

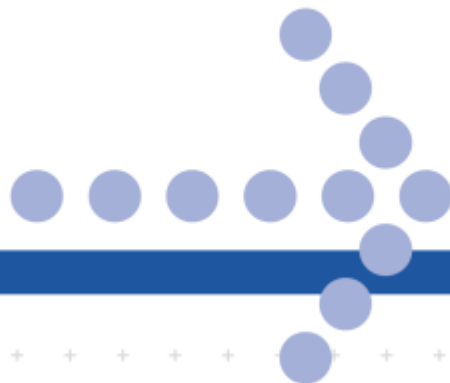
Hands-On System Safety Basics, Focused on FHA





Content

- 1) *What is Safety?***
- 2) *Safety Process***
- 3) *Basic Definitions***
- 4) *Safety Requirements***
- 5) *Methods/Techniques***
- 6) *Safety Case***
- 7) *Case Study***



What Is Safety?





Questions

- 1) What is System Safety all about?***
- 2) Why is System Safety necessary?***
- 3) What do we need for System Safety?***



Question I

What is System Safety all about?



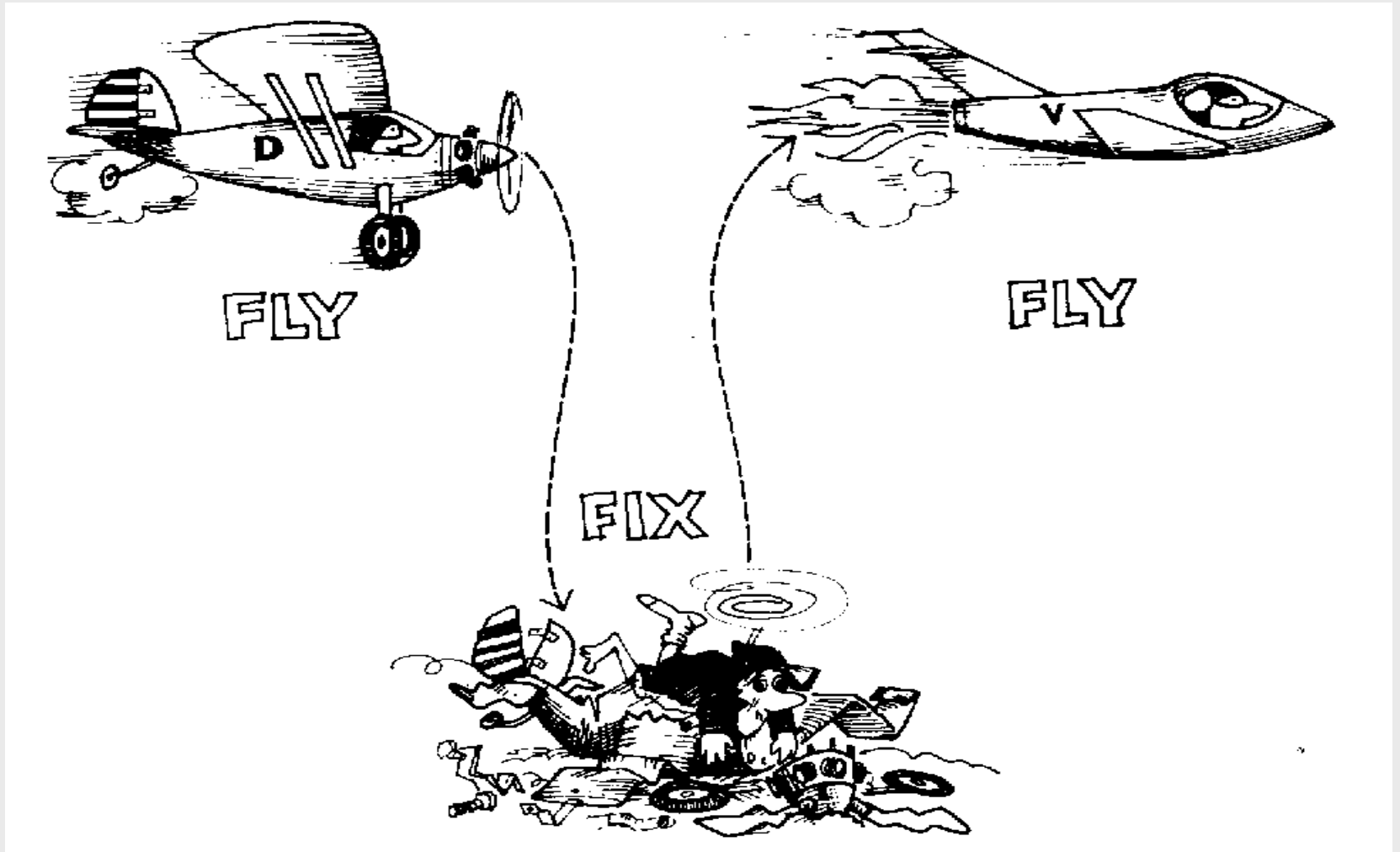
Objectives

- Minimize risk of accidents, before they happen first
- With reasonable costs
- Systematic approach

- No approach like this...



Fly – Crash – Fix - Fly





Benefits

→ Saving of lives ...

... and huge amounts of money



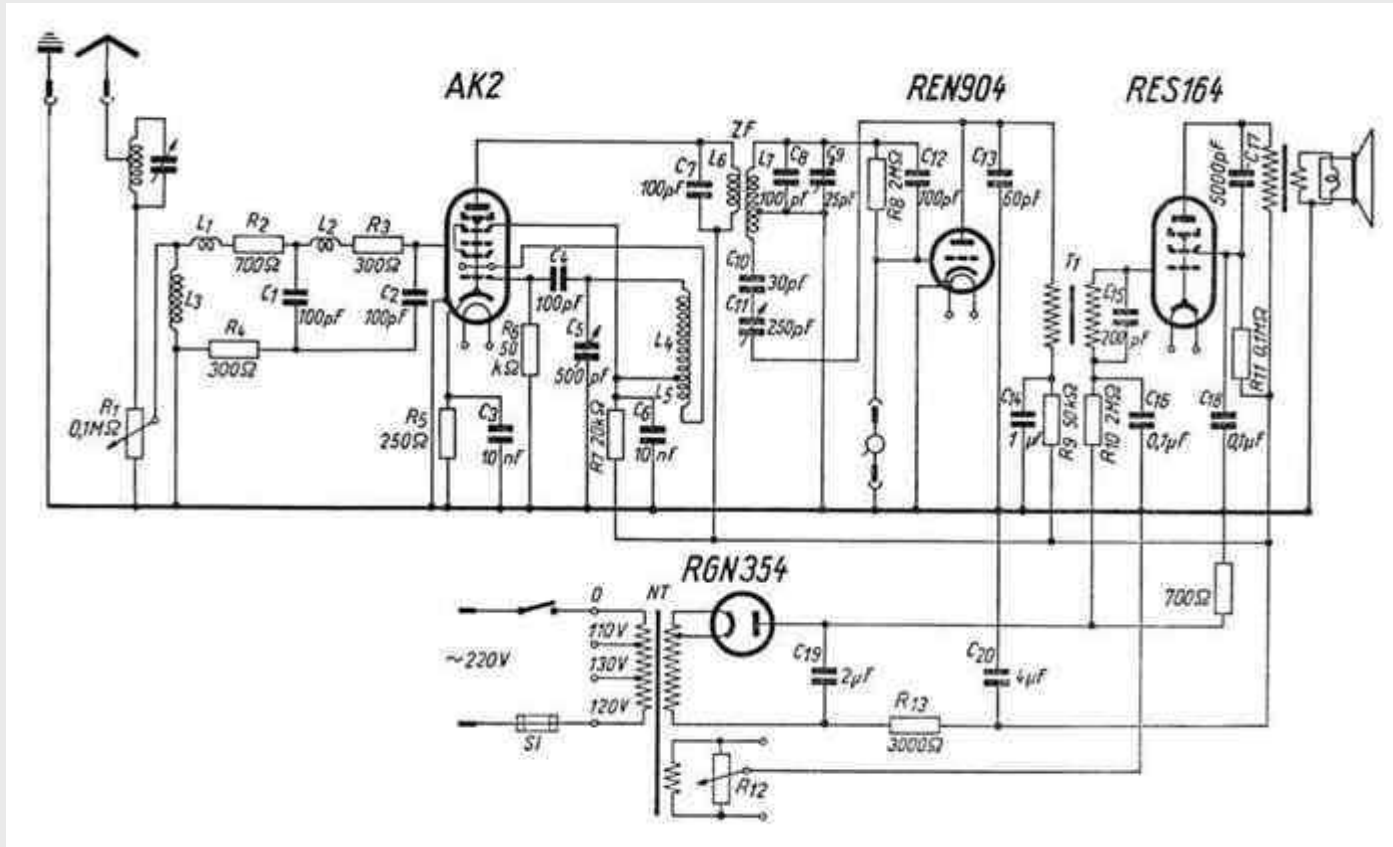
Question II

Why is System Safety necessary?



Reasons

→ Systems used to be simple ...





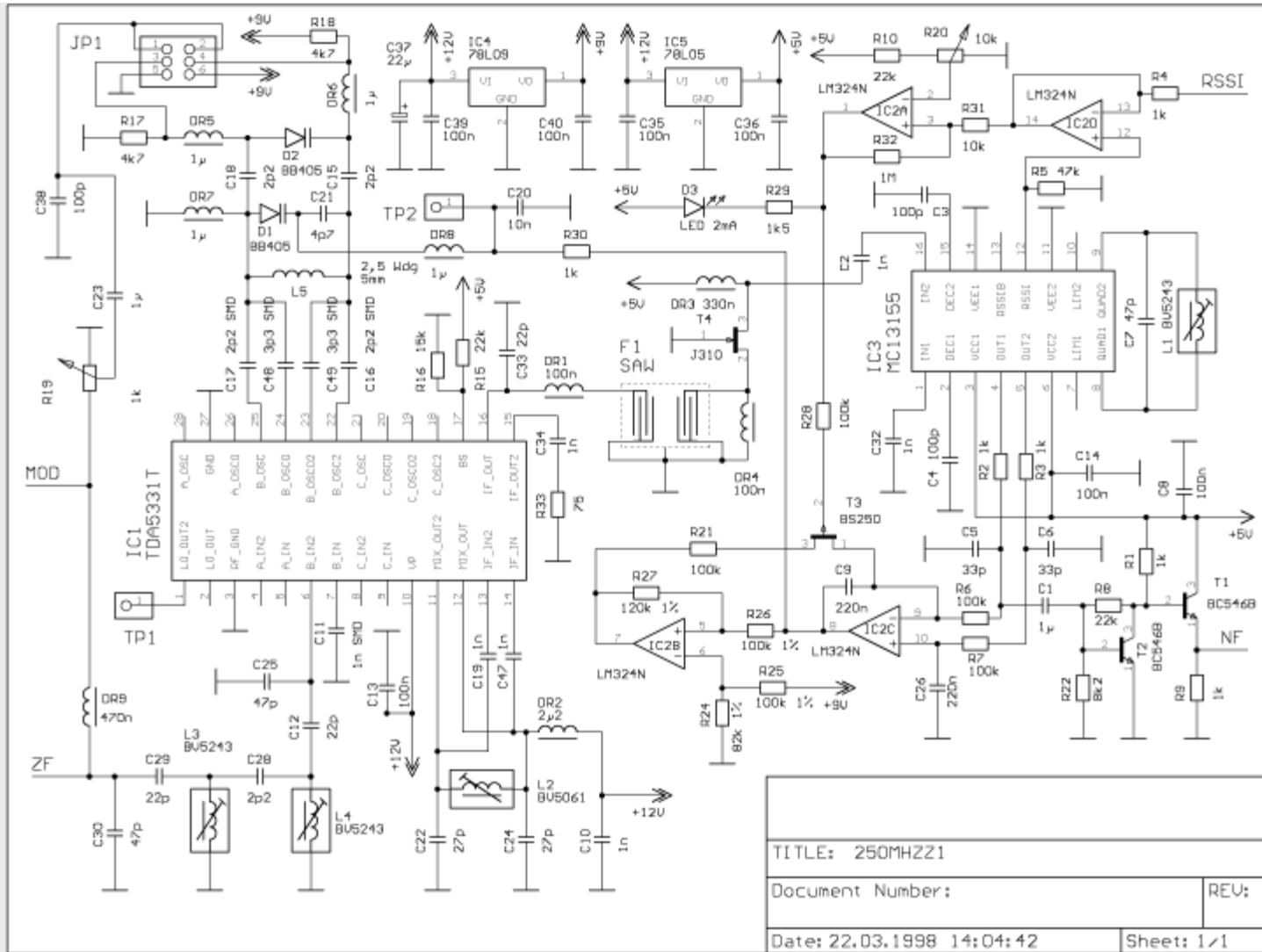
Reasons (2)

→ A single person could understand them completely

... but they ain't no more!

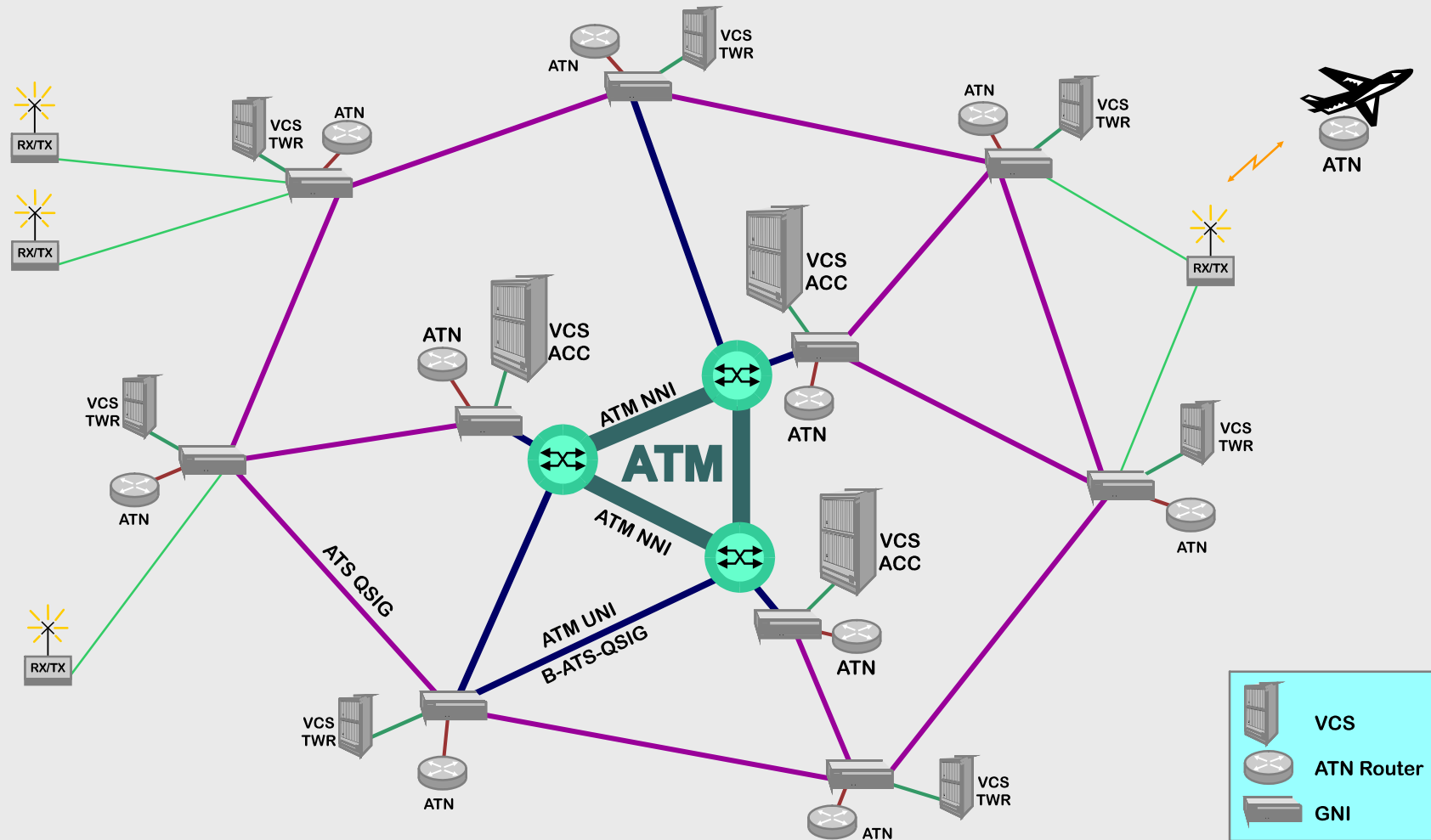


Exampel: Tranceiver





Systems of Systems





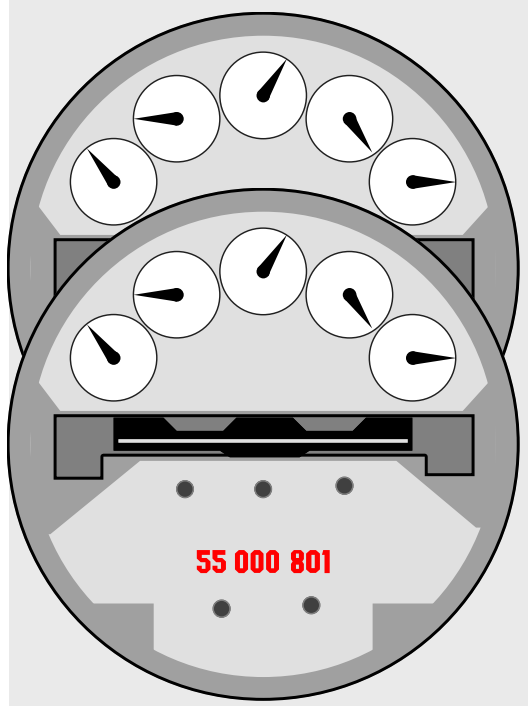
Systematic Approach Necessary!

- Therefore a systematic approach is necessary
 - to ensure completeness and avoid omissions

- Preferred method for demonstrating safety of a system is a “safety case”

... Different ways to meet Safety Objectives

Equipment Backup



Procedure Backup





Reliability vs. Safety

→ Fully duplicated...



...does not always make sense...!



Question III

What do we need for System Safety?



What Do We Need?

- **Safety Policy: Commitment** from the very top about
 - the importance of safety
 - the responsibility of all employees

- **Safety Culture**
 - awareness of all

- **Safety Management**
 - Organisation
 - Trainings
 - ...

- **Safety Engineering**
 - Hands on System Safety Work in projects
 - Not always equal to reliability



Importance of Competency

- Competency is important in any engineering discipline
 - It takes on greater importance in safety

- Consider a range of disciplines
 - electronics
 - we build, run and test circuits
 - mechanical engineering
 - we construct, operate and test mechanisms
 - structural engineering
 - we build structures and subject them to loads ...

- Safety Engineering
 - we analyse systems, and don't get feedback until things fail

- Generally safety activities are “open loop”



Mandatory Mindcheck



"Sorry, your mind isn't on safety.
You'll have to go out
and come in again."



Safety should be grown up with care ...



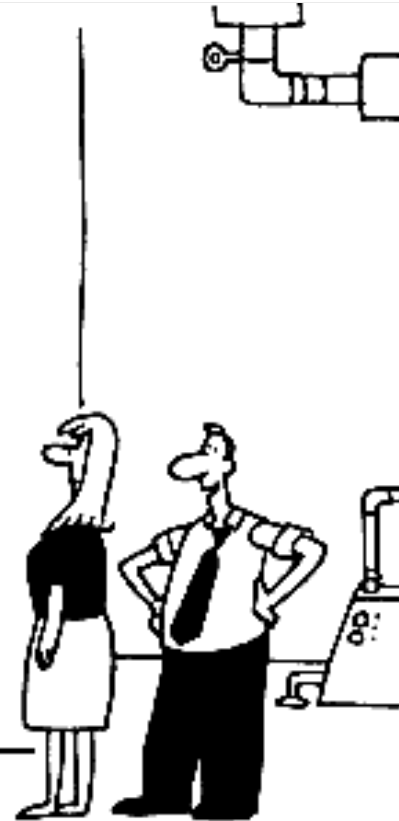


...that this never happens...



Worth1000.com

... remember that this is not enough!



Goff

"We've saved a lot of money with this safety plan so far."



Basic Definitions





What is a Hazard?

Accidents arise from hazards

→ Hazard

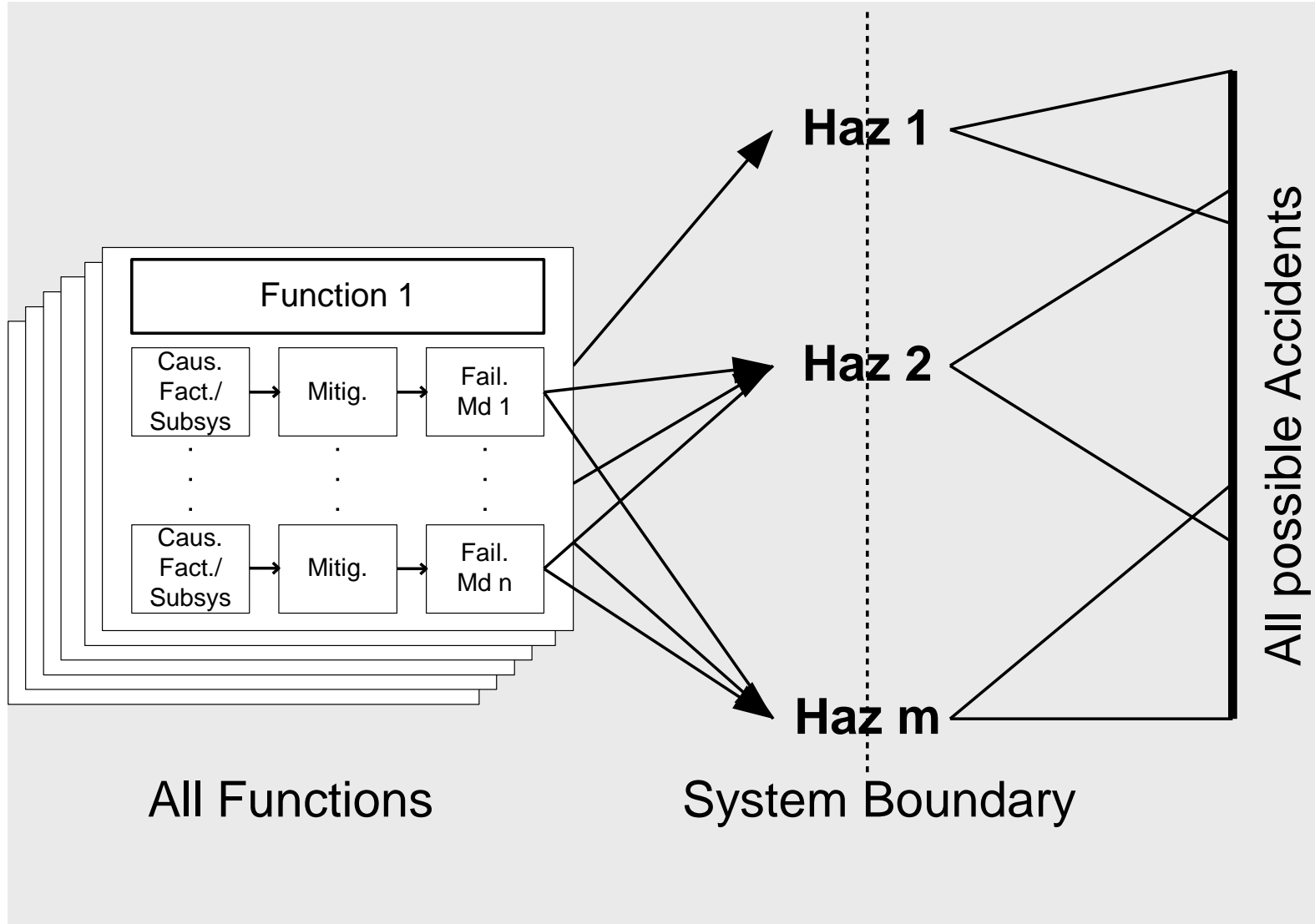
- “an accident waiting to happen”
- physical condition of platform that threatens the safety of personnel or the platform, i.e. can lead to an accident
- a condition of the platform that, unless mitigated, can develop into an accident through a sequence of normal events and actions

→ Examples:

- oil spilled on staircase
- failed train detection system at an automatic railway level crossing
- loss of thrust control on a jet engine

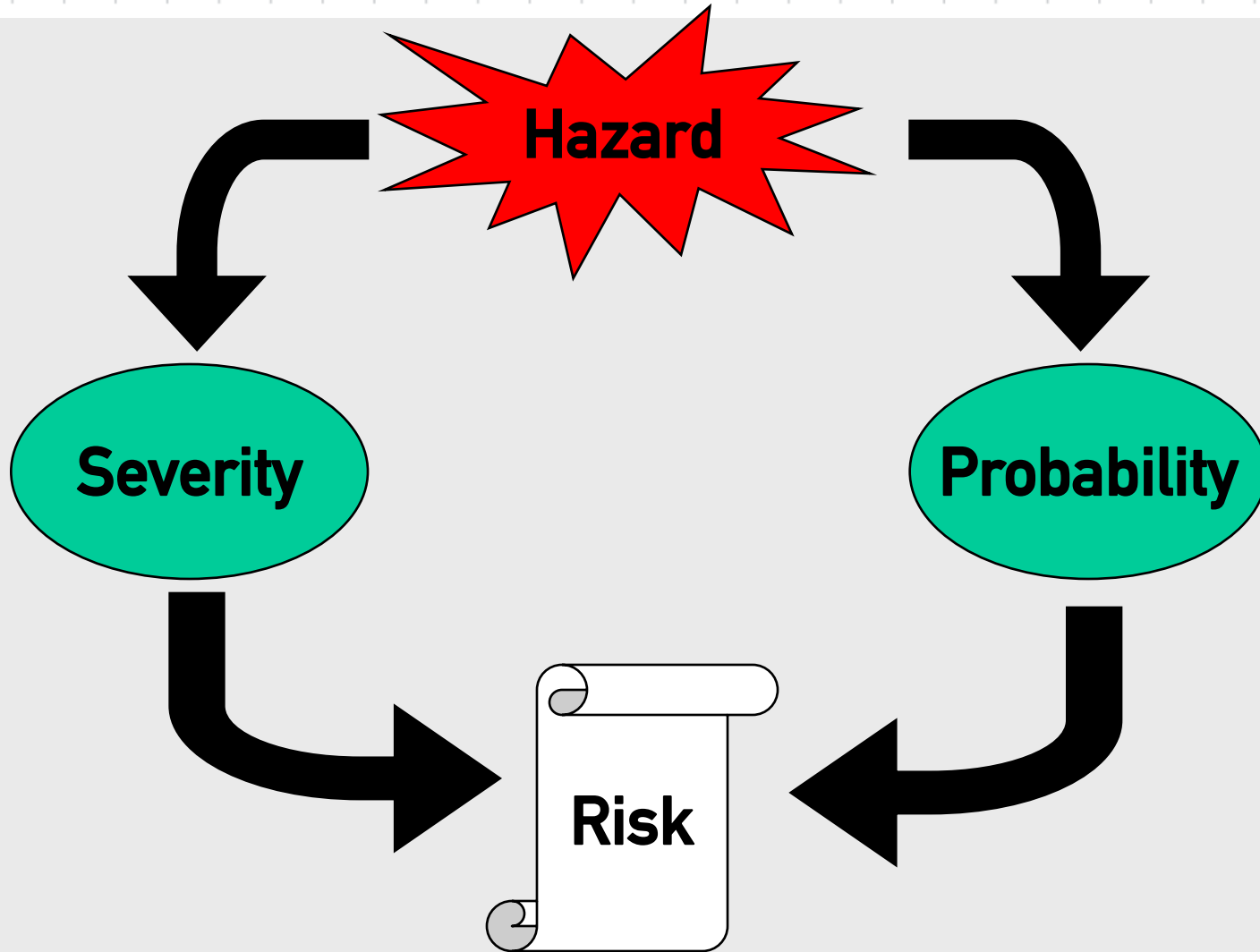


Failure Modes - Hazards - Accidents





What is Risk?





Hazard Severity Level

Category	Id.	Definition
CATASTROPHIC	I	<p><u>General:</u> death, system loss, or severe environmental damage.</p> <p><u>Specific:</u> the mission of the whole system is unavailable for more than one minute; there are no back-up facilities to compensate the absence of the mission.</p>
HAZARDOUS	II	<p><u>General:</u> severe injury, severe occupational illness, major system or environmental damage.</p> <p><u>Specific:</u> the mission can be re-established within one minute, either by reconfiguration of the system or by use of back-up facilities. However the users experience an unacceptable increase of workload.</p>
MAJOR	III	<p><u>General:</u> minor injury, minor occupational illness, or minor system or environmental damage.</p> <p><u>Specific:</u> the users can maintain the mission of the system by other means and the increase of work load by the use of these alternatives is in an acceptable range..</p>
MINOR	IV	<p><u>General:</u> all other hazards.</p> <p><u>Specific:</u> the effect of the hazard is either transparent to the user or does not cause any increase of the work.</p>



Hazard Probability Level

Level	Id.	Probability per h	Definition
Frequent	a	$P \geq 10^{-3}$	may occur several times a month
Probable	b	$10^{-3} > P \geq 10^{-4}$	likely to occur once a year
Occasional	c	$10^{-4} > P \geq 10^{-5}$	likely to occur once in the life of the system
Remote	d	$10^{-5} > P \geq 10^{-6}$	unlikely but possible to occur in the life of the system
Improbable	e	$10^{-6} > P \geq 10^{-7}$	very unlikely to occur
Incredible	f	$P < 10^{-7}$	extremely unlikely, if not inconceivable to occur



Risk Classification Scheme

Hazard Probability	CATASTROPHIC	HAZARDOUS	MAJOR	MINOR
Very Frequent	U	U	U	T
Frequent	U	U	U	T
Probable	U	U	T	T
Occasional	U	T	T	T
Remote	T	T	T	T
Improbable	T	T	A	A
Incredible	T	A	A	A

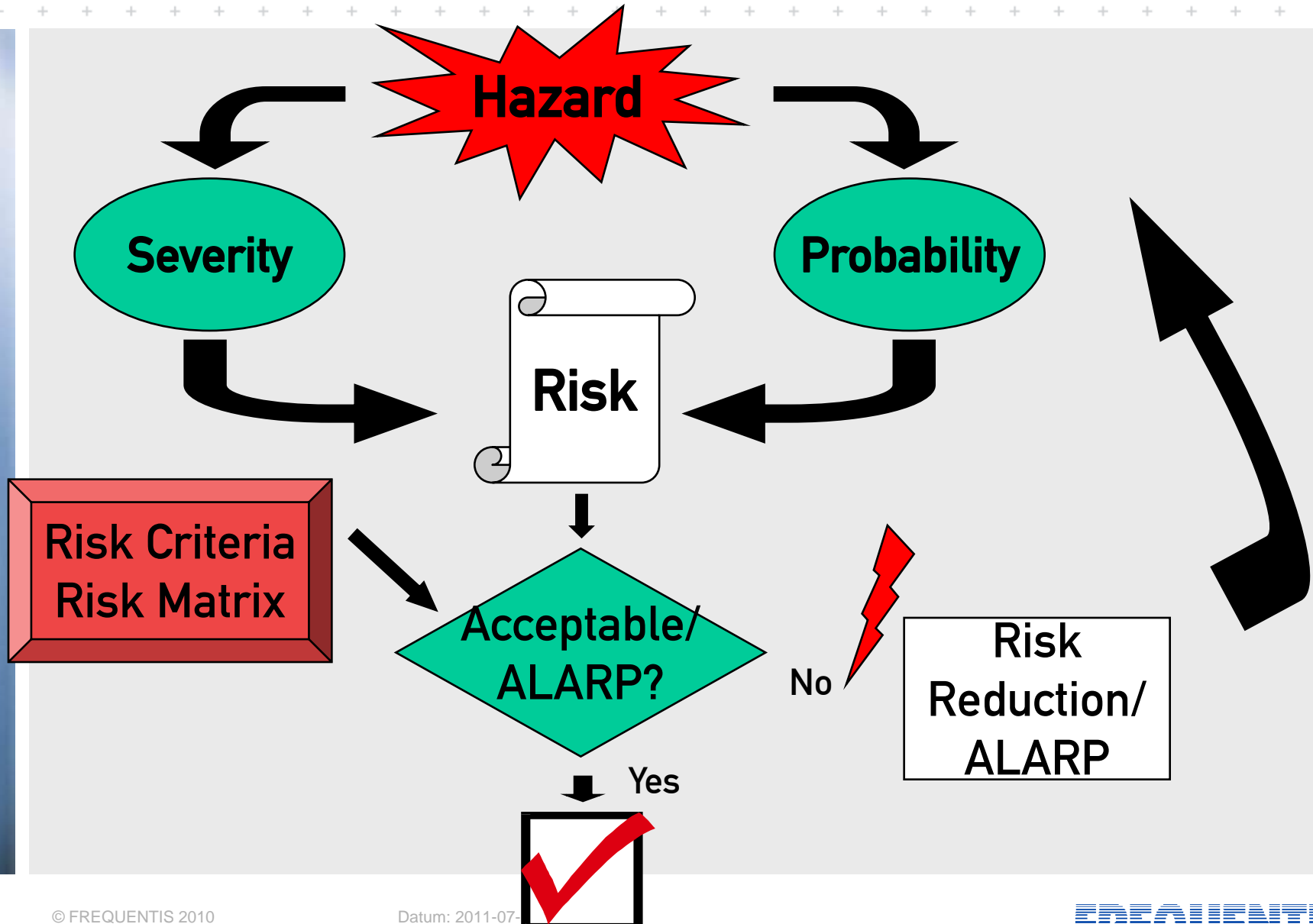


Risk Class Definition

Risk Class	Interpretation
U	Unacceptable
T	Tolerable; with the endorsement of the authority (As Low As Reasonably Practicable - ALARP Area)
A	Acceptable but has to be reported to the authority



Risk Tolerability



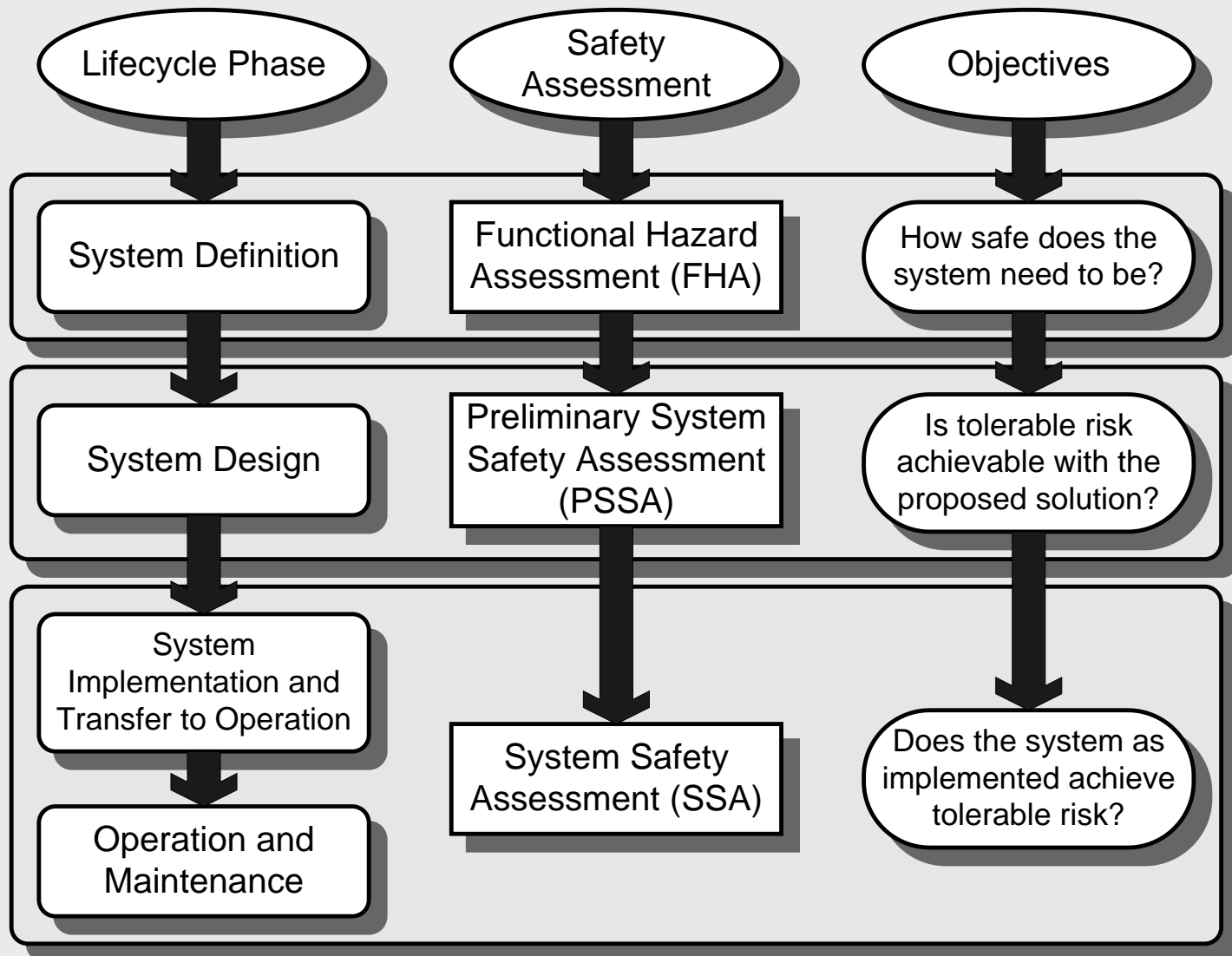


Safety Process





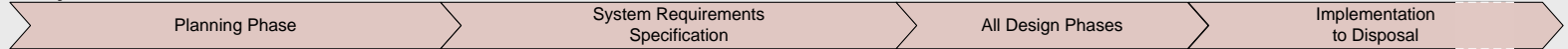
Safety Assessment in General



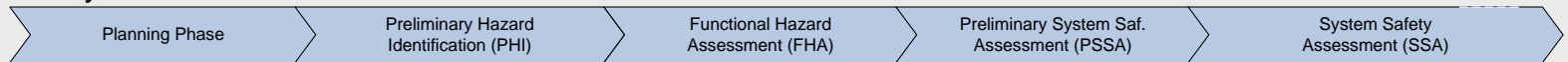


Safety Lifecycle

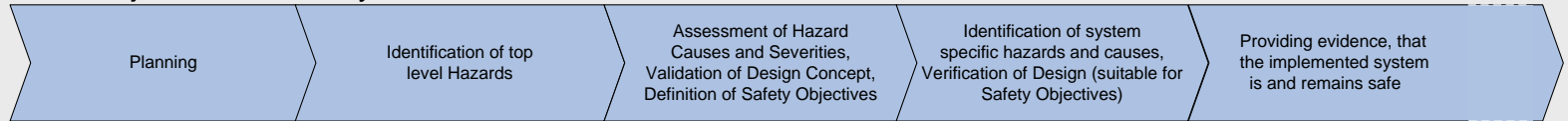
Project Phases



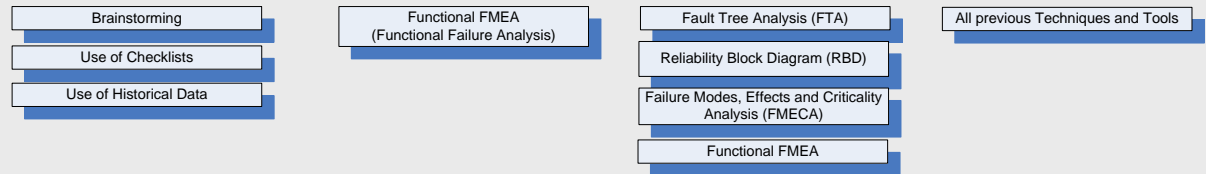
Safety Process Phases



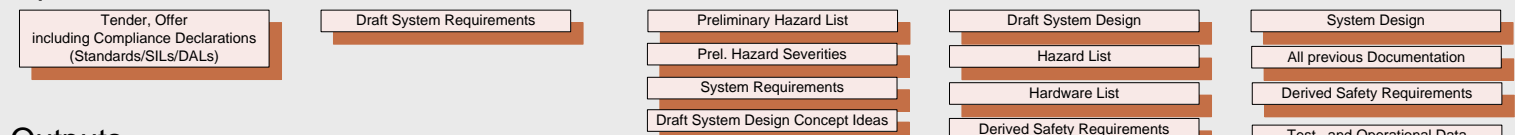
Main Objectives of Safety Process Phase



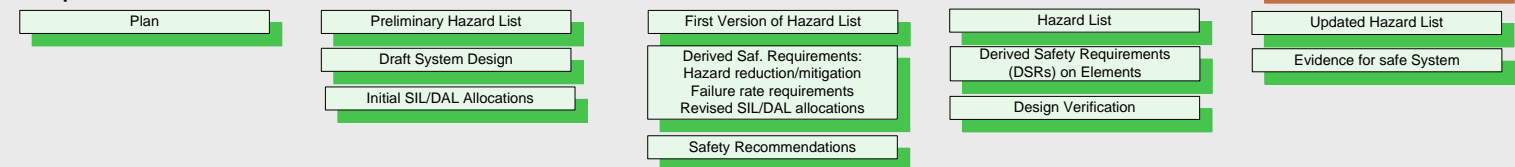
Techniques, Tools



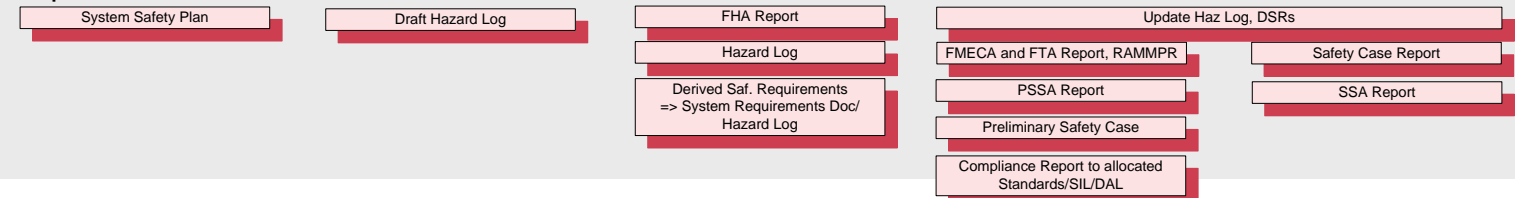
Inputs



Outputs



Reports, Documents



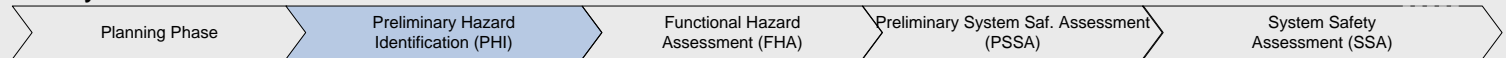


Safety Lifecycle

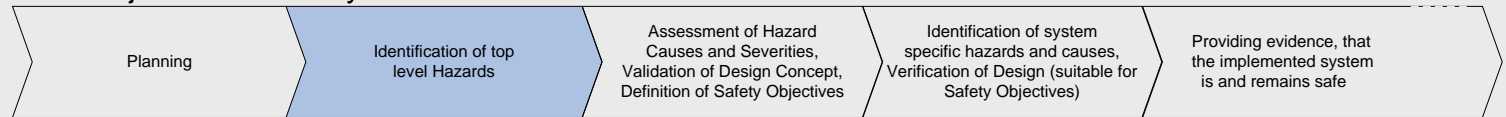
Project Phases



Safety Process Phases



Main Objectives of Safety Process Phase



Techniques, Tools

- Brainstorming
- Use of Checklists
- Use of Historical Data

Functional FMEA (Functional Failure Analysis)

Fault Tree Analysis (FTA)

All previous Techniques and Tools

Reliability Block Diagram (RBD)

Failure Modes, Effects and Criticality Analysis (FMECA)

Functional FMEA

Inputs

Tender, Offer including Compliance Declarations (Standards/SILs/DALs)

Draft System Requirements

Preliminary Hazard List

Draft System Design

System Design

Prel. Hazard Severities

Hazard List

All previous Documentation

System Requirements

Hardware List

Derived Safety Requirements

Draft System Design Concept Ideas

Derived Safety Requirements

Test- and Operational Data

Outputs

Plan

Preliminary Hazard List

First Version of Hazard List

Hazard List

Updated Hazard List

Draft System Design

Derived Saf. Requirements: Hazard reduction/mitigation Failure rate requirements Revised SIL/DAL allocations

Derived Safety Requirements (DSRs) on Elements

Evidence for safe System

Initial SIL/DAL Allocations

Safety Recommendations

Design Verification

Reports, Documents

System Safety Plan

Draft Hazard Log

FHA Report

Update Haz Log, DSRs

Hazard Log

FMECA and FTA Report, RAMMPR

Safety Case Report

Derived Saf. Requirements => System Requirements Doc/ Hazard Log

PSSA Report

SSA Report

Preliminary Safety Case

Compliance Report to allocated Standards/SIL/DAL



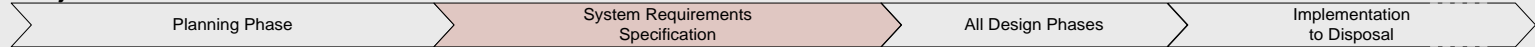
Preliminary Hazard Identification

- Start of safety process with PHI (Preliminary Hazard Identification) and PHA (Preliminary Hazard Assessment)
- This phase is often included in the FHA phase
- Preliminary hazard list and severities
 - Brainstorming
 - Historical Data
 - Checklists
 - => Target rates for hazards (Risk Matrix), Safety Objectives
 - => Initial SIL/DAL Allocations

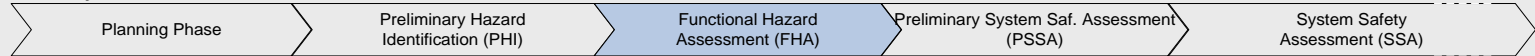


Safety Lifecycle

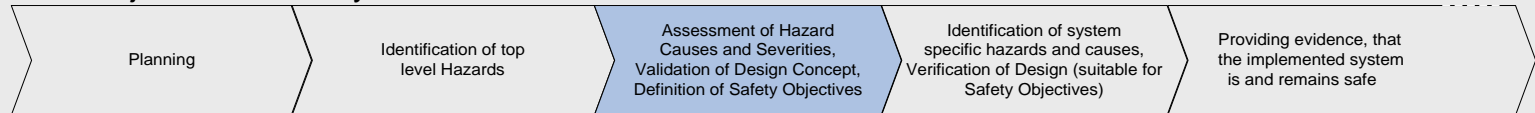
Project Phases



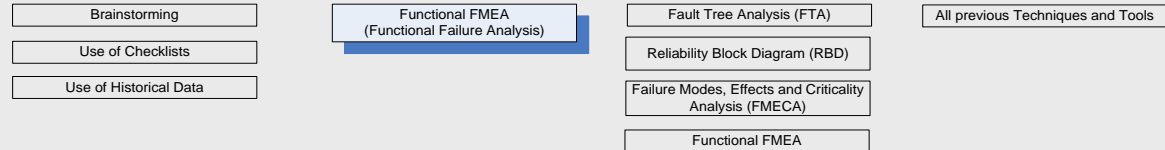
Safety Process Phases



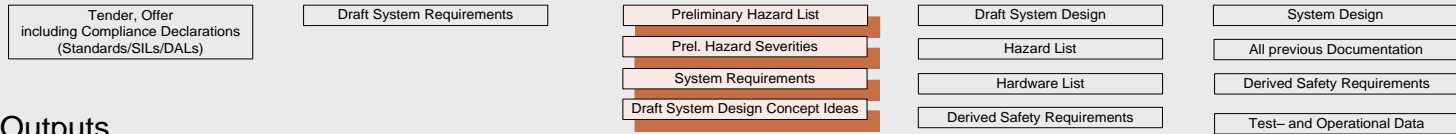
Main Objectives of Safety Process Phase



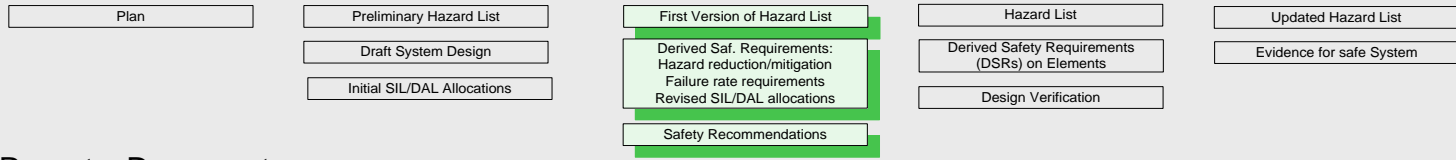
Techniques, Tools



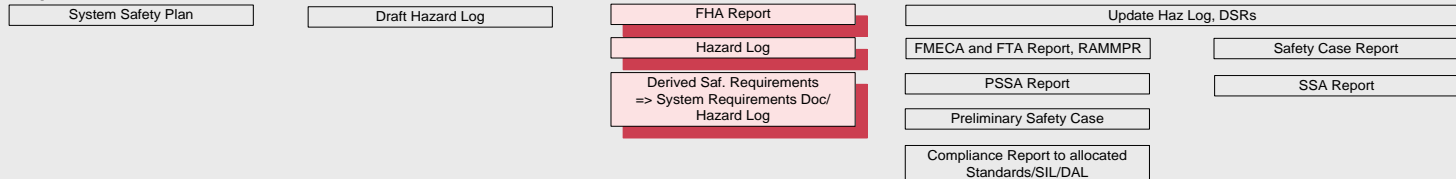
Inputs



Outputs



Reports, Documents





Functional Hazard Assessment

→ Functional Hazard Assessment (FHA)

“How safe does the system need to be?”

→ Functional Failure Modes and Effects Analysis

- Guided brainstorming of domain experts (Requirements Engineer, Designer, Developer, IV&V, Safety Engineer, Human Factors Engineer, End User, ...)
- Basic functions
- Theoretical failure modes and safety relevance/severities
- Mapping of failure modes to hazards
- => Update of Hazard Log (ongoing)

→ => Derived Safety Requirements (DSRs) - recorded during the whole assessment - main means for risk reduction by safety process

→ Recording of assumptions!!!

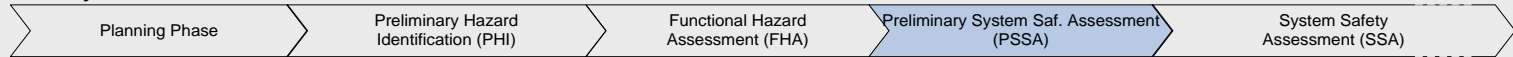


Safety Lifecycle

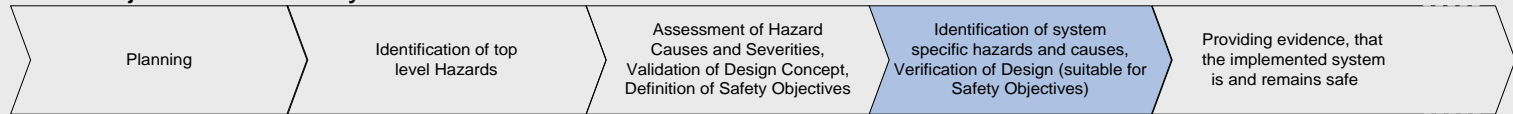
Project Phases



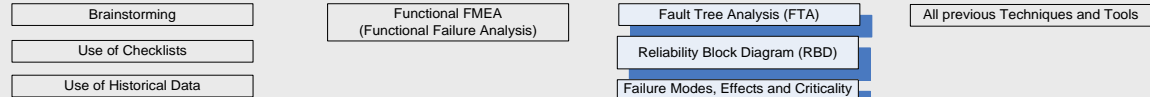
Safety Process Phases



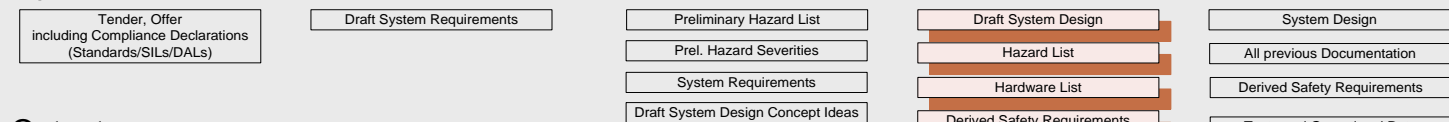
Main Objectives of Safety Process Phase



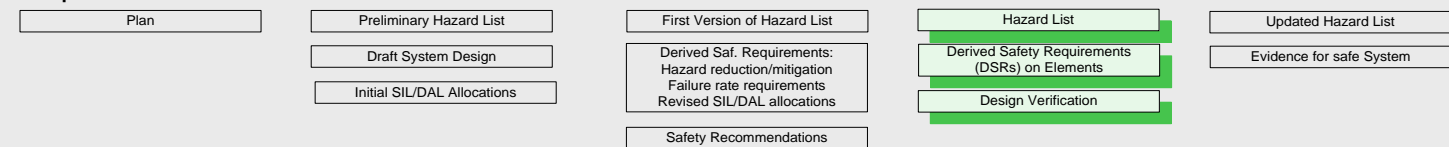
Techniques, Tools



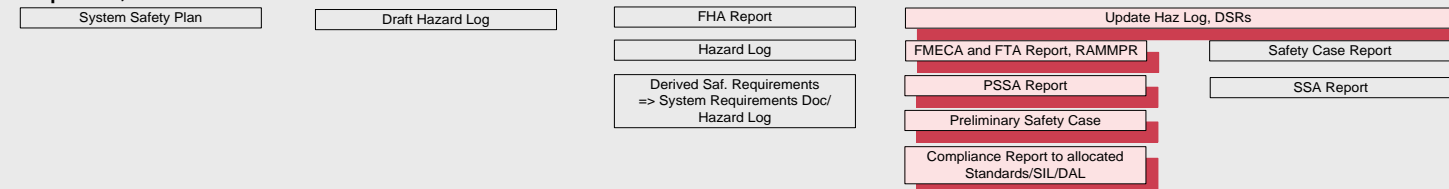
Inputs



Outputs



Reports, Documents





Preliminary System Safety Assessment

- Preliminary System Safety Assessment (PSSA)
 - “Does the proposed design reach the safety objectives?”
- Breaks down causes of hazards and functional failures
- Fault Tree Analysis (FTA)
- Reliability Block Diagrams (RBDs)
- Failure Modes and Effect Analysis (FMECA)
- Can lead to further requirements, e.g. additional redundancy necessary to meet hazard target rates

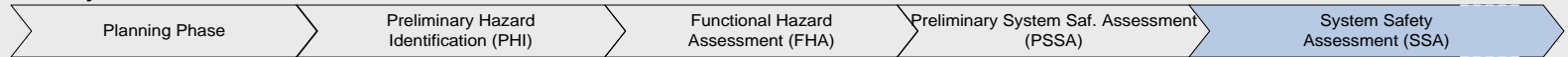


Safety Lifecycle

Project Phases



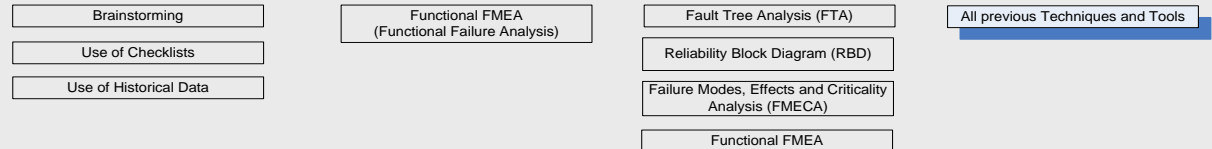
Safety Process Phases



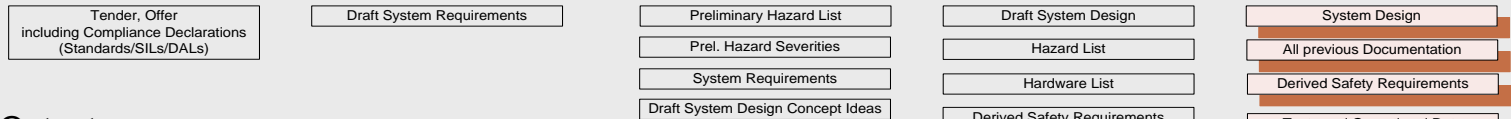
Main Objectives of Safety Process Phase



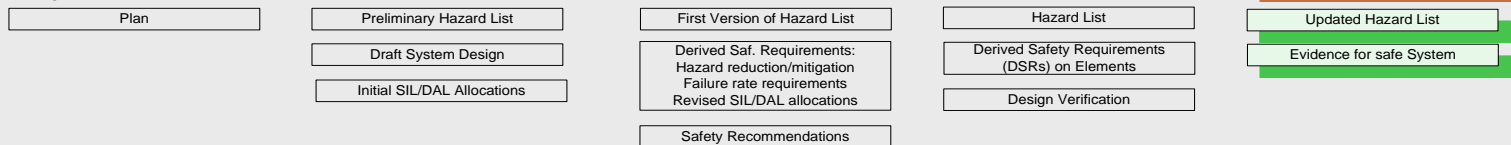
Techniques, Tools



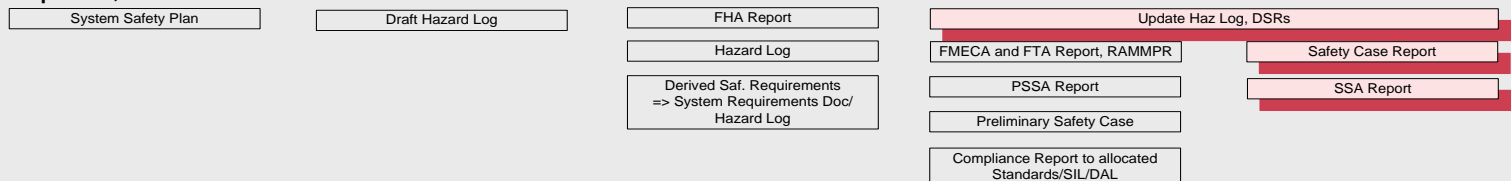
Inputs



Outputs



Reports, Documents





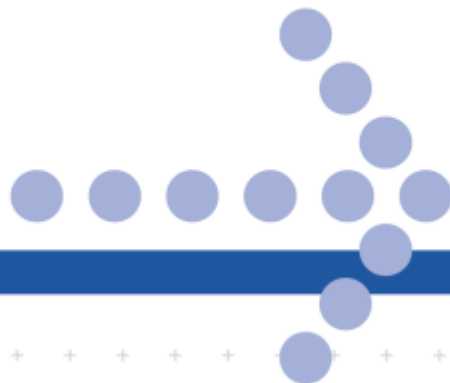
System Safety Assessment (SSA)

- “Does the system as implemented achieve tolerable Risk?”
- Update of all previously performed analyses
- Verification, whether all safety targets and safety requirements are met
- Production of a safety case or safety assessment report
- Transition to maintenance



Safety Process Standards

- IEC 61508
 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
- Def-Stan 00-56
 - Safety Management Requirements for Defence Systems
- Def-Stan 00-55 (superseded and incorporated to new 00-56)
 - Requirements for Safety Related Software in Defence Equipment
- European Air Traffic Management Program (EATMP):
 - System Safety Assessment Methodology from the European Organisation for the Safety of Air Navigation
- CENELEC Standards EN 50126, EN 50128 and EN 50129
- MilStd 882



Safety Requirements





Classes of Safety Requirements

→ Fundamental

- Top level requirements for project
- from standards
- from engineering practice

→ Derived safety requirements (DSRs)

- From all stages of safety life cycle:
- Product safety requirements
- Process safety requirements
- Procedural safety requirements



Product Safety Requirements

→ Functions

- Additional/changed functions to mitigate failures/risks
- Own system and/or interacting systems/environment

→ Safety Targets (Safety Objectives)

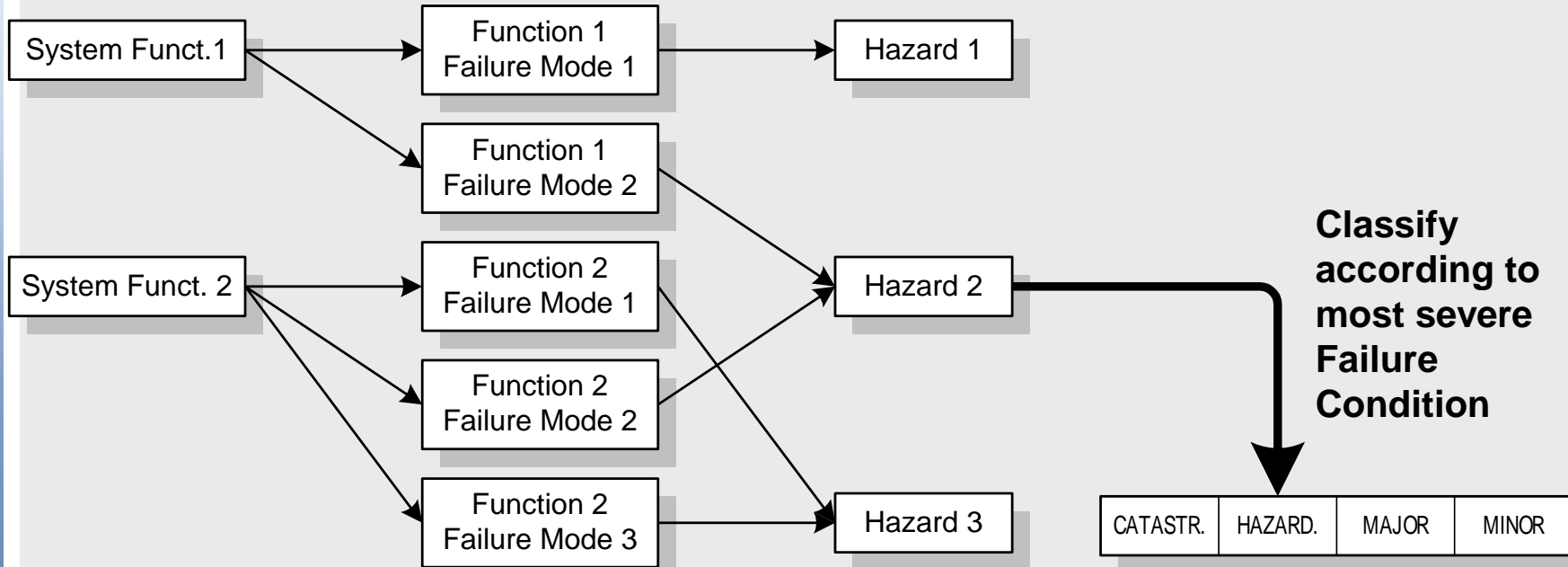
- Target rates or probabilities
- Allocation to sub-components possible

→ Architecture

- Increased redundancy
- Increased failure tolerability

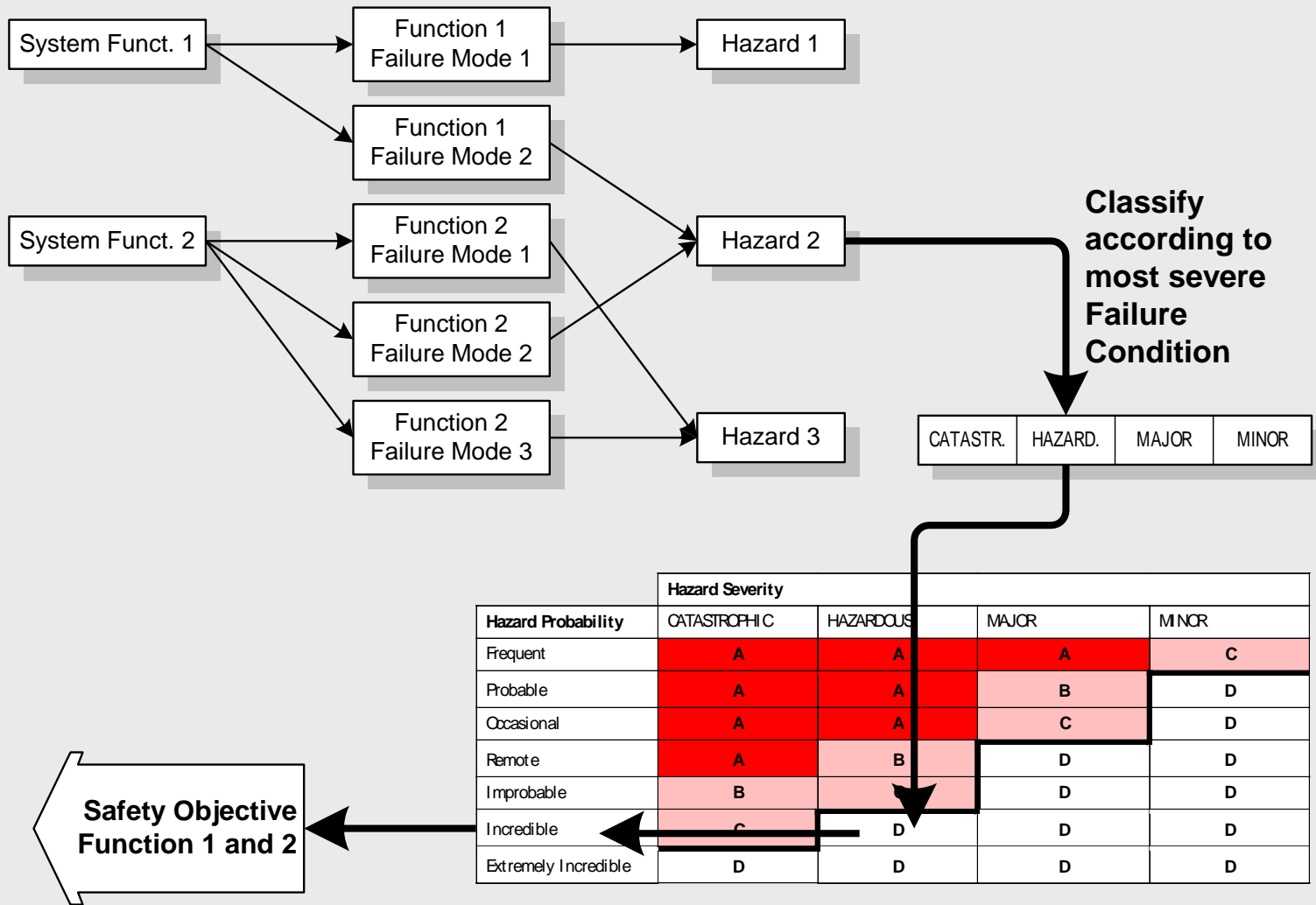


Safety Objectives





Safety Objectives (2)





Process and Procedural SRs

- Safety process requirements
 - safety standards
 - safety deliverables from subcontractors/suppliers
 - issues to assess/track (assumptions)

- Development process requirements
 - Development Standards, SILs, DALs, ...
 - Manufacturing/procurement requirements

- Installation rules
 - e.g. physical separation of redundant equipment
 - routing/cabling requirements

- Procedural requirements
 - commissioning, operation, maintenance, decommissioning



Recording of Safety Requirements

- Product SRs should integrate with main requirements/ traceability system
 - two choices:
 - Add to requirements document
 - Produce separate document and link in requirements document

- Process SRs:
 - add to respective plans, e.g. safety process as explicit activities in System Safety Program Plan
 - produce additional documents

- Need to be traced within Safety Case (if applicable)



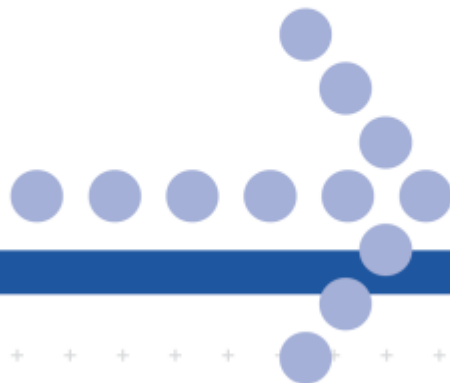
Assumptions

- Whole safety analysis is based on assumptions on
 - environmental conditions,
 - other systems,
 - procedures
 - other influences which are outside of our control
 - local assumptions about what can be achieved later in design

- Have to be evaluated!

- Have to be recorded explicitly!!

- Have to be verified!!!



Methods/Techniques





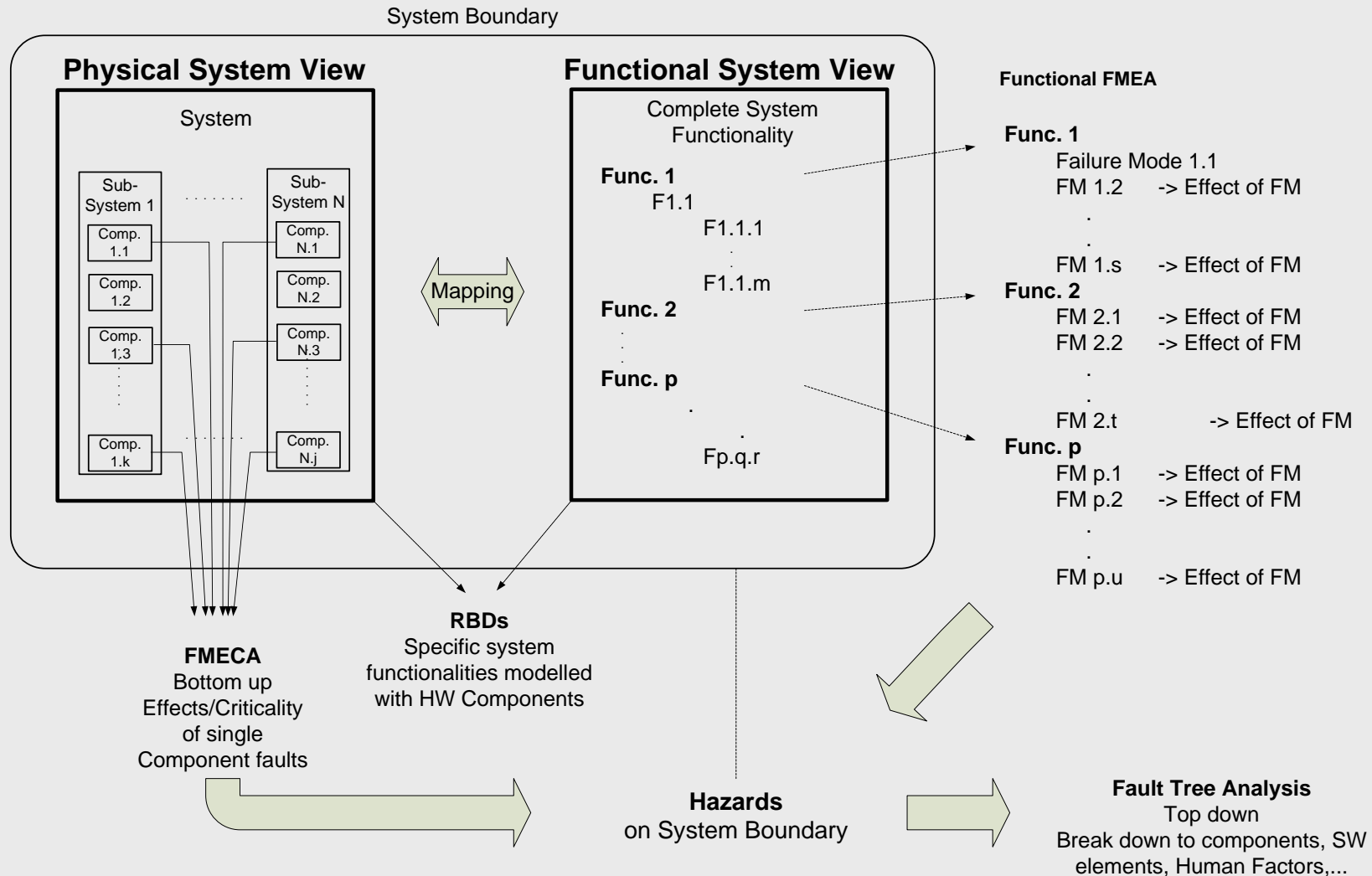
- Can view system from multiple viewpoints
 - Physical decomposition: What the system is made of
 - Platform
 - System 1, System 2,...
 - Control, Sensors, Actuators, Mechanics
 - Functional decomposition: What the system does
 - Function 1, Function 2, ... , Function n
 - 1.1, 1.2, ...; 1.1.1, 1.1.2,
 - Information flows needed
 - Timing behaviour, ...

- Physical to functional mapping

- Safety relates to both physical and functional views



Techniques Overview





Functional FMEA

- or Functional Failure Analysis
- Typically performed to support safety analysis effort during the design process and the FHA
- Early in the lifecycle
- Intended for iterative application
- Considers hypothetical failure modes
- Outputs:
 - Functional failure modes that may be eliminated/mitigated by functional level design changes
 - Gives confidence in overall design concept



- Analysis of effects of single failures (inductive)
- Used to
 - investigate effects of known component failures within (sub-) systems
 - provide information about sub-system failures for incorporation into system and platform level analyses
 - show that single component failures will not lead to system failure (hazard)
 - complement fault tree
- Results presented in tabular form
- In *principle* straightforward!



FMECA Implementation

- Define System to be analysed
 - Drawings, charts, system descriptions, ...

- Define targets of analysis
 - Eliminate single points of failure
 - Define maintainability actions
 - ...

- Break system down into convenient and logical elements
 - single pieces/components (e.g. resistor)
 - Line Replaceable Units (LRU) – lowest level at which repair is made by customer
 - Systems/Sub-systems
 - Interfaces



FMECA Implementation (2)

→ List of failure modes

- e.g. Switch – open, partially open, closed, partially closed, chatter
- Operator – wrong operation to proper item, wrong operation to wrong item, proper operation to wrong item, perform too early, perform too late, fail to perform

→ Identification of effects of failure

- Consequence a failure has on the operation, function or status of component/system
- Can be hierarchically built up (lower level FMEA effect -> higher level FMEA failure mode)

→ Criticality Analysis

- Rank each potential failure mode according to the combined influence of severity classification and its probability of occurrence based upon the best available data

→ Maintainability Information

- Provide early criteria for maintenance planning analysis, LSA, test planning etc. and identify maintainability design features requiring corrective action



FMECA Tables - Example

ID/Item	Failure Mode/Faults	Effects of the Failure Mode	Failure Detection Method	Recovery Provisions	Criticality, Rationale
SWITCH 08 JIF-board	one JIF-A: loss or corruption of communications with SDC-A	The communication in switch A to all devices (EPOS, LIF, ERIF, ALIF) connected to this JIF is lost Switch redundancy is reduced no effect to user	SDC-A reports to TMCS: JIF-A fault; all connected devices report via JIF-B: JIF-A fault to TMCS; fault indication on JIF-Board	automatic: connected devices (EPOS, LIF, ERIF, ALIF) use all voice and data information from Switch-B manual: Remove and replace JIF-Board of Switch-A	Severity is none, because Switch-B is used; redundancy is reduced
SWITCH 09 ISO-Board	one ISO-Board-A: loss or corruption of output to associated Highway-A	One Highway-A out of service Highway redundancy is reduced no effect to user	all feeding JIF-A report to TMCS: ISO-A fault;	automatic: connected devices (EPOS, LIF, ERIF, ALIF) use all voice information from Switch-B; manual: Remove and replace ISO-Board-A	Severity is none, because Switch-B is used; redundancy is reduced

ID/Item	Failure Mode/Fault	Failure Rate Lambda / hours	Failure Mode/Item Criticality	Failure Predictability	Maintenance Actions
SWITCH 08 JIF-board	one JIF-A: loss or corruption of communications with SDC-A	1.48311E-05	$C_{[none]} = 1.95$	Intermittent failure of JIF; intermittent communication alarms from SDC and/or connected devices	Manual: Remove and replace JIF-Board of Switch-A
SWITCH 09 ISO-Board	one ISO-Board-A: loss or corruption of output to associated Highway-A	8.99655E-07	$C_{[none]} = 0.12$	Intermittent highway alarms from JIF-A	Manual: Remove and replace ISO-Board-A

Reliability Block Diagrams (RBDs)

- Define and describe the system
 - physical configuration and functional operation
- Models “what is necessary for success” of defined function
 - Models a component state as “Working” or “Failed”
- Can be used for
 - design decisions – which design/configuration will reach RAM targets
 - verification – does the system reach the RAM targets
 - logistic support calculations (for repairable systems)



RBDs - Assumptions

- What does the quality of results from an RBD rely on?

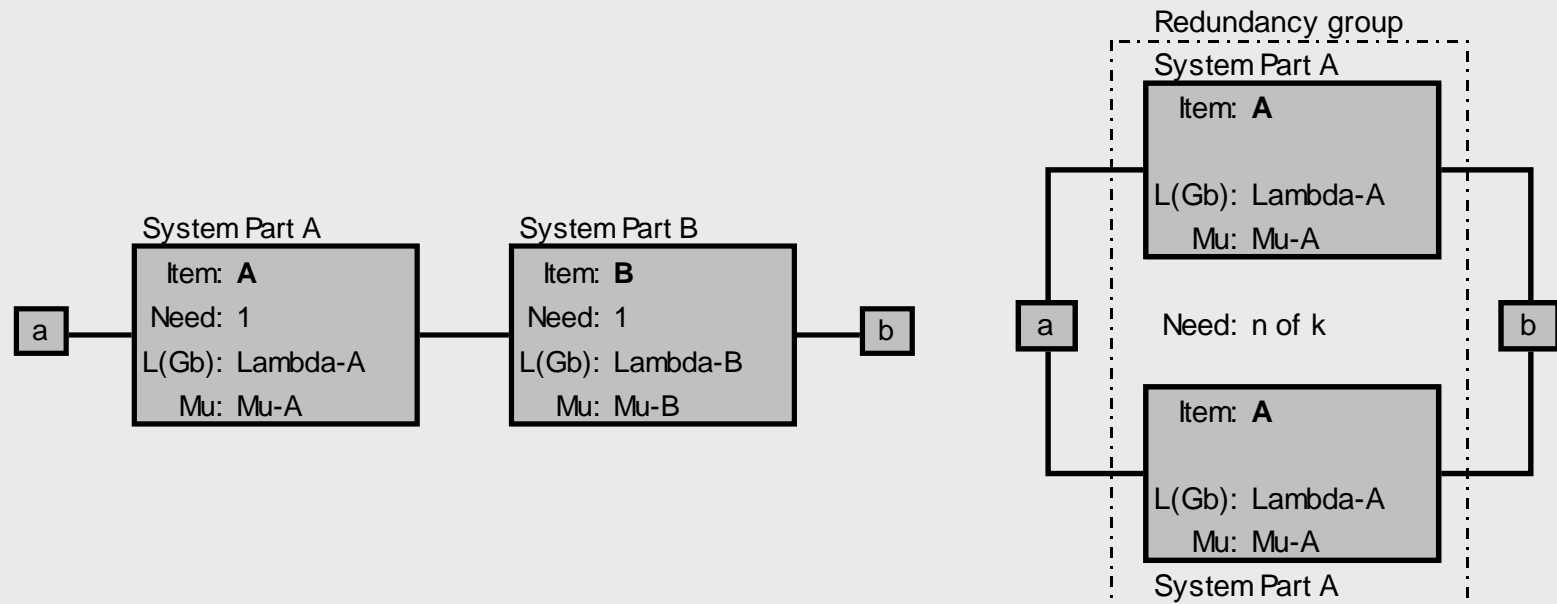
- General Assumptions:
 - Failure independence of blocks
 - Bimodal device status (working or failed)
 - Interconnection failures must be dealt with in boxes

- To be documented:
 - Any data deficiencies, approximations, truncations
 - Rationale for non-modeled or neglected devices
 - Failure distributions of boxes (exponential, Weibull, etc)
 - Potential failure independencies or common causes



RBDs – Basic Structures

→ RBDs model the system in series, parallel and "n out of k" structures

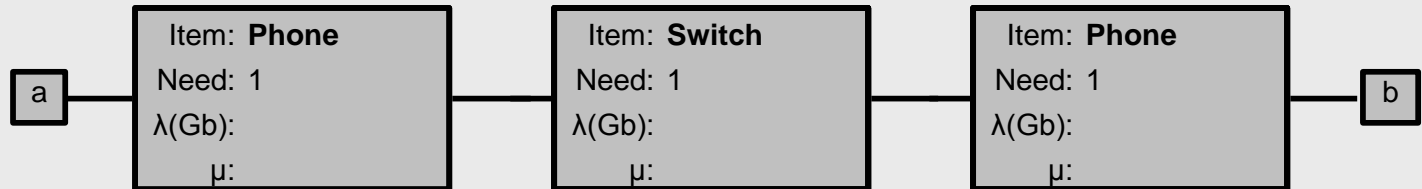
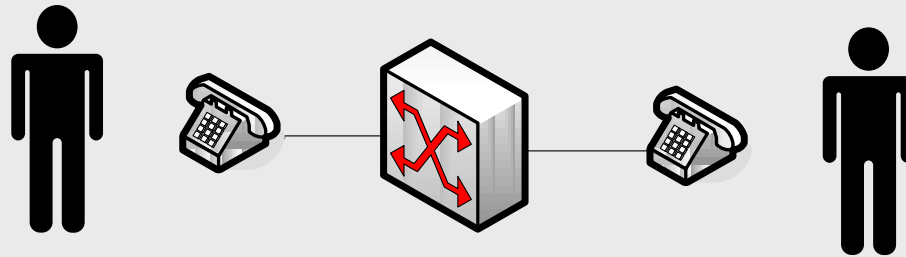


→ The results of these calculations are figures for **Availability** and **Reliability**



Example Phone

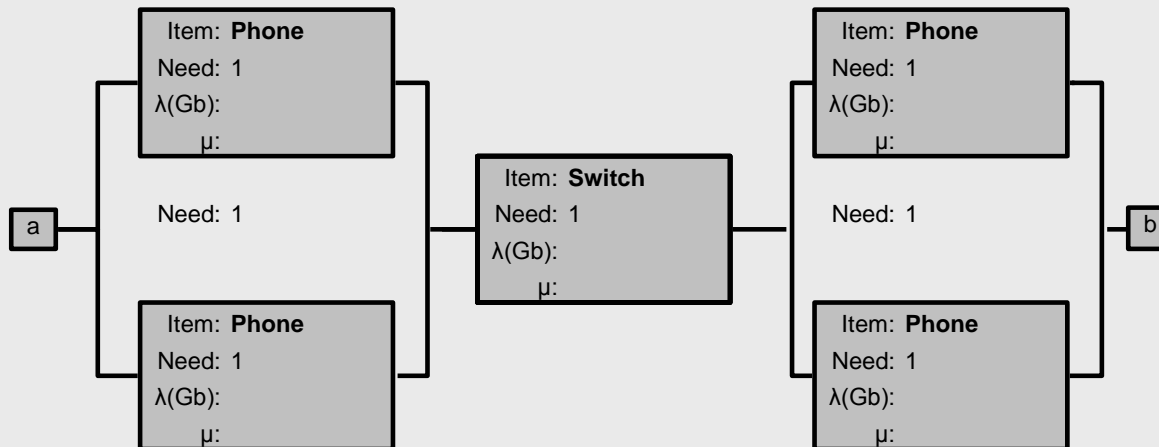
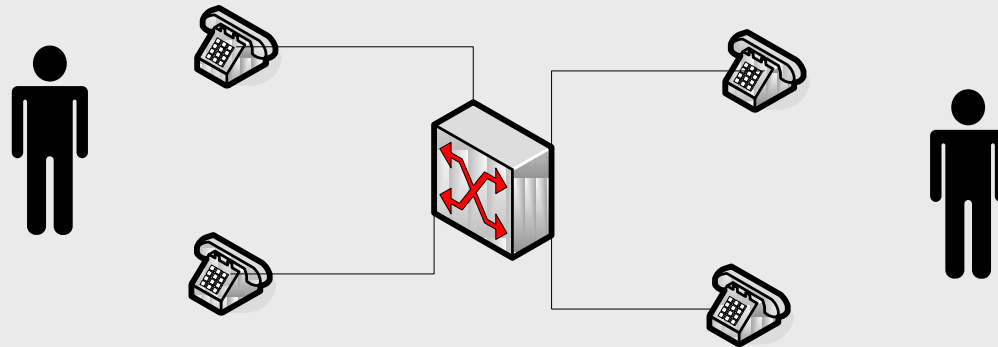
→ Series Structure





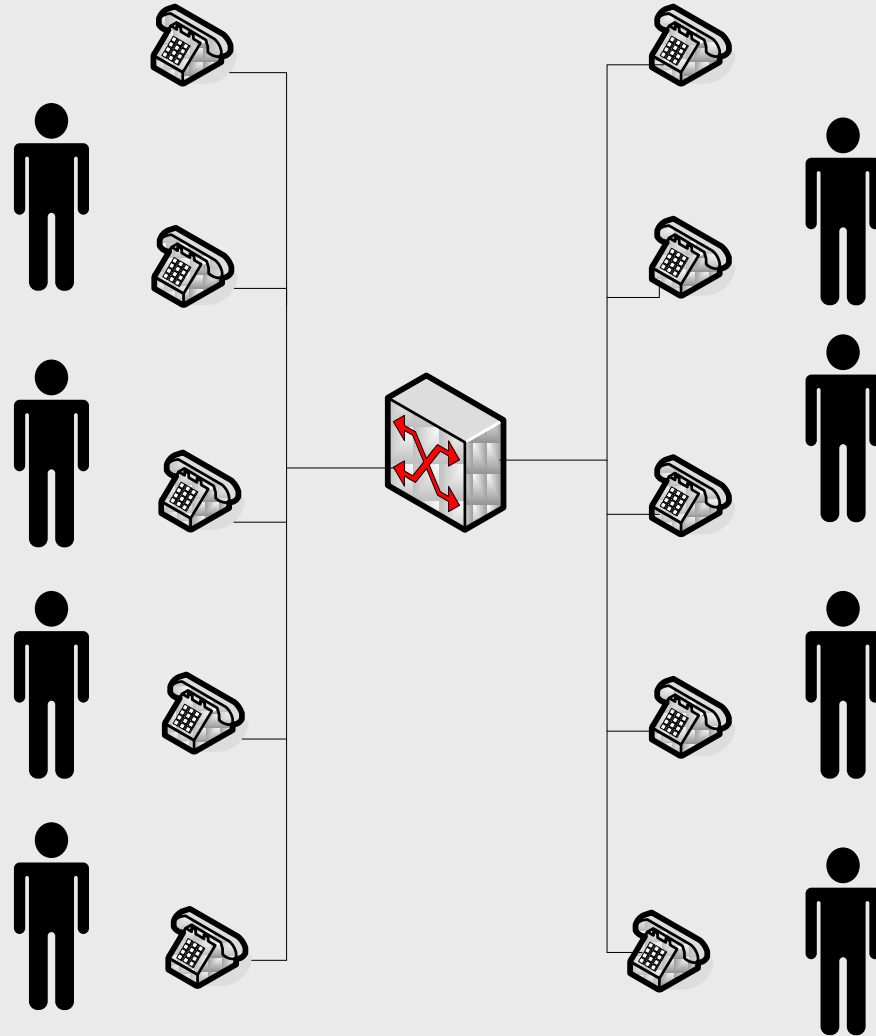
Example Phone (2)

→ Parallel Structure





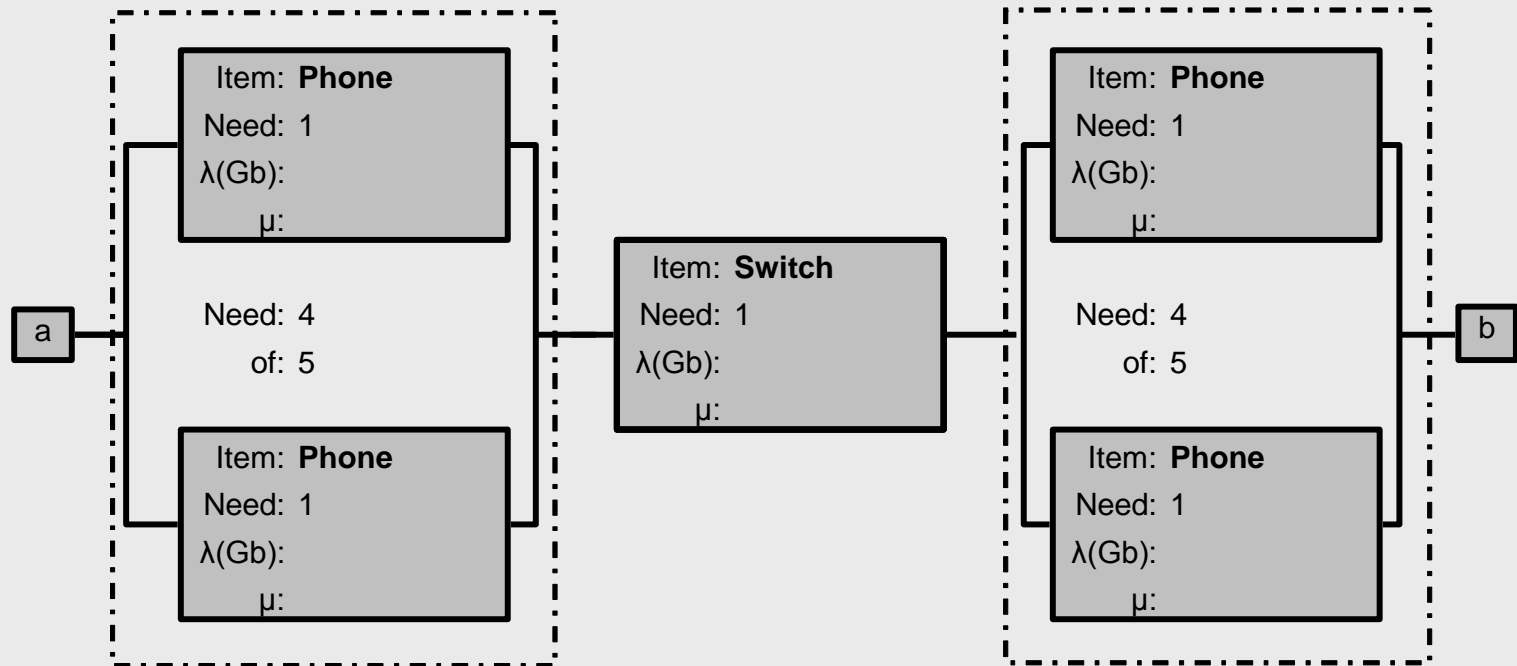
Example Phone (3)





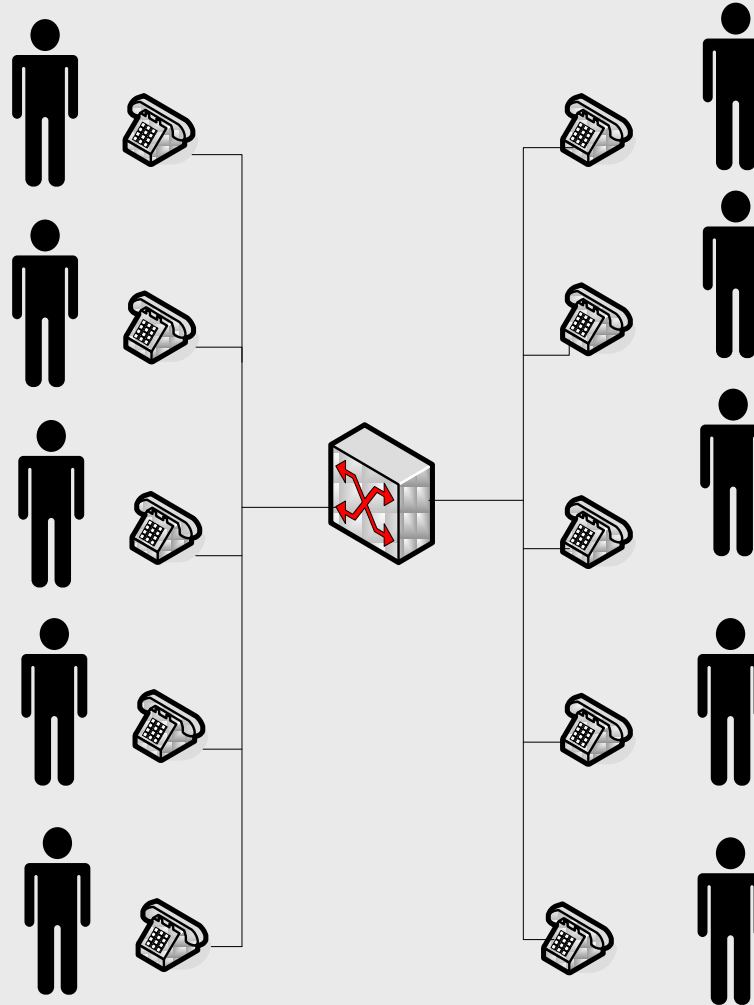
Example Phone (4)

→ Redundancy Group



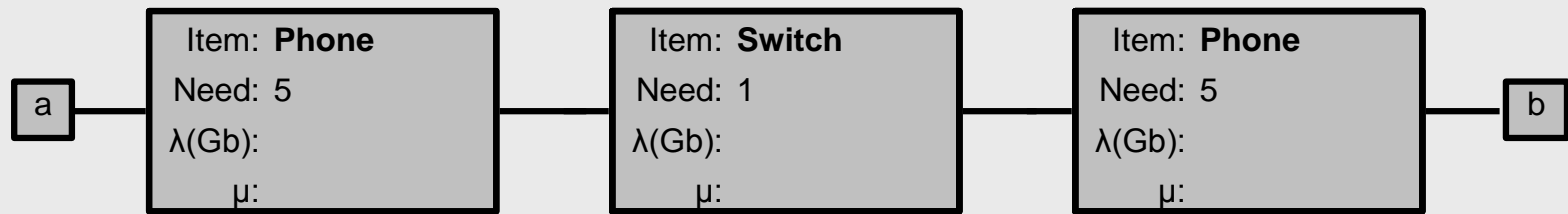


Example Phone (5)



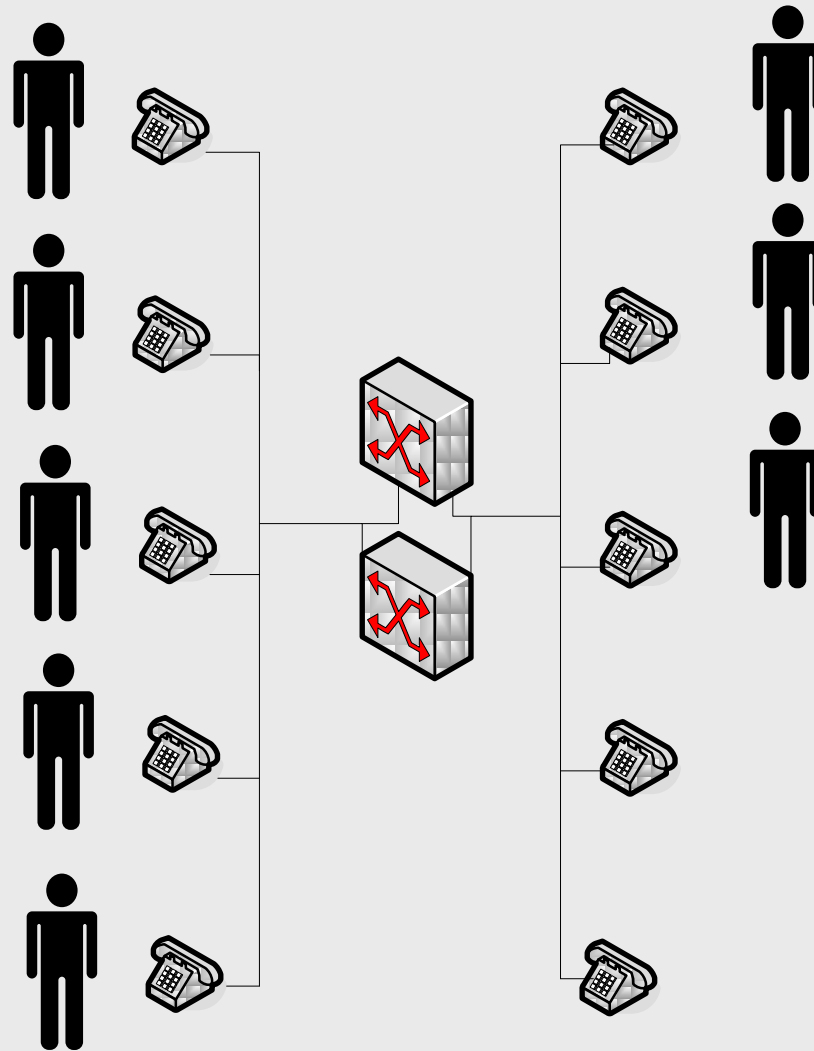


Example Phone (6)



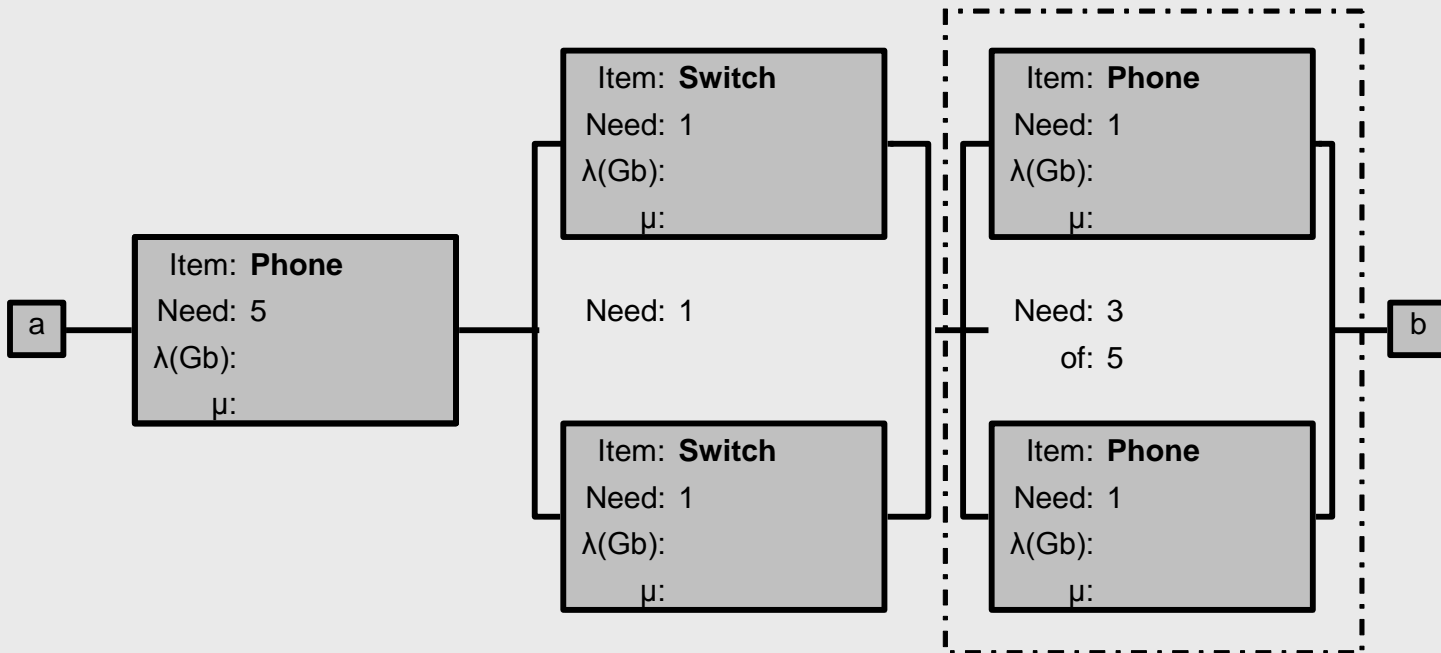


Example Phone (7)



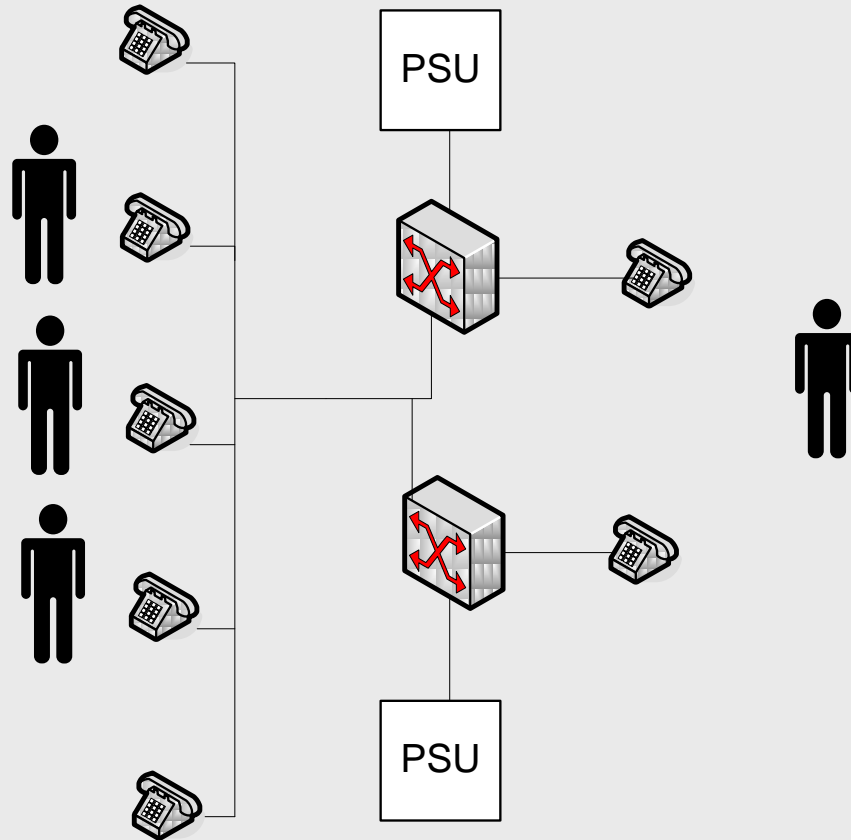


Example Phone (8)



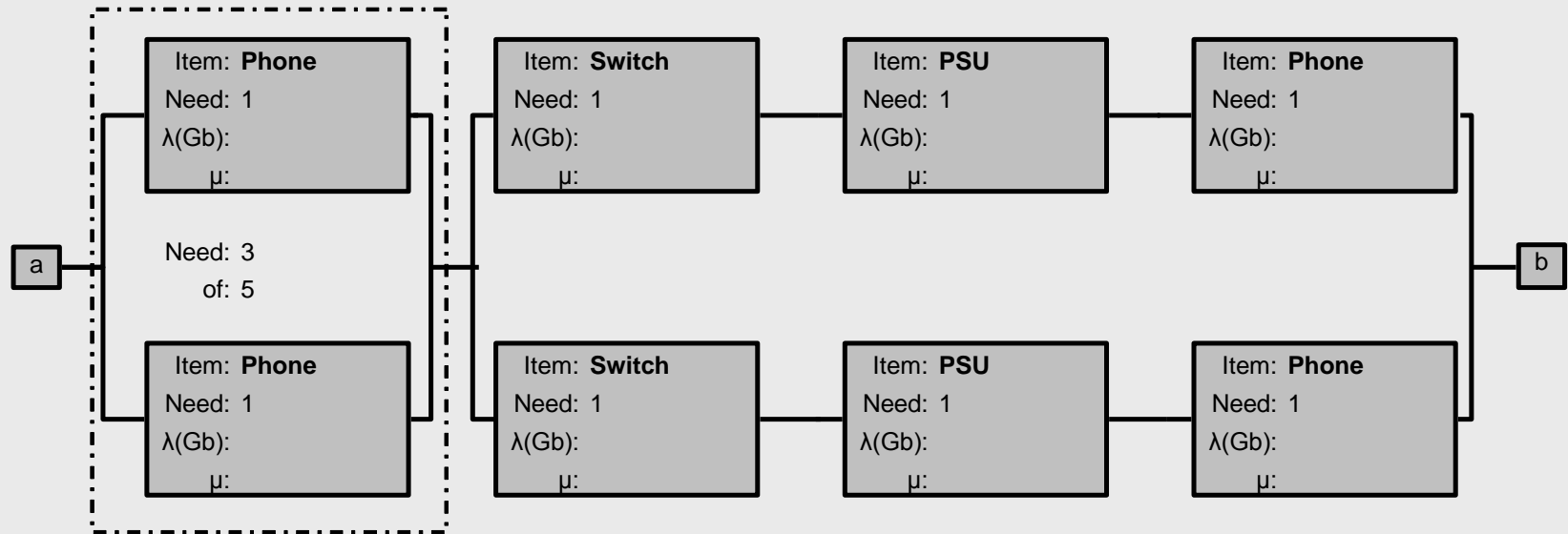


Example Phone (9)



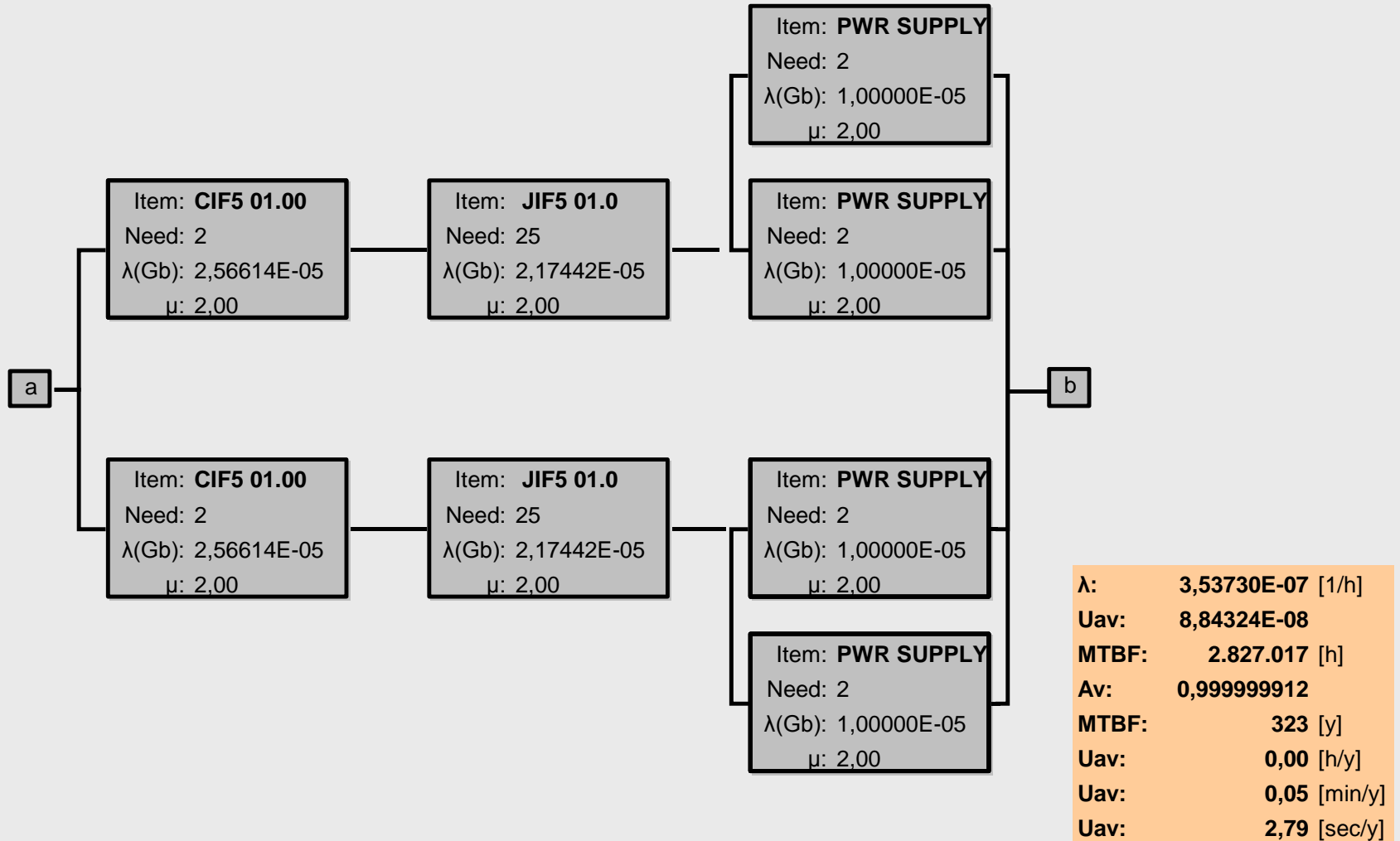


Example Phone (10)





RBDs – Example: Voice Switch



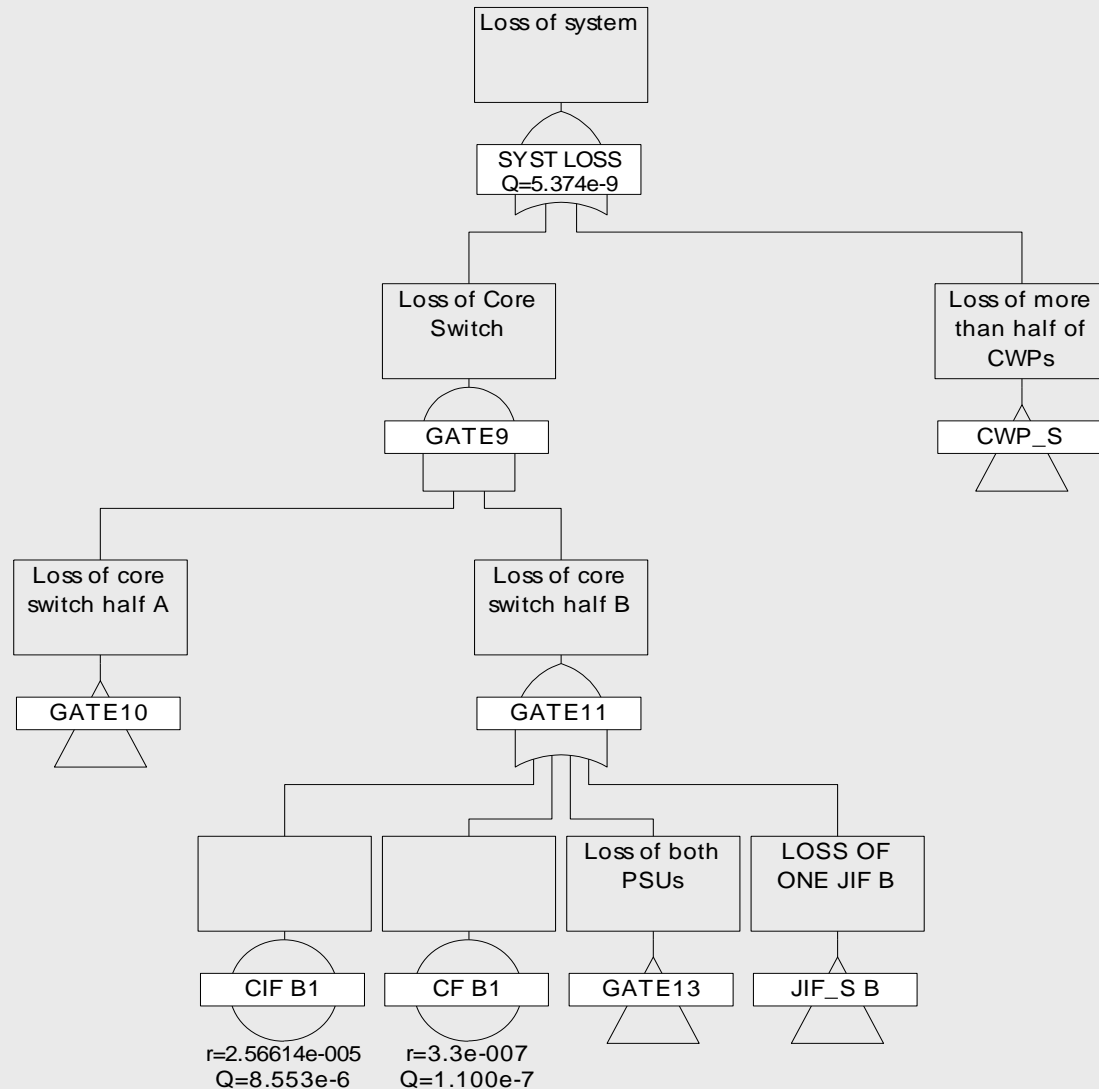


Fault Trees

- Well known and widely used safety tool
- Deductive, top down Approach
- Start with top level hazard and "work your way down"
 - Hazards have to be known in advance
- Can consider hardware, software, humans
- Identifies also multiple points of failure
- Based on Boolean Logic (AND, OR gates)
- Quantitative and qualitative analysis possible
 - Are there any single points of failure?
 - Which factors have to occur simultaneously to cause a failure?
 - What are the probabilities associated with each failure?



Fault Trees - Example





Common Cause Analysis

→ Dependence:

- Occurrence of event affects probability of other(s)
- $P(A \cap B) \neq P(A) \cdot P(B)$

→ Two types:

- dependence between failure events: $P(B) = P(B(A))$
- dependence of failure events on common system condition C – environmental condition: $P(A) = P(A(C))$, $P(B) = P(B(C))$

→ Can lead to „hidden“ Single Points of Failure and erroneous quantitative calculations

→ Are responsible for a high proportion of system failures!



Common Cause Analysis (2)

→ Environmental Hazards

- Ambient parameters, extremes
- Influence from accidents outside system boundary

→ Design and Analysis Errors

- Misunderstandings and -interpretations of requirements and environment
- Faulty or insufficient analysis (e.g. EMC protection, power consumption)
- Damage caused by tests
- Poor maintainability

→ Manufacturing & Assembly Errors

→ Operation and Maintenance Errors



Common Cause Analysis (3)

- Identification of Common Causes is difficult!
- Analysis techniques: extension of deductive analysis targeted at common causes of items previously considered as independent
- Very detailed system knowledge necessary
- General outline:
 - Identification of groups of critical components
 - Grouping of parts by common features
 - Identification of credible failure modes
 - Consideration of generic failure mechanisms and generic causes
 - Recording of observations and conclusions
 - Identification of affected system parts/areas



Zonal Hazard Analysis (ZHA)

- Common Cause analysis technique specifically considering effects of failures of adjacent components with different technologies, e.g. hydraulic leak -> short circuit
- Identification of interactions / invalid claims of independence
- Based on physical structure of platform
- Should be carried out at various stages



→ Determine Zones

- Determine threats to system (fire, water, ...) and the ways in which they can be contained
- Determine physical containment zones

→ Identify equipment in zones

→ Things to be addressed are e.g.:

- Clearance from moving parts, thermal heating/cooling, vibration, ionising/non-ionising radiation, sharp edges, stress on cables/pipes, electric shock/burns, foreign object damage, fuel/oil/hot air leak, oxygen/hydraulic fluids, water intrusion, electrostatic discharge and lightning, loose parts, positioning of components in system/difficulty of access, any common cause events which affect the system, also all effects of normal operation, not only failures

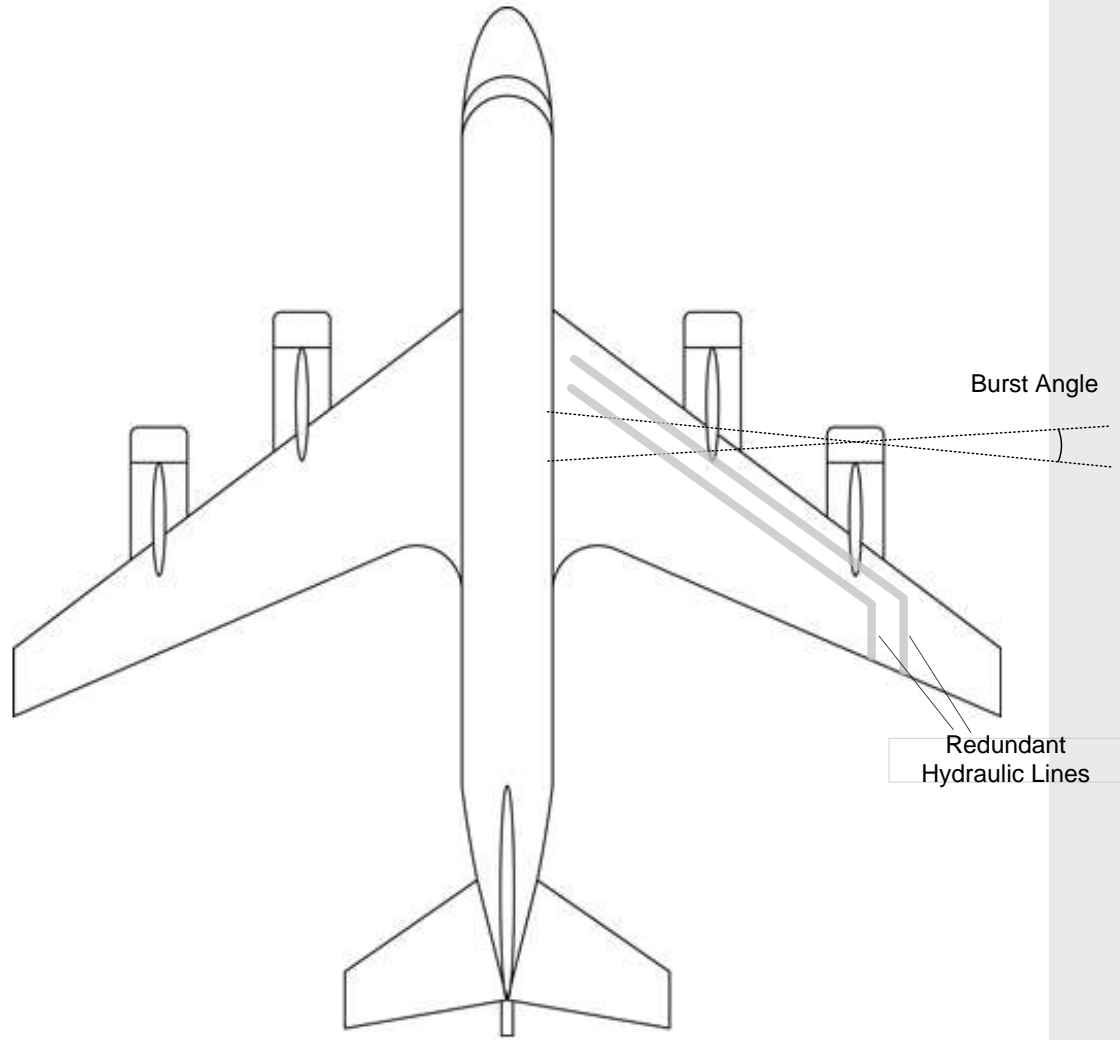


Particular Risk Assessment

- Modelling of specific risk of considered system in defined environment
- Technology/circumstance dependent
- May involve complex calculation or simulation
- Example: Fan burst
 - burst angle for fan defined
 - blade trajectory modelled
 - interaction with other aircraft systems identified, can lead to discovery of common causes



Particular Risk Assessment Example





Safety Case



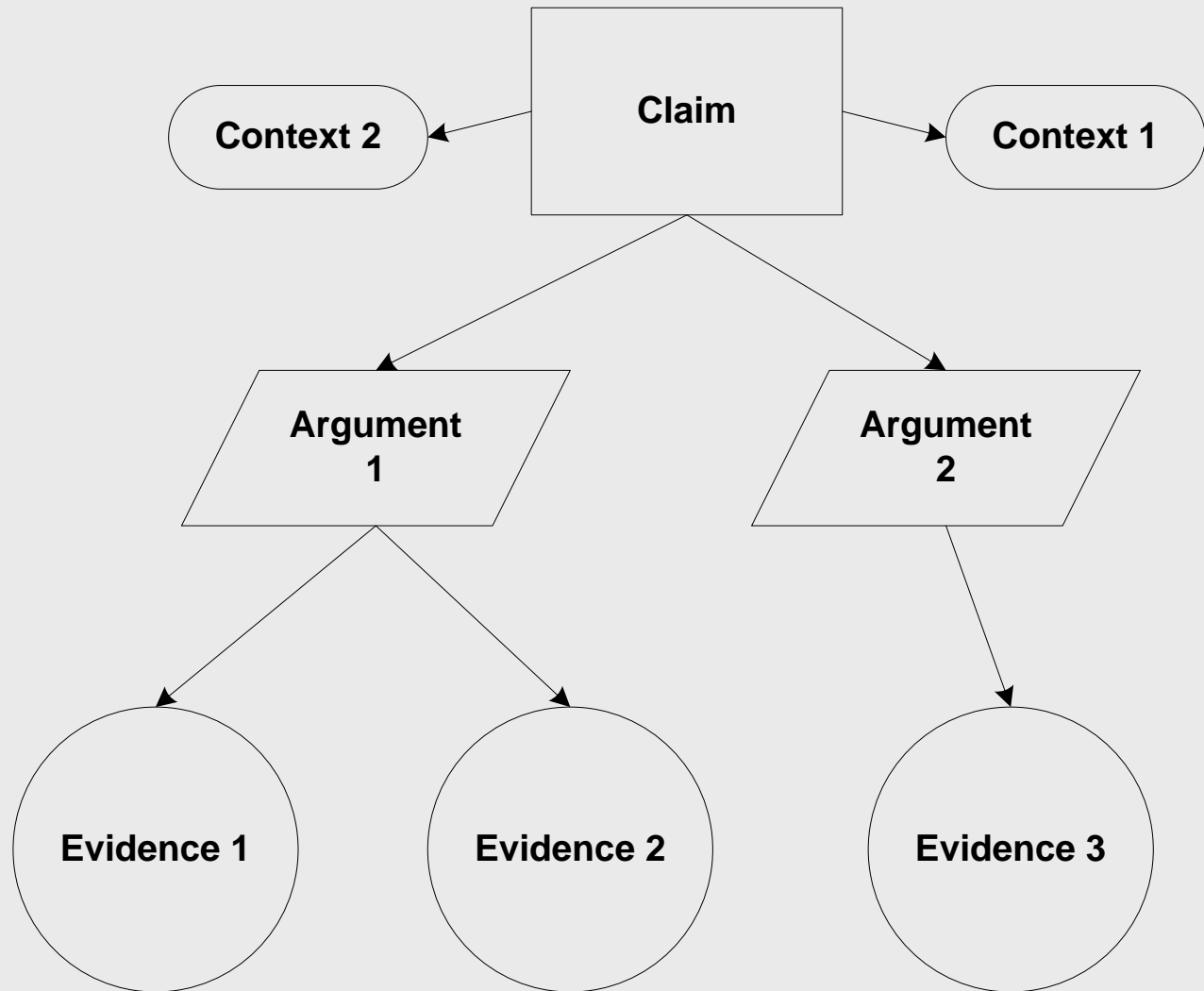


What is a Safety Case?

- Similar to a legal case
- Proves, that the system is safe for its intended use
- Conclusive argument

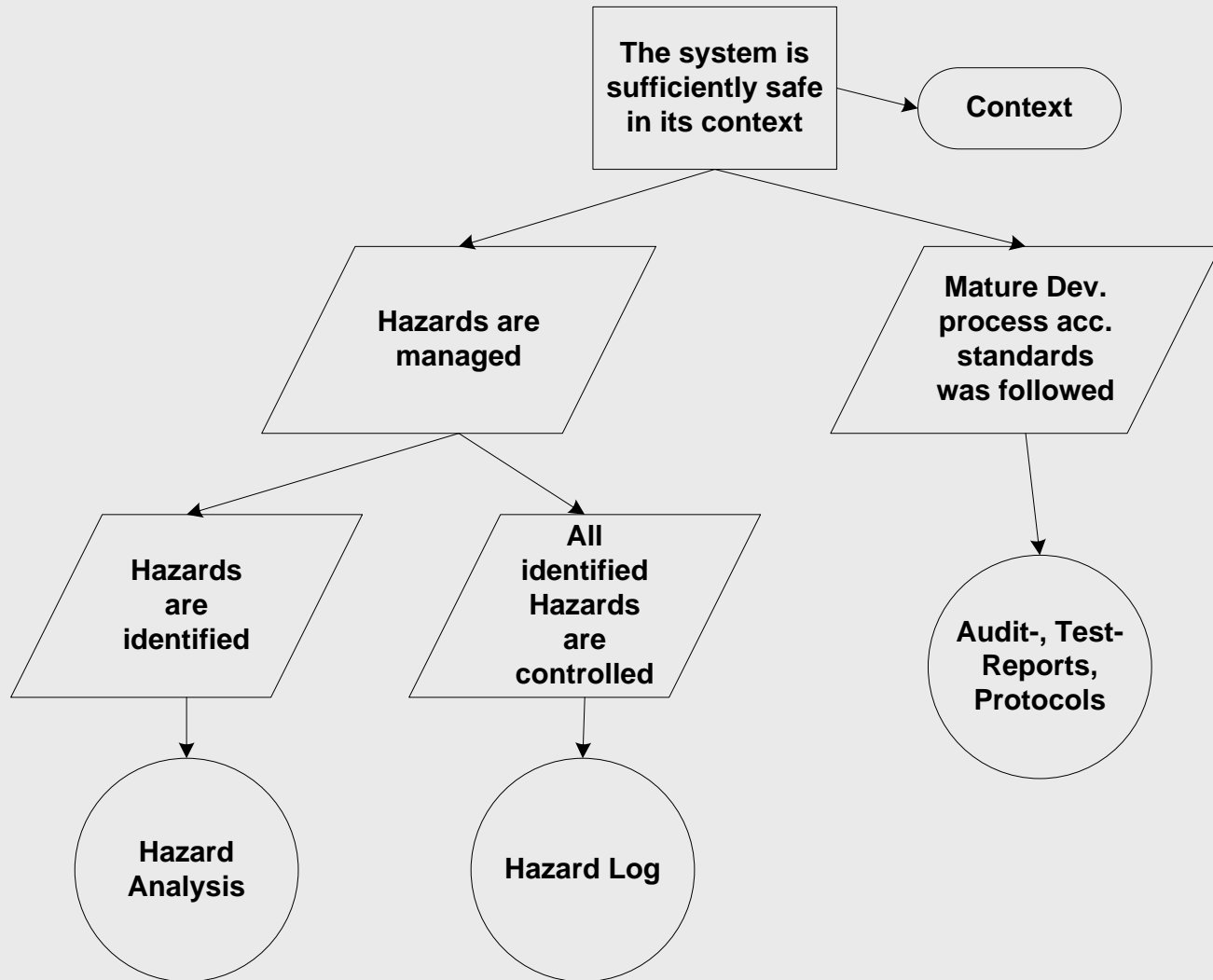


Argumentation Structure



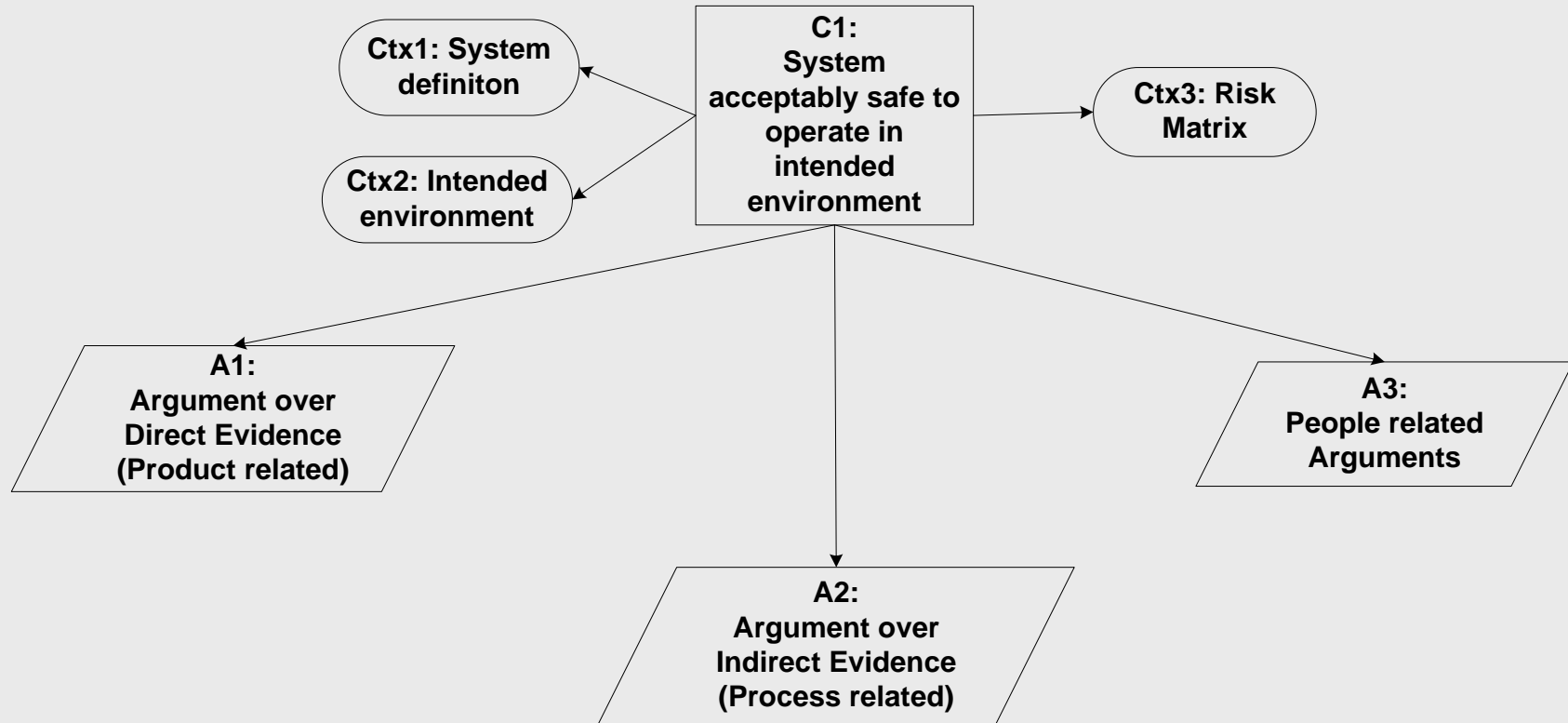


Typical Basic Structure



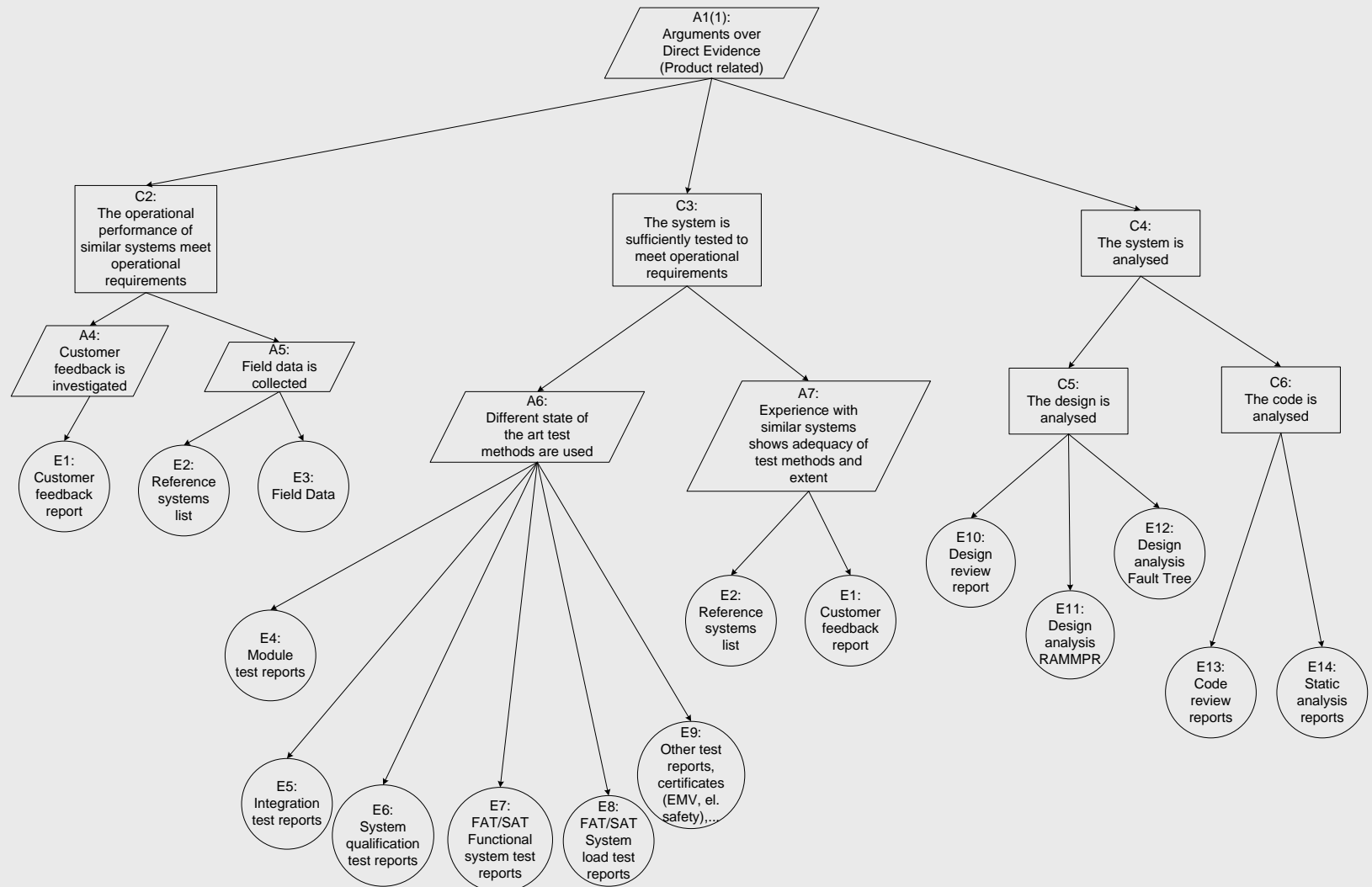


Example Top Level Structure



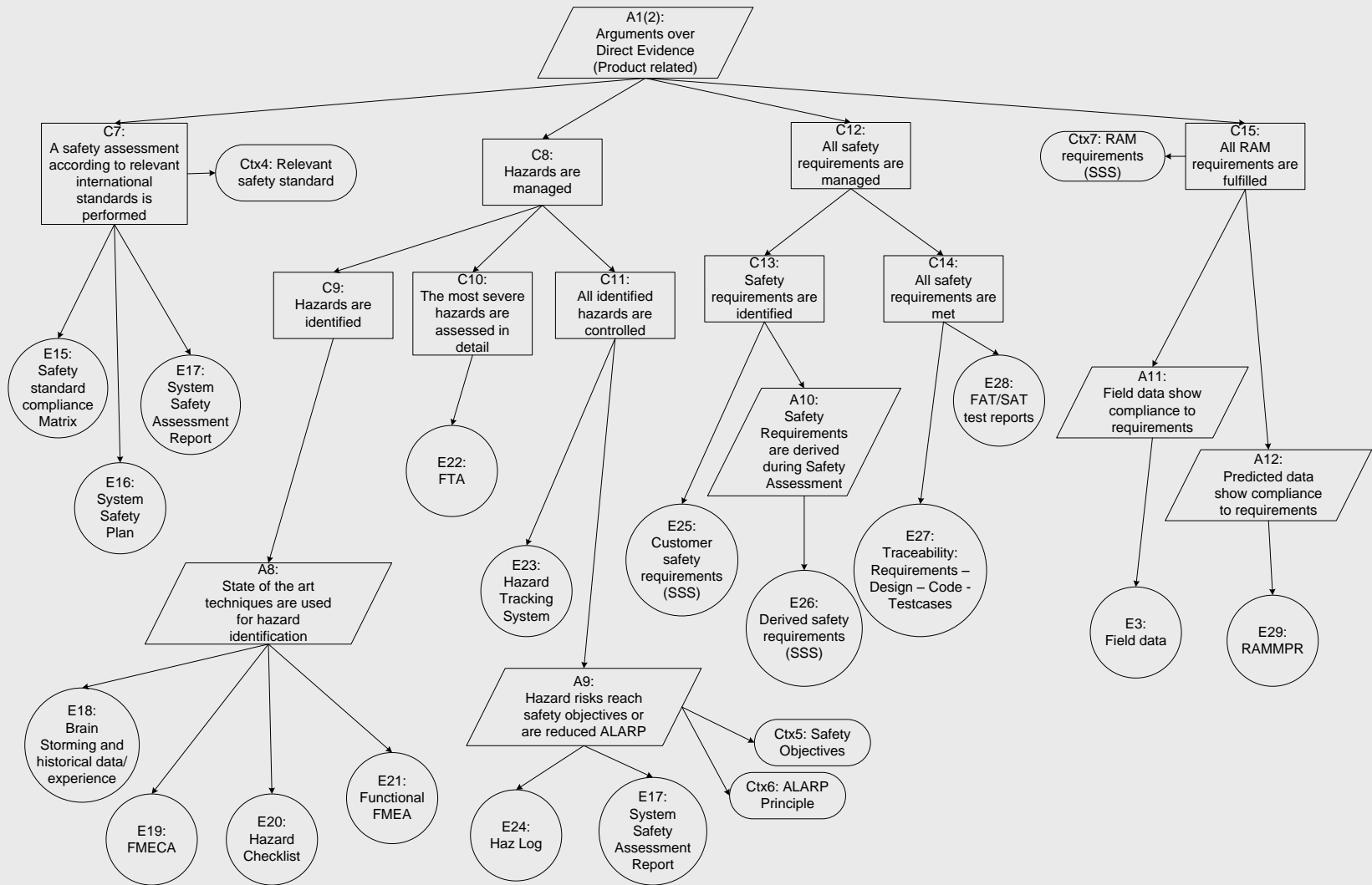


Example Detailed Structure (1)





Example Detailed Structure (2)





Sources of Evidence

- Organisational issues, safety management, competency
- The development processes
- The design
- Formal analysis
- Testing
- Simulated experience (via reliability testing)
- Prior field experience (proven in use)



Links



FREQUENTIS



Links

- The System Safety Society:
 - <http://www.system-safety.org/>
- The Aviation Safety Network:
 - <http://aviation-safety.net/index.php>
- EUROCONTROL:
 - <http://www.eurocontrol.int>
- ESARRs:
 - http://www.eurocontrol.int/src/public/standard_page/esims.html
 - http://www.eurocontrol.int/src/public/standard_page/esims_compliance_checklist.html
- Safety Assessment Methodology Level:
 - http://www.eurocontrol.int/safety/public/standard_page/SAMletter.html
- Yellow Book (Railway Safety UK):
 - <http://www.yellowbook-rail.org.uk>
- Search for and download of UK Defence Standards:
 - <http://www.dstan.mod.uk/>



Links (2)

- Safety Policy Guideline:
 - <http://www.healthandsafety.co.uk/writpolstat.html>
- Health and Safety Executive, UK:
 - <http://www.hse.gov.uk/>
- International Electrotechnical Commission (IEC)
 - <http://www.iec.ch/>
- IEC 61508
 - <http://www.iec.ch/functionalsafety/>
- NASA Safety Standards, Info:
 - <http://www.hq.nasa.gov/office/codeq/doctree/index.htm>
- US Standards:
 - <http://standards.gov>
- Dependability Information:
 - <http://www.dependability.org/>
- General Safety Information:
 - http://formalmethods.wikia.com/wiki/Safety-critical_systems



Questions, Comments?

→ Any questions? Any Comments ?

→ Please feel free to ask!



