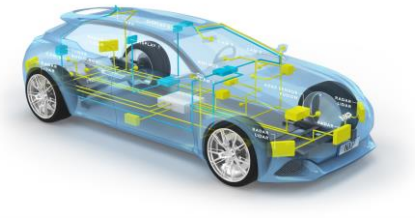
Hazard Analyses for Assessing System Safety

SLIDES: HTTPS://WWW.STEFAN-WINTER.NET/APPLICATION-MATERIALS/

System Safety



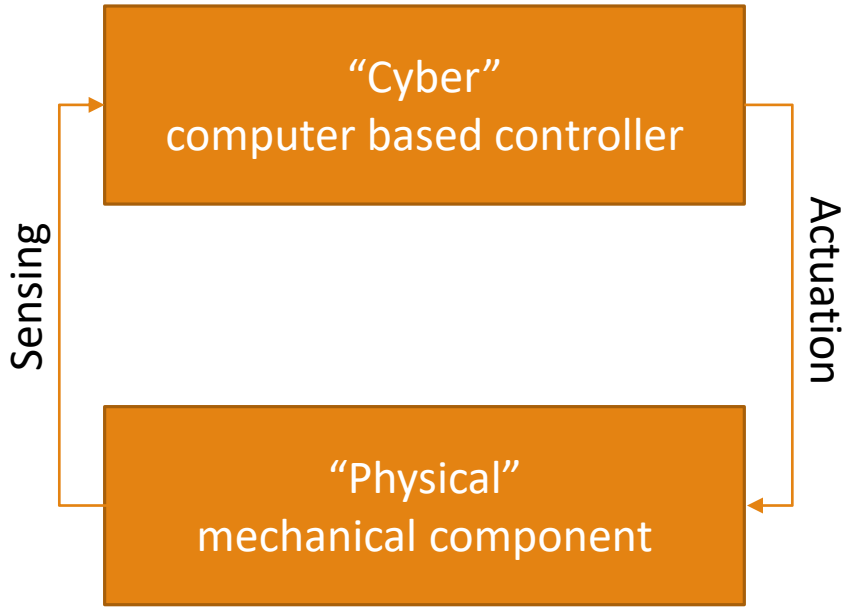
System: set of interrelated components working together toward some common objective

- technical and socio-technical systems

Safety: absence of unacceptable risk

Risk: severity of hazardous events x exposure to hazardous events

Hazard: condition with potential for injury, illness, environmental damage, financial loss



Safety is a System Property

Systems can be unsafe, even when each component works as intended.

Engineering Safe Systems: Hazard Control

Hazard analysis (know your enemy)

Objectives:

- Identify hazards arising from system operation
- Identify causes leading to hazards in system operation
- Determine risks associated with identified hazards

Methods:

- Fault tree analysis (FTA)
- Failure mode and effects analysis (FMEA)
- 5 Whys
- Hazard and operability analysis (HAZOP)
- Why-Because Analysis (WBA)
- System Theoretic Process Analysis (STPA)

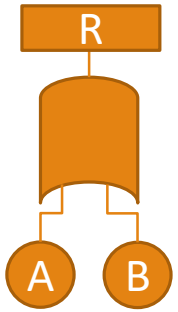
Fault-Tree Analysis (FTA)

Model elements:

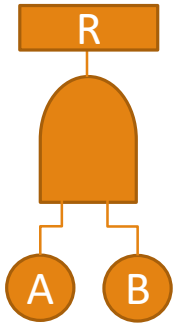
- Hazard as root node 

- Causal factors as leafs 

- Logic gates to relate safety violation to causal factors

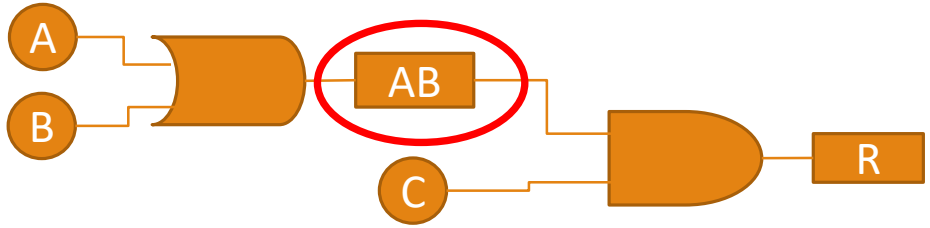


Logic inclusive OR: A=T => R=T
B=T => R=T
else R=F



Logic AND: A=F => R=F
B=F => R=F
else R=T

- Nesting with intermediate conditions



FTA Example: Car Engine Catching Fire

Root node: Engine catching fire

Prerequisites for fire:

- Fuel
- Oxygene
- Ignition

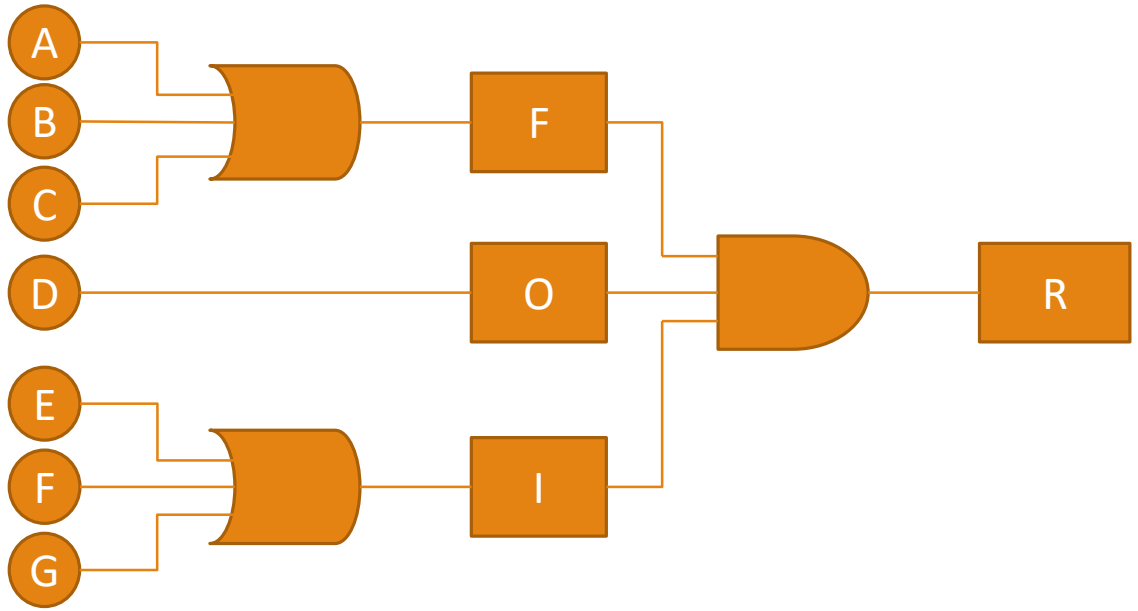
Cause for oxygene: Atmosphere D

Causes for fuel in engine proximity:

- Injector leak A
- Fuel line leak B
- Oil spill C

Causes for ignition:

- Overcurrent protection failure E
- Component surface overheat F
- Mechanical sparks G



Using FTA we found:
9 hazardous cause-event chains (e.g. oil spill plus mechanical sparks plus being in the earth atmosphere)

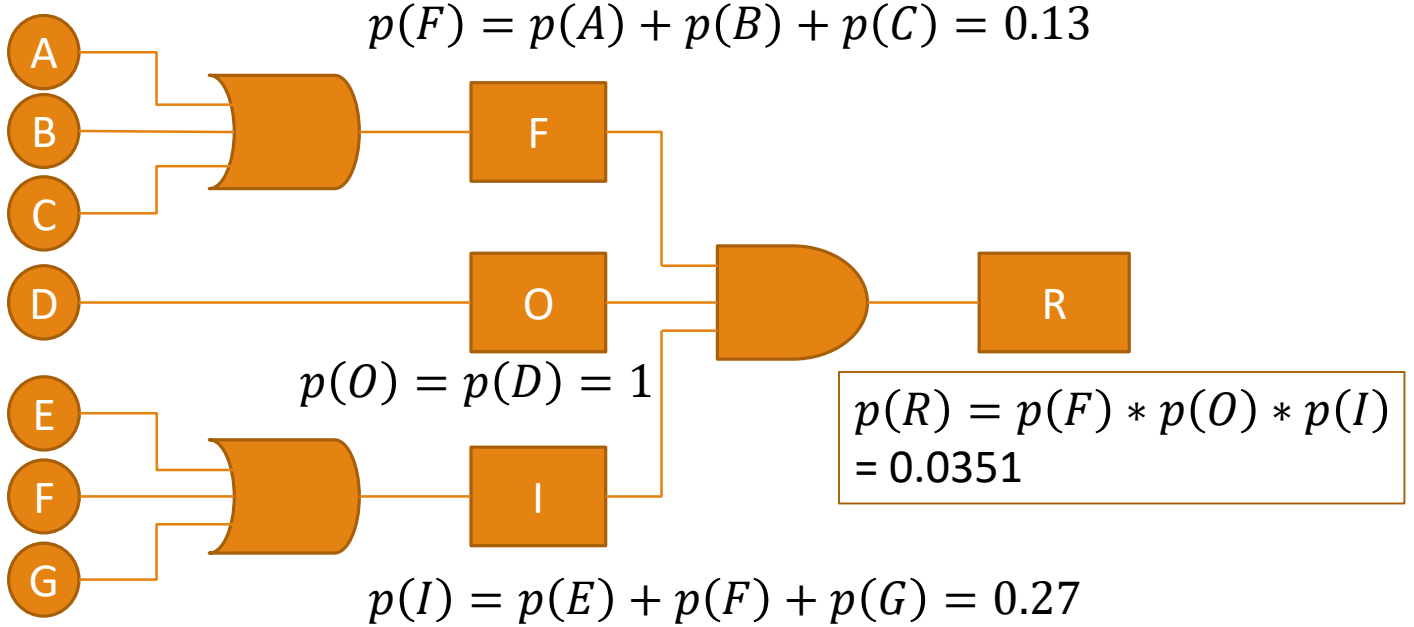
What about risks?

FTA Example with Probabilities

Cause for oxygene: Atmosphere (D)
- Probability of occurrence: 1

Causes for fuel in engine proximity:
- Prob. of injector leak: 0.01 (A)
- Prob. of fuel line leak: 0.02 (B)
- Prob. of oil spill: 0.1 (C)

Causes for ignition:
- Prob. of overcurrent protection failure: 0.02 (E)
- Prob. of component surface overheat: 0.05 (F)
- Prob. of mechanical sparks: 0.2 (G)



FTA Conclusions

Top-down approach to Hazard Analysis: Requires hazard hypothesis

Pro:

- Simple, logical model with simple risk calculation
- No need to consider all types of component failures
- Software support available (e.g., CAFTA, SAPHIRE, Riskspectrum, …)

Con:

- Tree structures become complex quickly
- Intractable without tool support

Failure Modes and Effects Analysis (FMEA)

Model elements:

- System components (technical and human)
- Components‘ functional specifications
- Component interactions

Analysis procedure:

- For each component, identify all possible failure modes (assuming all other system components are functional)
- For each identified failure mode, identify
  - possible causes
  - possible effects
  - failure mode severity

FMEA Example

System: Fire alarm system

Components: Control panel, smoke detectors,
manual call panel, sirens, LED indicators

Component	Failure Modes	Possible causes	Effects	Severity S (1-5)
LED indicator	LED on when fire alarm off	Incorrect junction	False impression of protection	4 (critical)
	LED off when fire alarm on	Incorrect junction, defective LED	False impression of system failure	1 (very minor)
	Electric fire	Defective/wrong voltage transformer, improper heat sink, high resistance connections	Smoke and fire in surrounding area	5 (catastrophic)

FMEA: Risk Quantification

Risk Priority Number $RPN = S * O * D$

- Severity S (higher -> worse)
- Occurrence O (higher -> worse)
- Detectability D (higher -> worse), factors in fault tolerance measures in the system

Failure Modes	Possible causes	Effects	Severity S (1-5)	Occurrence O (1-5)	Detectability D (1-5)	RPN
LED on when fire alarm off	Incorrect junction	False impression of protection	4	1	4	16
LED off when fire alarm on	Incorrect junction, defective LED	False impression of system failure	1	2	1	2
Electric fire	Defective/wrong voltage transformer, improper heat sink, high resistance connections	Smoke and fire in surrounding area	5	1	3	15

FMEA Progression

Iterative progression of analysis:

- Components: Control panel, smoke detector, manual call panel, siren
- Subsystems: Control panels + LED indicator, control panel + smoke detector, …
- System

FMEA Conclusions

Bottom-up approach to Hazard Analysis: Requires failure mode hypothesis

Pro:

- No a-priori knowledge/assumption of hazard required
- Analyzes hazards along with other quality aspects
- Supports qualitative and quantitative risk assessment
- Tool support available (e.g. Reliability Workbench, Xfmea)

Con:

- Not targeted for safety-relevant failures
- Can induce extreme overheads for complex systems

Summary

1. What is system safety? Can it be ensured at the component level?
2. What are hazards?
3. What are the pros and cons of the FTA and FME(C)A analyses and what is their fundamental difference?
4. You are entrusted with the creation of a coffee machine for the ISS. You are a bit nervous, because you haven't worked on space projects before, but all other vendors had to decline, because their expert staff is affected by a global scale pandemic. Which hazard analysis technique would you use and why?

Further reading:

Nicholas Bahr: "System Safety Engineering and Risk Assessment: A Practical Approach", Taylor & Francis

Nancy Leveson: "Engineering a Safer World", MIT Press