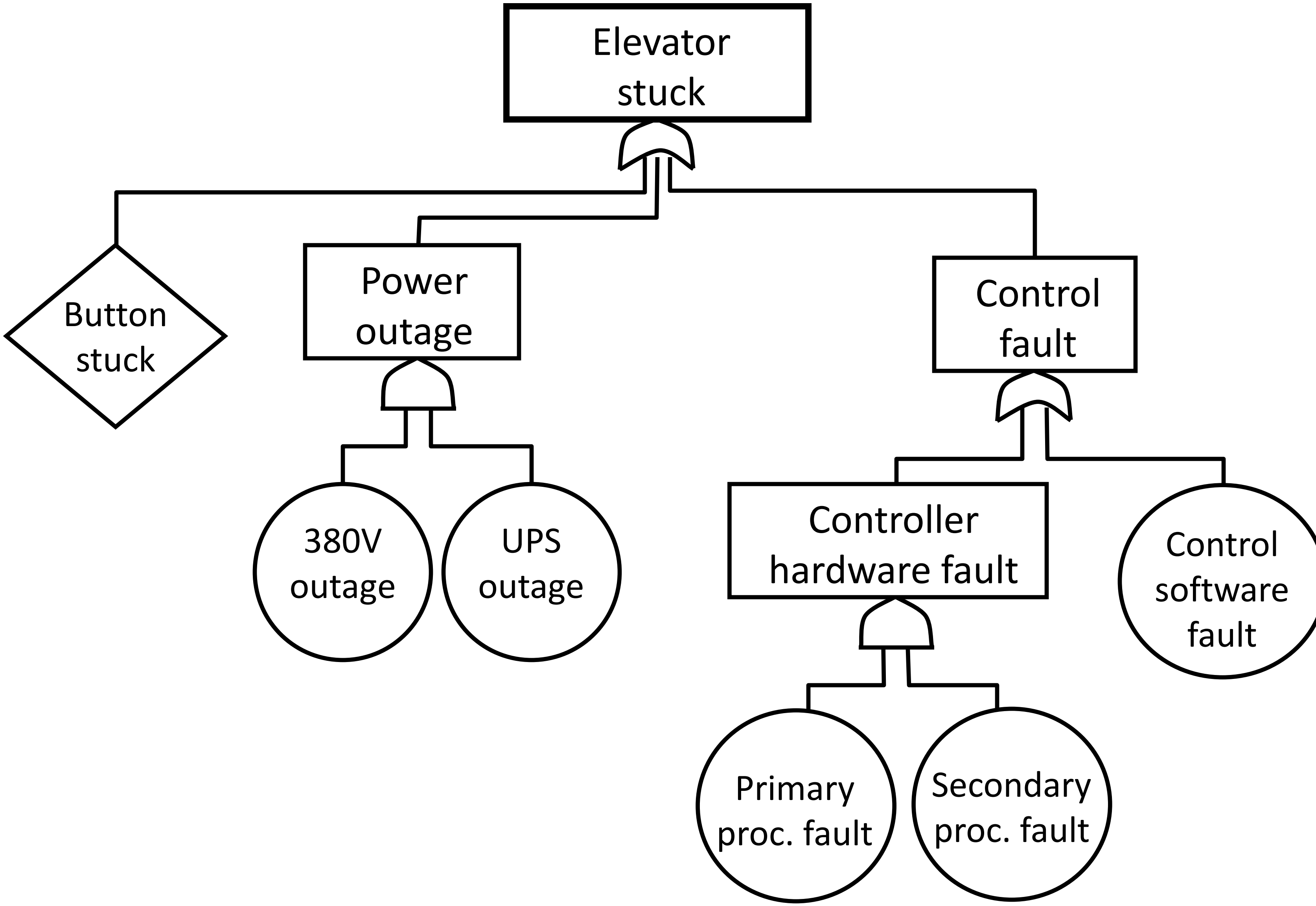
Fault tree example: Software analysis



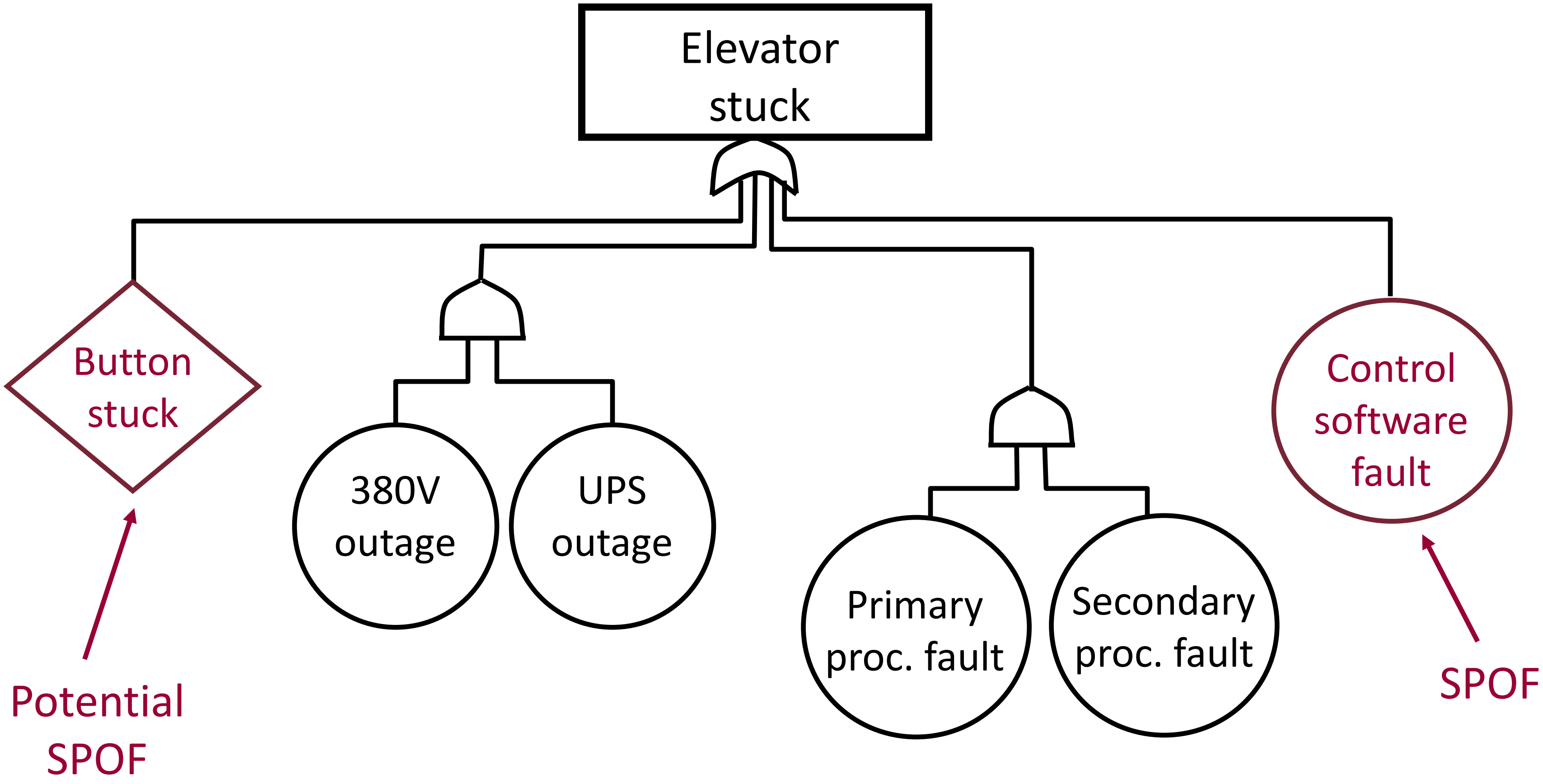
Qualitative analysis of the fault tree

- Fault tree reduction: Resolving intermediate events/pseudo-events using primary events
  → disjunctive normal form (OR on the top of the tree)
- Cut of the fault tree:
  AND combination of primary events
- Minimal cut set: No further reduction is possible
  - There is no cut that is a subset of another
- Outputs of the analysis of the reduced fault tree:
  - Single point of failure (SPOF)
  - Events that appear in several cuts

Original fault tree of the elevator example



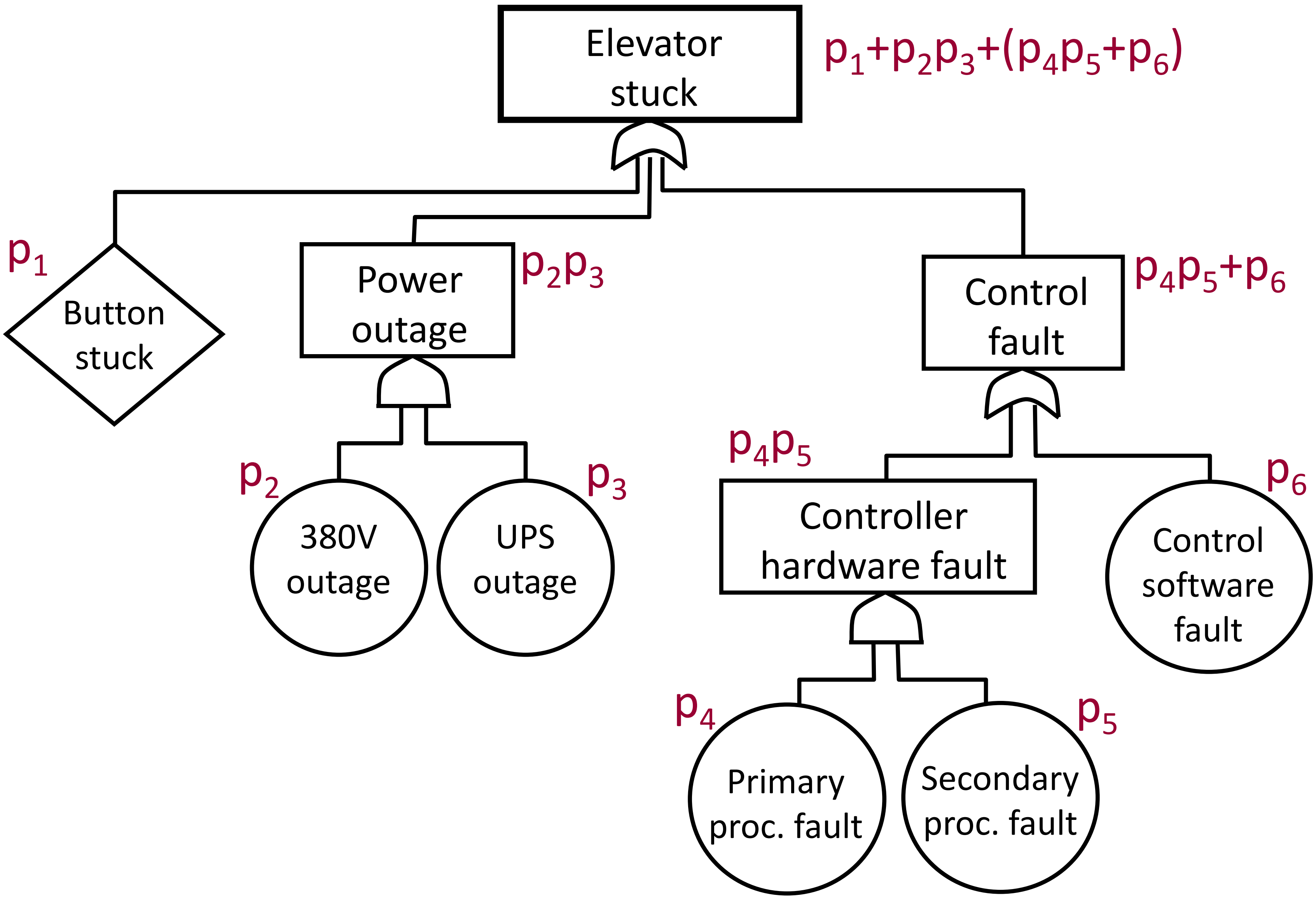
Reduced fault tree of the elevator example



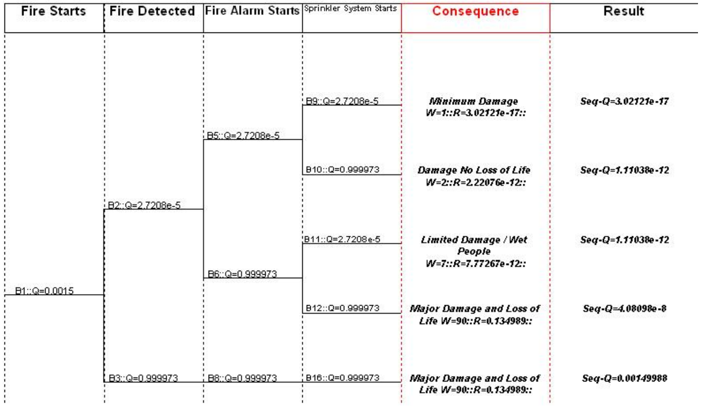
Quantitative analysis of the fault tree

- Basis: Probabilities of the primary events
  - Component level data, experience, or estimation
- Result: Probability of the system level hazard
  - Computing probability on the basis of the probabilities of the primary events, depending on their combinations
  - AND gate: Product (if the events are independent)
    - Exact calculation: P{A and B} = P{A} · P{B|A}
  - OR gate: Sum (worst case estimation)
    - Exact: P{A or B} = P{A} + P{B} - P{A and B} <= P{A} + P{B}
  - Probability as time function can also be used in computations
- Typical problems:
  - Correlated faults (not independent)
  - Representation of event sequences

Fault tree of the elevator with probabilities



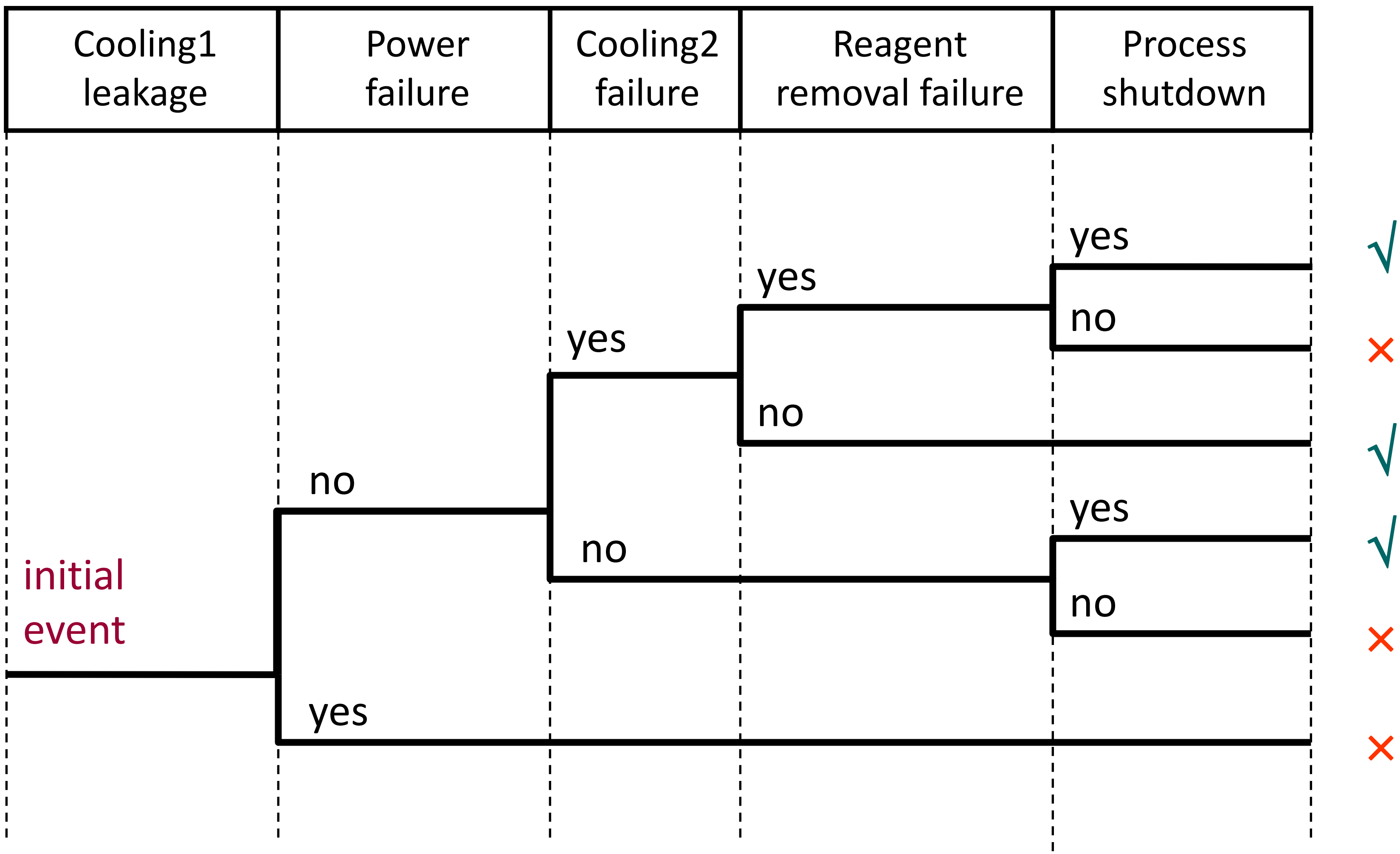
Event tree analysis



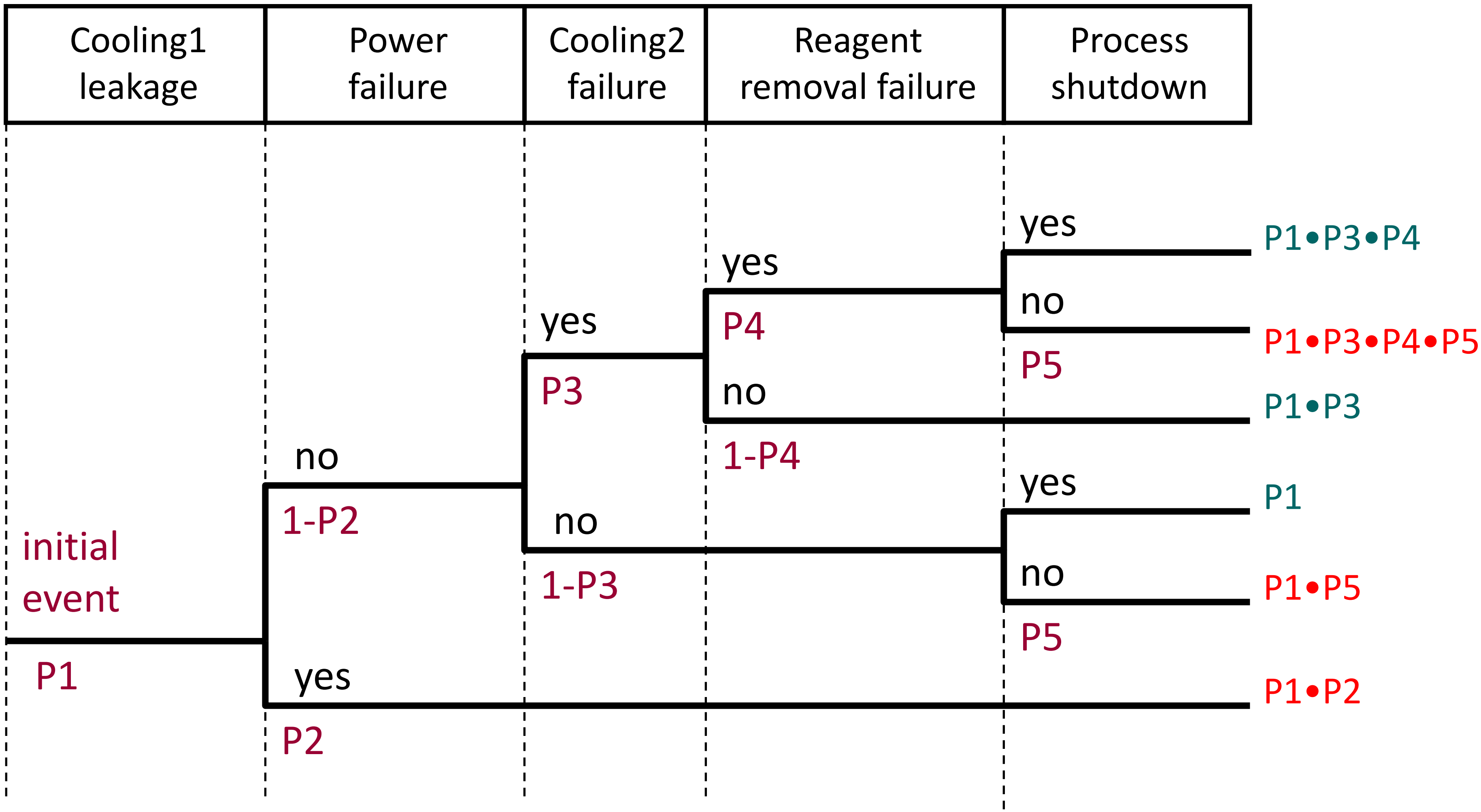
Event tree analysis

- Forward (inductive) analysis:
  Investigates the effects of an initial event (trigger)
  - Initial event: Component level fault/event
  - Related events: Faults/events of other components
  - Ordering: Causality, timing
  - Branches: Depend on the occurrence of events
- Investigation of hazard occurrence „scenarios”
  - Path probabilities (on the basis of branch probabilities)
- Advantages: Investigation of event sequences
  - Example: Checking protection systems (protection levels)
- Limits: Complexity, multiplicity of events

Event tree example: Reactor cooling



Event tree example: Reactor cooling

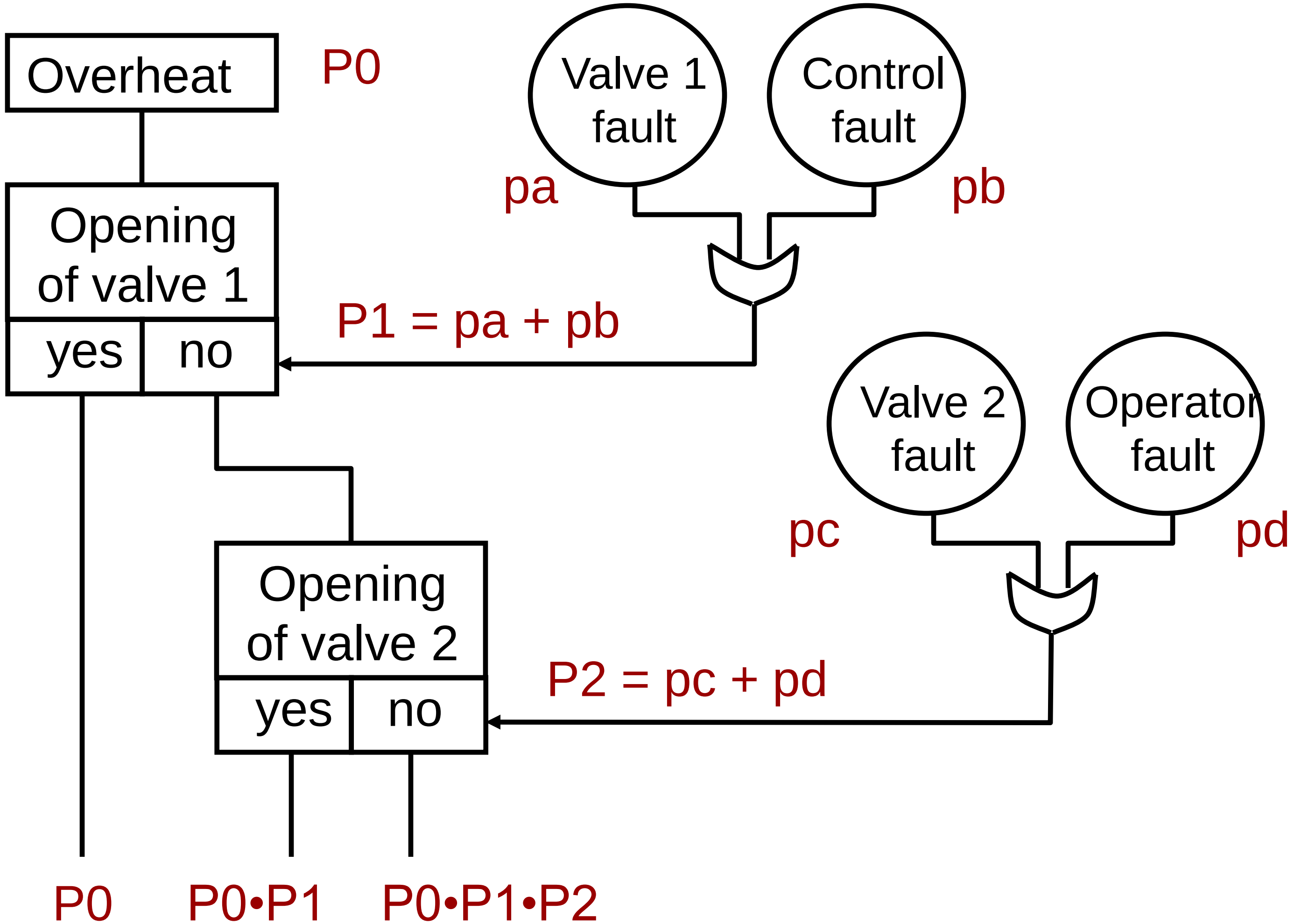


Cause-consequence analysis

4. Cause-consequence analysis

- Integration of an event tree with fault trees
  - Event tree: Event sequences (scenarios)
  - Attached fault trees: Analysis of the causes of the specific occurrence of an event in the event tree
- Advantages:
  - Event sequences (forward analysis) and analysis of causal relations (backward analysis) together
- Drawbacks:
  - Separate diagram for each initial event
  - Complexity of diagrams

Cause-consequence analysis example



Failure modes and effects analysis

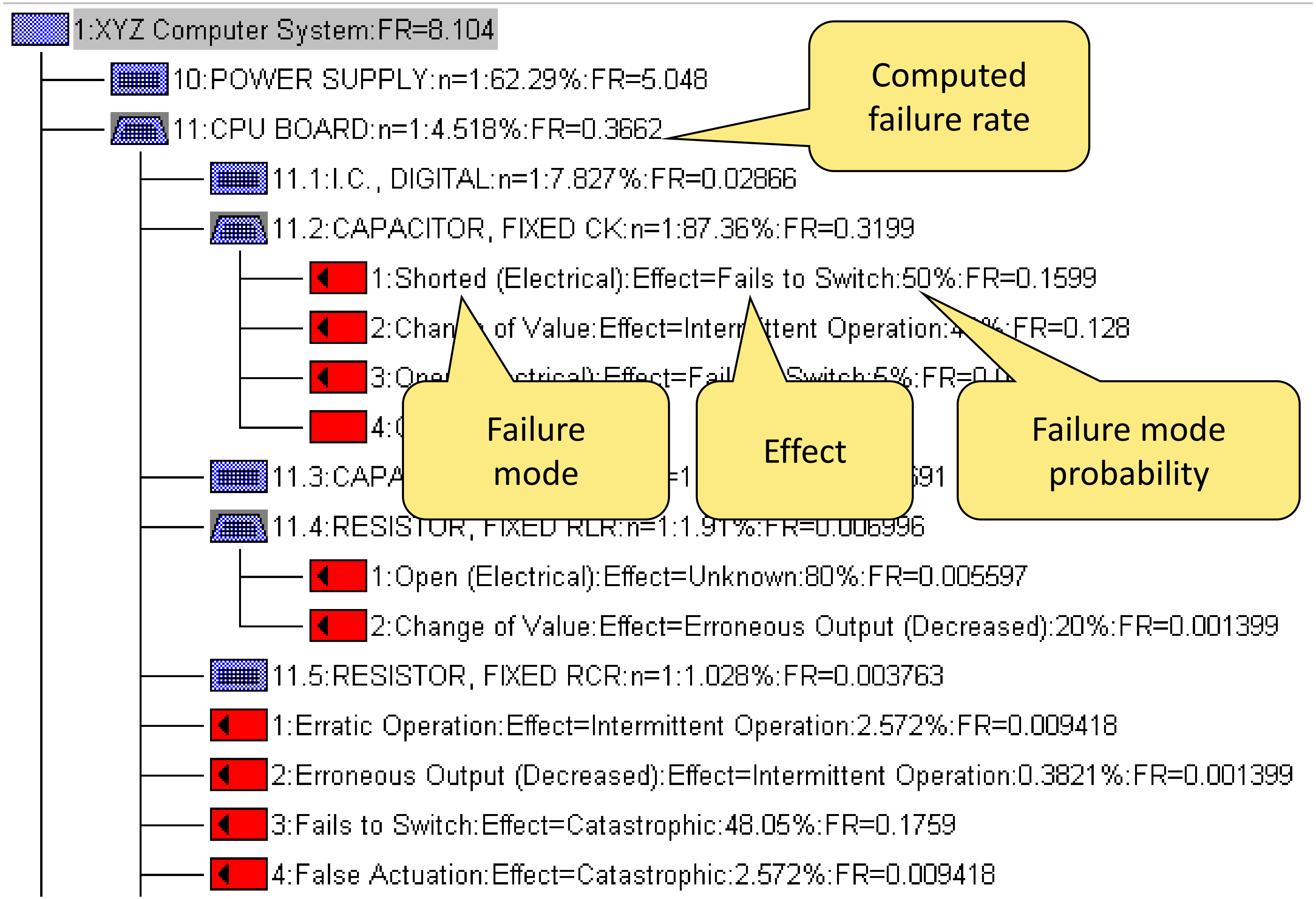
Item and (% chance of failure)	Failure mode		Effect of failure mode		Criticality of effect by severity type x 10^6			
	Description	Chance	Description	Chance	V.Hi	High	Med	Low
Main stack (0.2%)	Corruption	15%	Data loss	24%	180			
			System crash	66%		495		
	Overflow	60%	Shutdown	90%			2700	
			System crash	10%		300		
	Underflow	25%	Warning	98%				1225
Total					180	795	2700	1225

5. Failure modes and effects analysis (FMEA)

- Systematic investigation of component failure modes and their effects
- Advantages:
  - Known faults of components are included
  - Criticalities of effects can also be estimated (FMECA)

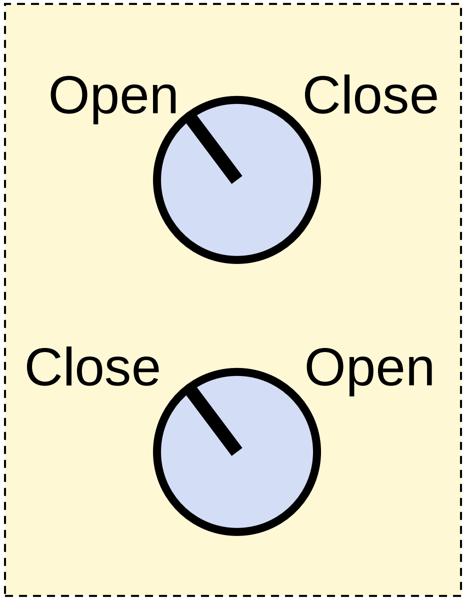
Component	Failure mode	Ratio	Effect
D1 diode	open circuit short circuit	65% 35%	- over-heating - damaged product
...	...	...	...

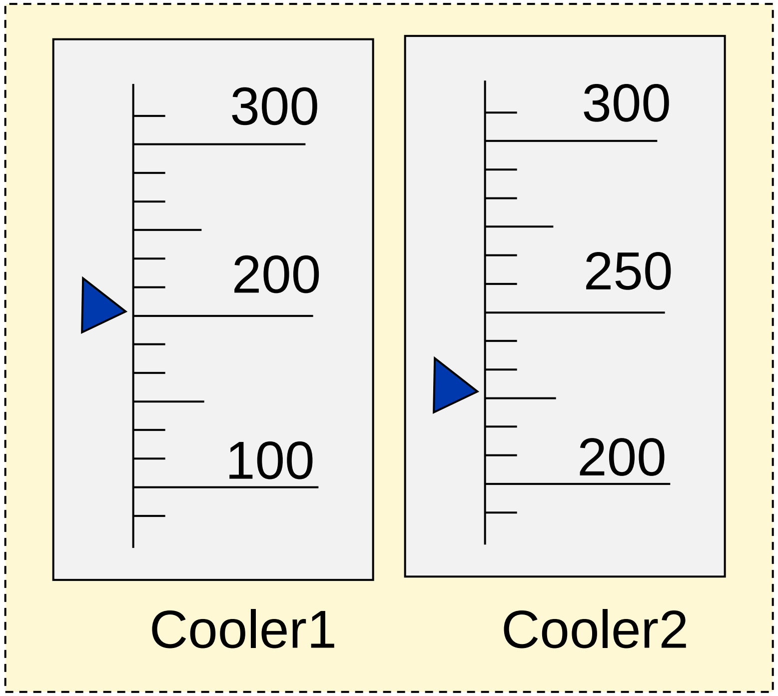
Example: Analysis of a computer system



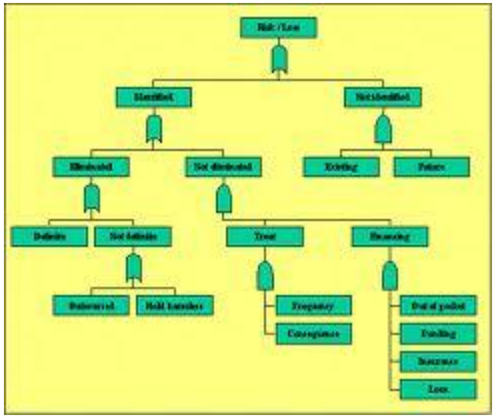
Analysis of operator faults

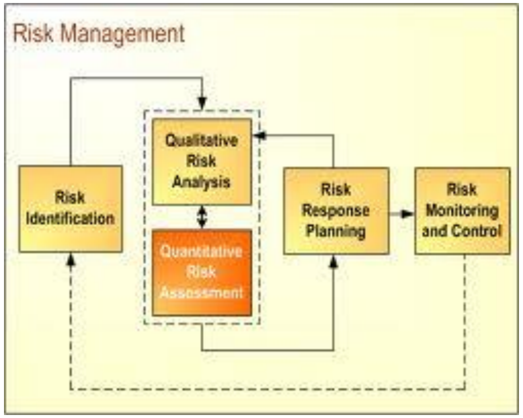
- Qualitative techniques:
  - Operation – hazards – effects – causes – mitigations
  - Analysis of physical and mental demands
  - Fault causes ← human-machine interface problems





Risk reduction techniques





Catalogue of hazards

- Categorization of hazards on the basis of hazard analysis (e.g., MIL-STD-822b, NASA):
  - Frequency of occurrence of hazards: Frequent, probable, occasional, remote, improbable, incredible
  - Severity level of hazard consequences: Catastrophic, critical, marginal, insignificant

  → Identification of risks
- Output of the categorization:
  - Risk matrix
  - Protection level: Identifies the risks to be handled

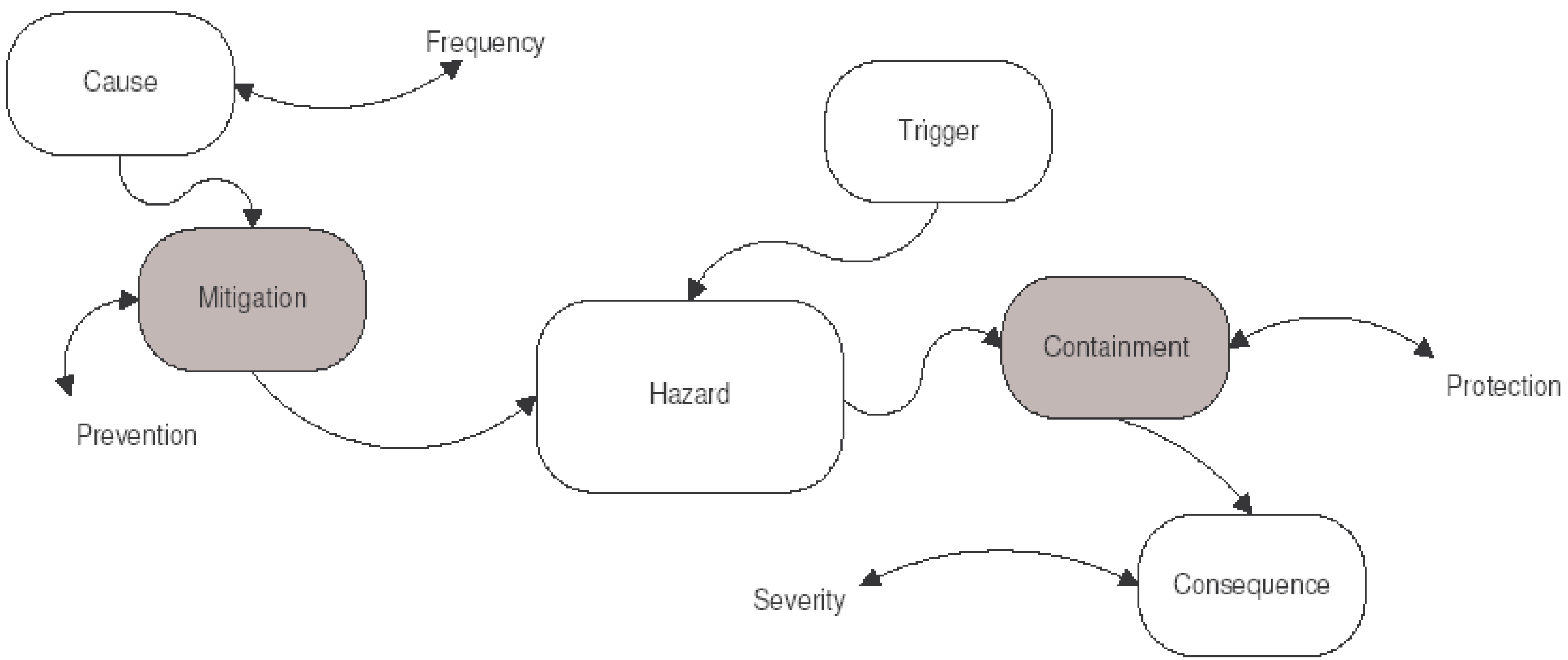
Example: Risk matrix (railway control systems)

	Frequency of Occurrence of a Hazardous Event	RISK LEVELS			
Daily to monthly	**FREQUENT (FRE)**	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)	Intolerable (INT)
Monthly to yearly	**PROBABLE (PRO)**	Tolerable (TOL)	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)
Between once a year and once per 10 years	**OCCASIONAL (OCC)**	Tolerable (TOL)	Undesirable (UND)	Undesirable (UND)	Intolerable (INT)
Between once per 10 years and once per 100 years	**REMOTE (REM)**	Negligible (NEG)	Tolerable (TOL)	Undesirable (UND)	Undesirable (UND)
Less than once per 100 years	**IMPROBABLE (IMP)**	Negligible (NEG)	Negligible (NEG)	Tolerable (TOL)	Tolerable (TOL)
	INCREDIBLE (INC)	Negligible (NEG)	Negligible (NEG)	Negligible (NEG)	Negligible (NEG)
		INSIGNIFICANT (INS)	**MARGINAL (MAR)**	**CRITICAL (CRI)**	**CATASTROPHIC (CAT)**
		Severity Levels of Hazard Consequence			

Basic idea for risk reduction

Intervening into the evolution of hazard consequences:

- Mitigation or prevention of causes
- Containment or protection of consequences



Summary

- Hazard analysis
  - Checklists
  - Fault tree analysis
  - Event tree analysis
  - Cause-consequence analysis
  - Failure modes and effects analysis (FMEA)
- Risk matrix
  - Frequency of hazard occurrence
  - Severity level of hazard consequences
  - Basic idea for risk reduction