HANDS-ON SYSTEM SAFETY BASICS, FOCUSED ON FHA
1. What is Safety?
2. Basic Definitions / Terminology
3. Safety Process and Methodologies

+ Supporting 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 1

What is System Safety all about?
Objectives

- Minimize risk of accidents
- With reasonable costs
- Systematic approach
The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.

Controlled risk and controlled error are acceptable in an inherently safe system.

No approach like this…
→ **Fly – Crash – Fix - Fly**

![Diagram](image-url)
→ Benefits

→ Saving of lives …

… and huge amounts of money

(considering lifecycles and not only the next milestone!)
Why is System Safety necessary?
Reasons

Systems used to be simple ...
Reasons

A single person could understand them completely

… but they are not any more!
Reasons

• ~ 100 microprocessor-based electronic control units
• ~ 10,000 controlled signals
• ~ 100 million lines of code
Operational Context
Systems of Systems
Systematic Approach Necessary

- Increased complexity
- Pace of technology change
- Safety relevant tasks are more and more centralised and automated
- Growing safety awareness of broad public
  - with often less personal sense of responsibility
  - resulting in more stringent product liability laws and standards/regulations

Therefore a systematic, team-based approach is necessary
...to ensure completeness and avoid omissions
Question 3

What do we need for System Safety?
What Do We Need?

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

- **Safety Culture**: awareness of all

- **Safety Management**
  - Organisation
  - Trainings / Communication / Promotion

- **Safety Engineering**
  - Hands on System Safety Work in projects
… this is near-sighted!

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

WALLY, I DISCOVERED A DEADLY SECRET FLAW IN OUR PRODUCT. WHO SHOULD I INFORM?

NO ONE. THE STOCK WOULD PLUNGE AND WE'D HAVE MASSIVE LAYOFFS. YOUR CAREER WOULD BE RUIN.

BUT INTELLIGENCE COULD COST THE DEATHS OF HUNDREDS OF CUSTOMERS. THE DOZENS ALWAYS THE HARDEST.

YOUR RISK MANAGEMENT SOFTWARE SAYS YOUR IDEA IS TOO RISKY.

WHICH ONE? WHICH ONE OF THE INPUTS.

HONESTY.
“Sorry, your mind isn't on safety. You’ll have to go out and come in again.”
Safety has to grow up with care …
…that this never happens…
Basic Definitions
What is a Hazard?

Accidents arise from hazards

Hazard

- “an accident waiting to happen”
- a condition of the platform that, unless mitigated, can develop into an accident through a sequence of normal events and actions
- ICAO: A hazard is defined as a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.

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

System Boundary
 Haz 1
 Haz m
 Haz 2
 All possible Accidents

Function 1
 Caus. Fact./ Subsys
 Mitig.
 Fail. Md 1
 Mitig.
 Fail. Md n

All Functions
 System Boundary
Failure Modes – Hazards – Accidents

Bow-Tie Diagram

- Faults
- Threats
- Control Measures
- Hazard (Top Event)
- Recovery Measures
- Effects

Controlling the threats which could release the hazard

Recovering from and/or minimising the effects of the hazard
What is Risk?

Safety Risk associated with a hazard
- Product of the probability and severity of hazard’s consequences (i.e. accidents)

Risk = Probability \times Severity

Probability
- How probable is the hazard/accident?
  - Per operation hour / during system lifetime / typical operation

Severity
- How severe is the accident?
  - Consequences on man (death, injury etc)
  - Environmental consequences (contamination, pollution, etc.)
Hazard Severity

- Hazard Severity Categories permit qualitative description of worst case credible consequences of hazard
- Below is an example definition of categories (from MIL-STD-882D)
  - usually defined either by regulatory context or through agreement with customer

<table>
<thead>
<tr>
<th>Description</th>
<th>Category</th>
<th>Environmental, Safety, and Health Result Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>I</td>
<td>Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.</td>
</tr>
<tr>
<td>Critical</td>
<td>II</td>
<td>Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.</td>
</tr>
<tr>
<td>Marginal</td>
<td>III</td>
<td>Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.</td>
</tr>
<tr>
<td>Negligible</td>
<td>IV</td>
<td>Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.</td>
</tr>
</tbody>
</table>
Hazard Probability

- Use historical results, analysis, and engineering judgement to determine appropriate qualitative probability category
- Again, particular interpretation will typically be defined by standards and/or agreed with customers

<table>
<thead>
<tr>
<th>Level</th>
<th>Probability per h</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>$P \geq 10^{-3}$</td>
<td>may occur several times a month or more often</td>
</tr>
<tr>
<td>Probable</td>
<td>$10^{-3} &gt; P \geq 10^{-4}$</td>
<td>likely to occur once a year</td>
</tr>
<tr>
<td>Occasional</td>
<td>$10^{-4} &gt; P \geq 10^{-5}$</td>
<td>likely to occur once in the life of the system</td>
</tr>
<tr>
<td>Remote</td>
<td>$10^{-5} &gt; P \geq 10^{-6}$</td>
<td>unlikely but possible to occur in the life of the system</td>
</tr>
<tr>
<td>Improbable</td>
<td>$10^{-6} &gt; P \geq 10^{-7}$</td>
<td>very unlikely to occur</td>
</tr>
<tr>
<td>Incredible</td>
<td>$10^{-7} &gt; P$</td>
<td>extremely unlikely, if not inconceivable to occur</td>
</tr>
</tbody>
</table>
### Determining Risk

- e.g. via Risk Matrix

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>CATASTROPHIC</th>
<th>CRITICAL</th>
<th>MARGINAL</th>
<th>NEGLIGIBLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>Probable</td>
<td>A</td>
<td>B</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>Occasional</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>Remote</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Improbable</td>
<td>C</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Incredible</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Class</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Intolerable</td>
</tr>
<tr>
<td>B</td>
<td>Undesirable and shall only be accepted when risk reduction is impracticable</td>
</tr>
<tr>
<td>C</td>
<td>Tolerable with the endorsement of either the Project Manager together with the internal ordering party or the Safety Director</td>
</tr>
<tr>
<td>D</td>
<td>Acceptable with the endorsement of the normal project reviews</td>
</tr>
</tbody>
</table>
## Risk Tolerability

<table>
<thead>
<tr>
<th>Hazard Probability</th>
<th>Hazard Severity</th>
<th>CATASTROPHIC</th>
<th>HAZARDOUS</th>
<th>MARGINAL</th>
<th>NEGLIGIBLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Probable</td>
<td>A</td>
<td>B</td>
<td>B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>B</td>
<td>C</td>
<td>C</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>C</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Incredible</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
</tr>
</tbody>
</table>
Risk Acceptance

Means, if there is a hazard it must be shown:

→ That the risk is so low to be considered at least “tolerable”.

→ That steps have been taken, so far as is reasonably practicable, to reduce the risk to “acceptable” level.
  (As Low As Reasonably Practicable - ALARP)
Risk Acceptance Limits

- Limits of risk acceptability/tolerability depend on
  - Customer
  - User/Operator
  - Regulator/Law/Standards
  - Society

- Decision criteria for risk acceptance / rejection
  - Absolute vs. relative risk (compare with previous, background)
  - Risk-cost trade-offs (e.g. ALARP, GALE)
  - Risk-benefit of technological options
Risk Management

- Risk underestimated
- Risk overrated

Direct and Indirect Incident Costs (Maintenance, Loss of Prestige)

Hazard Controls (Redesign, Safety Features, etc.)
Risk Reduction

**Precedence in Risk Reduction:**

1. Redesign to eliminate risk
   - Best where practicable (at a realistic cost)

2. Redesign to reduce hazard risk
   - Reduce hazard likelihood through design selection
     - E.g. duplex architecture rather than simplex
     - E.g. choose higher integrity (lower failure rate) components
   - Reduce hazard severity through design selection
     - E.g. limit size/pressure of chemical storage tanks

3. Incorporate additional mitigations
   - Safety devices
     - Automatic or other protective safety design features or devices
     - E.g. release valve to dissipate excessive pressure in vessel
     - Where applicable, provision should be made for periodic functional checks of safety devices
Precedence in Risk Reduction (cont.):

4. Provide monitoring and alarming devices
   - Used to detect the hazardous condition and to produce an adequate warning signal to alert personnel of the hazard
     - E.g. indicate that landing gear has not fully deployed
     - E.g. warning to evacuate when build up of toxic fumes

5. Develop procedures and training
   - Procedures may include the use of personal protective equipment
     - Can’t assume procedures will be followed
       - E.g. evolution of protection on power guillotines

6. Reduce risk by adding warning signs and notices
Risk Reduction

**Precedence in Risk Reduction - Example:**

“Aircraft retractable landing gear fails to extend for landing, resulting in a gear-up crash landing that causes death/injury of passengers”
Precedence in Risk Reduction - Example:

“Aircraft retractable landing gear fails to extend for landing, resulting in a gear-up crash landing that causes death/injury of passengers”

<table>
<thead>
<tr>
<th>Precedence Order</th>
<th>Method of Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eliminate Hazard</td>
<td></td>
</tr>
<tr>
<td>Reduce Hazard-Probability</td>
<td></td>
</tr>
<tr>
<td>Safety Device / Feature</td>
<td></td>
</tr>
<tr>
<td>Alarming Device</td>
<td></td>
</tr>
<tr>
<td>Procedure</td>
<td></td>
</tr>
</tbody>
</table>
Safety Process
Safety Assessment in General

Lifecycle Phase
- System Definition
- System Design
- System Implementation and Transfer to Operation
- Operation and Maintenance

Safety Assessment
- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

Objectives
- How safe does the system need to be?
- Is tolerable risk achievable with the proposed solution?
- Does the system as implemented achieve tolerable risk?
Safety Lifecycle

**Project Phases**
- Planning Phase
- System Requirements Specification
- All Design Phases
- Implementation to Disposal

**Safety Process Phases**
- Planning Phase
- Preliminary Hazard Identification (PHI)
- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

**Main Objectives of Safety Process Phase**
- Planning
  - Identification of top level Hazards
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)
- Providing evidence, that the implemented system is and remains safe

**Techniques, Tools**
- Brainstorming
- Functional FMEA (Functional Failure Analysis)
- Fault Tree Analysis (FTA)
- All previous Techniques and Tools
  - Failure Modes, Effects and Criticality Analysis (FMECA)
  - Functional FMEA

**Inputs**
- Tender, Offer including Compliance Declarations (Standards/SIL/DALs)
- Draft System Requirements
- Preliminary Hazard List
- Hazard List
- Test- and Operational Data

**Outputs**
- Draft System Design
- Hazard List
- Hazard Analysis Report
- Design Verification

**Reports, Documents**
- System Safety Plan
- Draft Hazard Log
- FHA Report
- FMECA and FTA Report, RAMMPR
- Update Haz Log, DSRs
- Safety Case Report
- Preliminary Safety Case
- SSA Report
- Compliance Report to allocated Standards/SIL/DAL
Preliminary Hazard Identification

Safety Lifecycle

Project Phases
- Planning Phase
- System Requirements Specification
- All Design Phases
- Implementation to Disposal

Safety Process Phases
- Preliminary Hazard Identification (PHI)
- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

Main Objectives of Safety Process Phase
- Planning
  - Identification of top level Hazards
- Assessment of Hazard Causes and Severities, Validation of Design Concept, Definition of Safety Objectives
- Identification of system specific hazards and causes, Verification of Design (suitable for Safety Objectives)
- Providing evidence, that the implemented system is and remains safe

Techniques, Tools
- Brainstorming
- Use of Checklists
- Use of Historical Data
- Functional FMENA (Functional Failure Analysis)
- Fault Tree Analysis (FTA)
- Reliability Block Diagram (RBD)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- Functional FMEA
- All previous Techniques and Tools

Inputs
- Tender, Offer including Compliance Declarations (Standards/SILs/DALs)
- Draft System Requirements
- Preliminary Hazard List
- Prel. Hazard Severities
- System Requirements
- Draft System Design Concept Ideas
- First Version of Hazard List
- Derived Safety Requirements: Hazard reduction/mitigation Failure rate requirements Revised SIL/DAL allocations
- Design Verification
- Safety Recommendations
- All previous Documentation
- Derived Safety Requirements
- Test- and Operational Data
- Updated Hazard List
- Evidence for safe System

Outputs
- System Safety Plan
- Draft Hazard Log
- FHA Report
- Hazard Log
- Derived Saf. Requirements => System Requirements Doc/ Hazard Log
- Compliance Report to allocated Standards/SIL/DAL
- FHA Report
- PSSA Report
- Preliminary Safety Case
- Safety Case Report
- SSA Report
- Update Haz Log, DSRs
- FMECA and FTA Report, RAMMPR

Reports, Documents
- Draft System Design
- Hazard List
- Derived Safety Requirements (DSRs) on Elements
- Test- and Operational Data
- Hazard List
- System Design
- Test- and Operational Data
- Evidence for safe System
- System Design
- Test- and Operational Data
- Evidence for safe System

© FREQUENTIS 2015
Hands-On System Safety Basics_2015.pptx
Preliminary Hazard Identification

→ Bow-Tie Diagram

Faults

Controlling the threats which could release the hazard

Threats

Hazard (Top Event)

Recovery Measures

Recovering from and/or minimising the effects of the hazard

Control Measures

Effects

Controllin

g the threats

which could release the hazard

Ph

Peff
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 / AL Allocations
Preliminary Hazard Identification

Hazards are identified by a number of means:

- Experience – Hazard Identification is usually a collation / filtering exercise on data from:
  - previous projects (review hazard logs)
  - similar systems / technologies (domain knowledge)
  - accidents / incidents (lessons learned)
  - perhaps variations for new technologies (unstable aircraft?)

- Checklists
  - comprehensive or short prompt lists
  - Note: usually prompt with causes which must be interpreted

- Brainstorming
  - expert knowledge, creative thinking
  - structured techniques such as Energy Trace & Barrier Analysis, Structured What If Technique (SWIFT)
Preliminary Hazard Identification

- Hazardous materials
  - explosives, fuels, propellants, corrosives, asphyxiants, toxic substances

- Environment
  - weather, vibration, noise, lightning, temperature

- Energy Sources
  - mechanical energy, pressure, heat, RF radiation, electrical

- Human interactions / processes
  (prompts to consider exposure, and ways humans can place system in hazardous state)
  - assembly, operation, maintenance, testing, training, life support / safety equipment
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 recorded explicitly!

Have to be evaluated and verified!
- If invalid, re-assessment of all analyses that are based on this assumption is necessary
Case Study

Go Cart - Preliminary Hazard Identification
**Hands-On System Safety Basics_2015.pptx**

**Presentation Date:** 2015-08-23

Author: W. Winkelbauer

---

**Safety Lifecycle**

**Project Phases**

- Planning Phase
- System Requirements Specification
- All Design Phases
- Implementation to Disposal

**Safety Process Phases**

- Preliminary Hazard Identification (PHI)
- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

**Main Objectives of Safety Process Phase**

- Identification of top level hazards
- Assessment of hazard causes and severities, validation of design concept
- Definition of safety objectives
- Identification of system specific hazards and causes, verification of design (suitable for safety objectives)
- Providing evidence that the implemented system is and remains safe

**Techniques, Tools**

- Brainstorming
- Use of Checklists
- Use of Historical Data
- Functional FMEA (Functional Failure Analysis)
- Fault Tree Analysis (FTA)
- Reliability Block Diagram (RBD)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- All previous Techniques and Tools

**Inputs**

- Tender, Offer including Compliance Declarations (Standards/SILs/DALs)
- Draft System Requirements
- Preliminary Hazard List
- Prel. Hazard Severities
- System Requirements
- Draft System Design Concept Ideas
- Draft System Design
- Preliminary Hazard List
- Draft System Design
- Hazard List
- Hardware List
- Derived Safety Requirements
- Test- and Operational Data
- System Design
- All previous Documentation
- Derived Safety Requirements
- Updated Hazard List
- Evidence for safe System

**Outputs**

- Plan
- Draft System Design
- Initial SIL/DAL Allocations
- Preliminary Hazard List
- First Version of Hazard List
- Derived Saf. Requirements: Hazard reduction/mitigation Failure rate requirements Revised SIL/DAL allocations
- Derived Safety Requirements
- Design Verification
- Hazard List
- Design Verification
- Hazard List
- Derived Safety Requirements (DSRs) on Elements
- Evidence for safe System

**Reports, Documents**

- System Safety Plan
- Draft Hazard Log
- Safety Recommendations
- FHA Report
- Hazard Log
- Derived Saf. Requirements -> System Requirements Doc/ Hazard Log
- Update Haz Log, DSRs
- FMECA and FTA Report, RAMMAPR
- PSSA Report
- SSA Report
- Preliminary Safety Case
- Compliance Report to allocated Standards/SIL/DAL
“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 severities

→ Mapping of failure modes to hazards, check for omissions

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

HAZOP Analysis / Functional Failure Analysis (FFA):

→ A Functional Failure Analysis (FFA) is a structured and systematic examination of a planned or existing process or system in order to identify and evaluate problems that may represent risks to personnel, equipment, the environment, or prevent efficient operation.

→ The FFA technique was initially developed to analyse chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems.

→ A FFA is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team during a set of meetings.

→ The FFA should preferably be carried out as early in the design phase as possible – to have influence on the design – and shall be repeated/completed at later stages (add mitigations).
Functional Hazard Assessment

HAZOP Analysis / Functional Failure Analysis – Process:

➔ Define system/operation to be analyzed
➔ Define all functions that will be analyzed
➔ Record assumptions/conditions
➔ Analyze failure modes for all functions using the guide-words (thereby record all mitigations required to reduce the risk of safety related failure modes)
➔ Map safety related failure modes to identified hazards and define additional hazards if required
➔ Define safety requirements and safety recommendations for the found mitigations
## Functional Hazard Assessment

<table>
<thead>
<tr>
<th>Guideword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFTER</td>
<td>The activity occurs too late in the sequence</td>
</tr>
<tr>
<td>AS WELL AS</td>
<td>An additional activity occurs</td>
</tr>
<tr>
<td>BEFORE</td>
<td>The activity occurs too early in the sequence</td>
</tr>
<tr>
<td>EARLY</td>
<td>The activity occurs earlier than expected</td>
</tr>
<tr>
<td>LATE</td>
<td>The activity occurs later than expected</td>
</tr>
<tr>
<td>LESS</td>
<td>Quantitative decrease in a parameter</td>
</tr>
<tr>
<td>MORE</td>
<td>Quantitative increase in a parameter</td>
</tr>
<tr>
<td>NO/NOT</td>
<td>Design intent is not achieved</td>
</tr>
<tr>
<td>OTHER THAN</td>
<td>Complete substitution – another activity takes place</td>
</tr>
<tr>
<td>PART OF</td>
<td>Only some of the design intention is achieved</td>
</tr>
<tr>
<td>REVERSE</td>
<td>Logical opposite of the design intention occurs</td>
</tr>
</tbody>
</table>
Functional Hazard Assessment

HAZOP Example:

- **Function**: Open power operated doors on train once train has stopped at platfform.
## Functional Hazard Assessment

<table>
<thead>
<tr>
<th>Guideword</th>
<th>Deviation</th>
<th>Cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>Doors fail to open</td>
<td>Defective mechanism</td>
<td>No passenger egress</td>
</tr>
<tr>
<td>EARLY</td>
<td>Doors open too early (train moving) or not adjacent to platfform</td>
<td>Operator error</td>
<td>Possible harm to Passengers</td>
</tr>
<tr>
<td>LESS</td>
<td>Only one door opens</td>
<td>Defective mechanism</td>
<td>Restricted passenger egress, may lead to injuries</td>
</tr>
<tr>
<td>AS WELL</td>
<td>Doors open on both sides of train</td>
<td>Failure in control circuitry</td>
<td>Possible harm to passengers if they exit the wrong door</td>
</tr>
<tr>
<td>PART OF</td>
<td>Same as less</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>OTHER THAN</td>
<td>Doors open wrong side</td>
<td>Failure in control circuitry</td>
<td>Possible harm to passengers if they exit the wrong door</td>
</tr>
</tbody>
</table>
Case Study

Go Cart – Functional Failure Analysis
Preliminary System Safety Assessment

Safety Lifecycle

Project Phases
- Planning Phase
- System Requirements Specification
- All Design Phases
- Implementation to Disposal

Safety Process Phases
- Planning Phase
  - Preliminary Hazard Identification (PHI)
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)

Main Objectives of Safety Process Phase
- Planning
  - Identification of top level hazards
  - Assessment of hazard causes and severities, validation of design concept, definition of safety objectives
  - Identification of system specific hazards and causes, verification of design (suitable for safety objectives)
  - Providing evidence, that the implemented system is and remains safe

Techniques, Tools
- Brainstorming
- Functional FMEA (Functional Failure Analysis)
- Fault Tree Analysis (FTA)
- Reliability Block Diagram (RBD)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- All previous Techniques and Tools

Inputs
- Tender, Offer including Compliance Declarations (Standards/SIL/DALs)
- Draft System Requirements
- Preliminary Hazard List
- Draft System Design Concept Ideas
- System Requirements
- Draft System Design
- Hazard List
- Derived Safety Requirements
- Draft System Requirements (DSRs) on Elements
- Use of Checklists
- Functional FMEA
- Design Verification
- All previous Documentation

Outputs
- Plan
- Preliminary Hazard List
- First Version of Hazard List
- Hazard List
- Updated Hazard List
- Design Requirements
- Hazard List
- Evidence for safe System
- Draft System Design
- Hazard Log
- Updated Hazard Log
- Derived Safety Requirements
- Design Verification
- Test- and Operational Data
- Initial SIL/DAL Allocations
- Derived SAF Requirements: Hazard reduction/mitigation Failure rate requirements Revised SIL/DAL allocations
- Safety Objectives
- Security
- Failed Test Report
- Safety Objectives
- Functional FMEA and FTA Report, RAMMPPR
- Design Verification
- Update Haz Log, DSRs
- Safety Case Report
- Preliminary Safety Case
- FHA Report
- PSSA Report
- Compliance Report to allocated Standards/SIL/DAL
“Does the proposed design reach the safety objectives?”

- Breaks down causes of hazards and functional failures
  - e.g. with Fault Tree Analysis (FTA)

- Further analyses of design
  - Reliability Block Diagrams (RBDs)
  - Hardware Failure Modes, Effect and Criticality Analysis (FMECA)
  - Interface Failure Modes and Effect Analysis (IF-FMEA)
  - Software Failure Modes and Effect Analysis (SW-FMEA)

- Can lead to further requirements, e.g. additional redundancy necessary to meet hazard target rates
Preliminary System Safety Assessment

Bow-Tie Diagram

- Faults
- Threats
- Control Measures
- Hazard (Top Event)
- Recovery Measures
- Effects

Controlling the threats which could release the hazard

Recovering from and/or minimising the effects of the hazard
Hardware FMECA

Analysis of effects of single hardware 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
Hardware FMECA

→ 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
Hardware FMECA

- **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
<table>
<thead>
<tr>
<th>ID/Item</th>
<th>Failure Mode/Faults</th>
<th>Effects of the Failure Mode</th>
<th>Failure Detection Method</th>
<th>Recovery Provisions</th>
<th>Criticality, Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWITCH 08 JIF-board</td>
<td>one JIF-A: loss or corruption of communications with SDC-A</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>Severity is none, because Switch-B is used; redundancy is reduced</td>
</tr>
<tr>
<td>SWITCH 09 ISO-Board</td>
<td>one ISO-Board-A: loss or corruption of output to associated Highway-A</td>
<td>One Highway-A out of service; Highway redundancy is reduced; no effect to user</td>
<td>all feeding JIF-A report to TMCS: ISO-A fault;</td>
<td>automatic: connected devices (EPOS, LIF, ERIF, ALIF) use all voice information from Switch-B; manual: Remove and replace ISO-Board-A</td>
<td>Severity is none, because Switch-B is used; redundancy is reduced</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID/Item</th>
<th>Failure Mode/Fault</th>
<th>Failure Rate Lambda / hours</th>
<th>Failure Mode/Item</th>
<th>Failure Predictability</th>
<th>Maintenance Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWITCH 08 JIF-board</td>
<td>one JIF-A: loss or corruption of communications with SDC-A</td>
<td>1.48311E-05</td>
<td>C[none] = 1.95</td>
<td>Intermittent failure of JIF; intermittent communication alarms from SDC and/or connected devices</td>
<td>Manual: Remove and replace JIF-Board of Switch-A</td>
</tr>
<tr>
<td>SWITCH 09 ISO-Board</td>
<td>one ISO-Board-A: loss or corruption of output to associated Highway-A</td>
<td>8.99655E-07</td>
<td>C[none] = 0.12</td>
<td>Intermittent highway alarms from JIF-A</td>
<td>Manual: Remove and replace ISO-Board-A</td>
</tr>
</tbody>
</table>
Reliability Block Diagram

- Define and describe the system
  - physical configuration and functional operation

- Model “what is necessary for success” of defined function
  - Model 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)

MTBF = 50 000h
MTTR = 0,5h
A₆ = 99,999%
Reliability Block Diagram

Failure Rate $\lambda_s$: $\lambda_s = \lambda_A + \lambda_B = \frac{MTBF_A + MTBF_B}{MTBF_A * MTBF_B}$

Repair Rate $\mu_s$: $\mu_s = \frac{MTBF_A + MTBF_B}{MTBF_A * MDT_B + MTBF_B * MDT_A + MDT_A * MDT_B}$

Availability $A_s$: $A_s = A_A * A_B$

MTBF = 25 000h
MTTR = 0,5h
$A_s = 99,998\%$
Reliability Block Diagram

Failure Rate $\lambda_p$: 
$$\lambda_p = \frac{MDT_A + MDT_B}{MTBF_A * MTBF_B + MTBF_A * MDT_B + MTBF_B * MDT_A}$$

Repair Rate $\mu_p$: 
$$\mu_p = \mu_A + \mu_B$$

Availability $A_p$: 
$$A_p = A_A + A_B - A_A A_B$$

MTBF = 2 500 000 000h
MTTR = 0,25h
$A_p = 99,99999999\%$
Reliability Block Diagram

\[
\lambda_{\text{red}} = \frac{1 - \sum_{i=k}^{n} \binom{n}{i} * A_A^i * UA_A^{n-i}) * (n - k + 1)}{MDT_A * \sum_{i=k}^{n} \binom{n}{i} * A_A^i * UA_A^{n-i}}
\]

Failure Rate \( \lambda_{\text{red}} \): 

\[
\mu_{\text{red}} = \mu_A * (n - k + 1)
\]

Repair Rate \( \mu_{\text{red}} \): 

Availability \( A_{\text{red}} \): 

\[
A_{\text{red}} = \sum_{i=k}^{n} \binom{n}{i} * A_A^i * UA_A^{n-i}
\]

MTBF = 833 333 333h
MTTR = 0,25h
A_{\text{red}} = 99,99999997%

System Part A

Item: A
Need: 1
\( \lambda(Gb) \): \( \lambda_A \)
\( \mu \): \( \mu_A \)

Need: k
of: n

Item: A
Need: 1
\( \lambda(Gb) \): \( \lambda_A \)
\( \mu \): \( \mu_A \)
Reliability Block Diagram

- Item: Phone
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \): 
- Item: Switch
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \): 
- Item: PSU
  - Need: 3
  - \( \lambda(G_b) \): 
  - \( \mu \): 
- Item: Phone
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \): 
  - a
  - b

- PSU
  - Item: Phone
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \): 
  - Item: Switch
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \): 
  - Item: PSU
  - Need: 1
  - \( \lambda(G_b) \): 
  - \( \mu \):
Operational Availability

\[ A_o = \frac{MTBF}{MTBF + MDT} \]

\[ MDT = MLDT + MTT + MTTR \]

Inherent Availability

\[ A_i = \frac{MTBF}{MTBF + MTTR} \]

<table>
<thead>
<tr>
<th>Down-Time / year</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 day</td>
<td>99,7%</td>
</tr>
<tr>
<td>1 hour</td>
<td>99,98%</td>
</tr>
<tr>
<td>1 minute</td>
<td>99,9998%</td>
</tr>
<tr>
<td>1 second</td>
<td>99,999996%</td>
</tr>
</tbody>
</table>
MTBF = 50 000h

MDT = 0.5h  Ao = 99.999%

MDT = 5h  Ao = 99.99%

MDT = 50h  Ao = 99.9%
Fault Tree Analysis

- 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 Tree Analysis

Basic Event
An initiating fault requiring no further development

Intermediate Event
An event arising from the combination of other, more basic events

Gate - AND
All input events must occur for the output to occur
\[ P = P(A) \times P(B) \]

Gate - OR
The occurrence of one or more input events will cause the output to occur
\[ P = P(A) + P(B) - P(A) \times P(B) \]
Fault Tree Analysis

- Emergency power supply
- Main power supply
- Main water supply
- Nozzle
- Pump
- Smoke detector

Fire protection system fails

- Deluge system fails
- Fire detection fails

- Smoke detector failure
- No water in pipe
- Nozzle blocked

1
Fault Tree Analysis

- Emergency power supply
- Main power supply
- Main water supply
- Nozzle
- Pump
- Smoke detector
- No water in pipe
  - Pump does not work
    - No main water supply
    - No power supply
      - Pump failure
    - Emergency power supply outage
    - Main power supply outage
Case Study

Fault Tree Analysis
Frequent assumption: Failures are independent.
- May be subverted by systematic errors/interference/coupling i.e. Common Cause Failure

Definition of Common Cause Failure
- “A failure of two or more components, systems, or structures due to a single specific event or cause.”
- “Common cause failures are defined as that cutset of dependent failures for which causes are not explicitly included in the logic model as basic events.”

Approaches to Mitigation
- Diversity, Separation, Checks and Tests,
- thorough Analysis (FTA, RBD)
- dedicated Common Cause Analysis
→ Common Cause Analysis

→ Consider a redundant system. Both components of the system must fail before the system does fail.

→ If each of the components has a failure rate of $10^{-4}$ per hour and the failures are completely independent then the overall system would have a failure rate of $10^{-8}$ per hour.

→ However if just 1% of the failures are common cause failures then the failure rate rises to $10^{-6}$ per hour.

Common cause failure modes tend to dominate highly reliable systems!
→ Common Cause Analysis

→ 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

- 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
  - Identification of affected system parts/areas
  - Recording of observations and conclusions
Common Cause Analysis - Example

- Burst Angle
- Redundant Hydraulic Lines
- Burst angle
- Hydraulics
Consequence Analysis

Bow-Tie Diagram

- Faults
- Threats
- Control Measures
- Hazard (Top Event)
- Recovery Measures
- Effects

Controlling the threats which could release the hazard

Recovering from and/or minimising the effects of the hazard
Consequence Analysis

Purpose
- To determine the intermediate conditions and final consequences arising from the identified hazards

Approach
- Diagrammatic representation
- Quantitative estimate of probabilities

Techniques
- Cause Consequence Diagrams
- Event Trees
Consequence Analysis

The causes and consequences of operational errors are not linear in their magnitude.

Source: Dedale
Consequence Analysis

Cause Consequence Diagram (CCD):

- Ignition
  - Sprinkler Works
    - Fire Put Out
      - YES: 0.9
      - NO: 0.1
    - Minor Fire
      - YES: 0.9
      - NO: 0.1
    - Major Fire
      - YES: 0.09
      - NO: 0.01
  - Alarm Sounds
    - YES: 0.9
    - NO: 0.1

© FREQUENTIS 2015
Hands-On System Safety Basics_2015.pptx
Page: 85
Presentation Date: 2015-08-23
Author: W. Winkelbauer
Methods - Limitations

- All techniques have their limitations due to
  - representation → abstraction of real system that is “good-enough” is hard to find
  - data availability and accuracy
  - analysis is based on incomplete model of the system
    E.g. mechanical engineering drawings - they show how a system is constructed, but not what it does

- Important to respect limitations of techniques because
  - inappropriate use of techniques produces inaccurate results

- Analyses can identify sets of potential hazards, failure sequences and accident sequences, but they are only as good as domain knowledge, engineering knowledge, creativity, ... of participants!
Safety Lifecycle

Project Phases
- Planning Phase
- System Requirements Specification
- All Design Phases
- Implementation to Disposal

Safety Process Phases
- Preliminary Hazard Identification (PHI)
- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

Main Objectives of Safety Process Phase
- Planning
  - Identification of top level Hazards
  - Assessment of Hazard Causes and Severities, Validation of Design Concept, Definition of Safety Objectives
  - Identification of system specific hazards and causes, Verification of Design (suitable for Safety Objectives)
  - Providing evidence, that the implemented system is and remains safe

Techniques, Tools
- Brainstorming
- Use of Checklists
- Use of Historical Data
- Functional FMEA (Functional Failure Analysis)
- Fault Tree Analysis (FTA)
- Reliability Block Diagram (RBD)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- All previous Techniques and Tools
- System Design
- All previous Documentation
- Derived Safety Requirements
- Test- and Operational Data
- Updated Hazard List
- Evidence for safe System

Inputs
- Tender, Offer including Compliance Declarations (Standards/SILs/DALs)
- Draft System Requirements
- Preliminary Hazard List
- Draft System Design
- Initial SIL/DAL Allocations

Outputs
- Plan
- Preliminary Hazard List
- First Version of Hazard List
- Derived Saf. Requirements: Hazard reduction/mitigation
- Derived Saf. Requirements (DSRs) on Elements
- Safety Recommendations
- Hazard Log
- Design Verification
- System Safety Plan
- Draft Hazard Log
- FHA Report
- Hazard Log
- Derived Saf. Requirements: Hazard reduction/mitigation
- Compliance Report to allocated Standards/SIL/DAL

Reports, Documents
- FHA Report
- PSSA Report
- Preliminary Safety Case
- SSA Report
- Update Haz Log, DSRs
- FMECA and FTA Report, RAMMPR
- Safety Case Report
- Compliance Report to allocated Standards/SIL/DAL
System Safety Assessment (SSA)

“Does the system as implemented achieve tolerable Risk?”

→ Update of all previously performed analyses
→ Verification, whether assumptions are still valid and all safety targets and safety requirements are met
→ Production of a safety case or safety assessment report
→ Transition to operation and maintenance
→ Maintenance of safety case
What is a Safety Case?

- Similar to a legal case
- Proves, that the system is safe for its intended use
- Provides conclusive argument
Goal Structuring Notation

Graphical argumentation notation

Can be used to explicitly document
- the elements of any argument (claims, evidence and context) and
- the relationships that exist between them.

Presents, how goals are supported by sub-goals
- sub-goals supported by subsequent supporting goals.

Supporting evidence documented via so called “solution”
Goal Structuring Notation

A **goal** presents a claim forming part of the argument.

A **strategy** describes the nature of the inference that exists between one or more goals and another goal.

A **solution** presents a reference to evidence items.

A **context** presents a contextual artefact. This can be a reference to contextual information or statement.
Goal Structuring Notation

A justification presents a statement of rationale.

An assumption presents an intentionally unsubstantiated statement.

Undeveloped entity indicates that a line of argument has not been developed. It can apply to goals and strategies.

Supported by declares an inferential or evidential relationship.

In context of declares a contextual relationship.
Example

C1 Press Design

C2 Press Operation

G1 Press is acceptably safe to operate within Whatford Plant

C3 Whatford Plant

C4 Risk Matrix

C5 Identified hazards

S1 Argument by addressing all identified hazards

S2 Argument of compliance with applicable safety standards & regulations

C6 Applicable standards & regulations

G2 Hazard of “Operator hands trapped by press plunger” is mitigated

G3 Hazard of “Operator hands trapped by press drive machinery” is mitigated

G4 Hazard of “Operator upper body trapped by press drive machinery” is mitigated
Example

G3
Hazard of “Operator Hands” trapped by press drive machinery is mitigated

G5
Motor / Clutch / Drive Belts surrounded with safety cage

G6
Press operation will halt if safety cage tampered with

Sn1
Press Design (Safety Cage)
Typical Top Level Structure

- **C1** System definition
- **C2** Intended environment
- **G1** System is acceptably safe to operate in intended environment
- **C3** Risk Matrix
- **S1** Argument over direct evidence (Product related)
- **S2** Argument over indirect evidence (Process related)
- **S3** People related arguments.
Process Overview

Step 1
Identify goals to be supported

Step 2
Define basis on which goals stated

Step 3
Identify strategy to support goals

Step 4
Define basis on which strategy stated

Step 5
Elaborate strategy

Step 6
Identify Basic Solution
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
Links

→ The System Safety Society:
  - http://www.system-safety.org/

→ The Aviation Safety Network:

→ EUROCONTROL:
  - http://www.eurocontrol.int

→ Safety Assessment Methodology Level:
  - https://www.eurocontrol.int/articles/safety-assessment-methodology-sam

→ UK Defence Standards (registration necessary):
  - http://www.dstan.mod.uk/
Links (2)

- Health and Safety Executive, UK:

- International Electrotechnical Commission (IEC)
  - [http://www.iec.ch/](http://www.iec.ch/)

- IEC 61508
  - [http://www.iec.ch/functionalsafety/](http://www.iec.ch/functionalsafety/)

- NASA Safety Standards, Info:

- US Standards:
  - [http://standards.gov](http://standards.gov)

- Dependability Information:
  - [http://www.dependability.org/](http://www.dependability.org/)
Thank you for your attention!