Safety Frameworks for Self Driving

Module 3, Lesson 3

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

In this lesson, we will cover

- Generic Safety Frameworks
  - Fault Trees, FMEA, HAZOP
- Autonomous/Automotive Safety Frameworks
  - Functional Safety, Safety of Intended Functionality

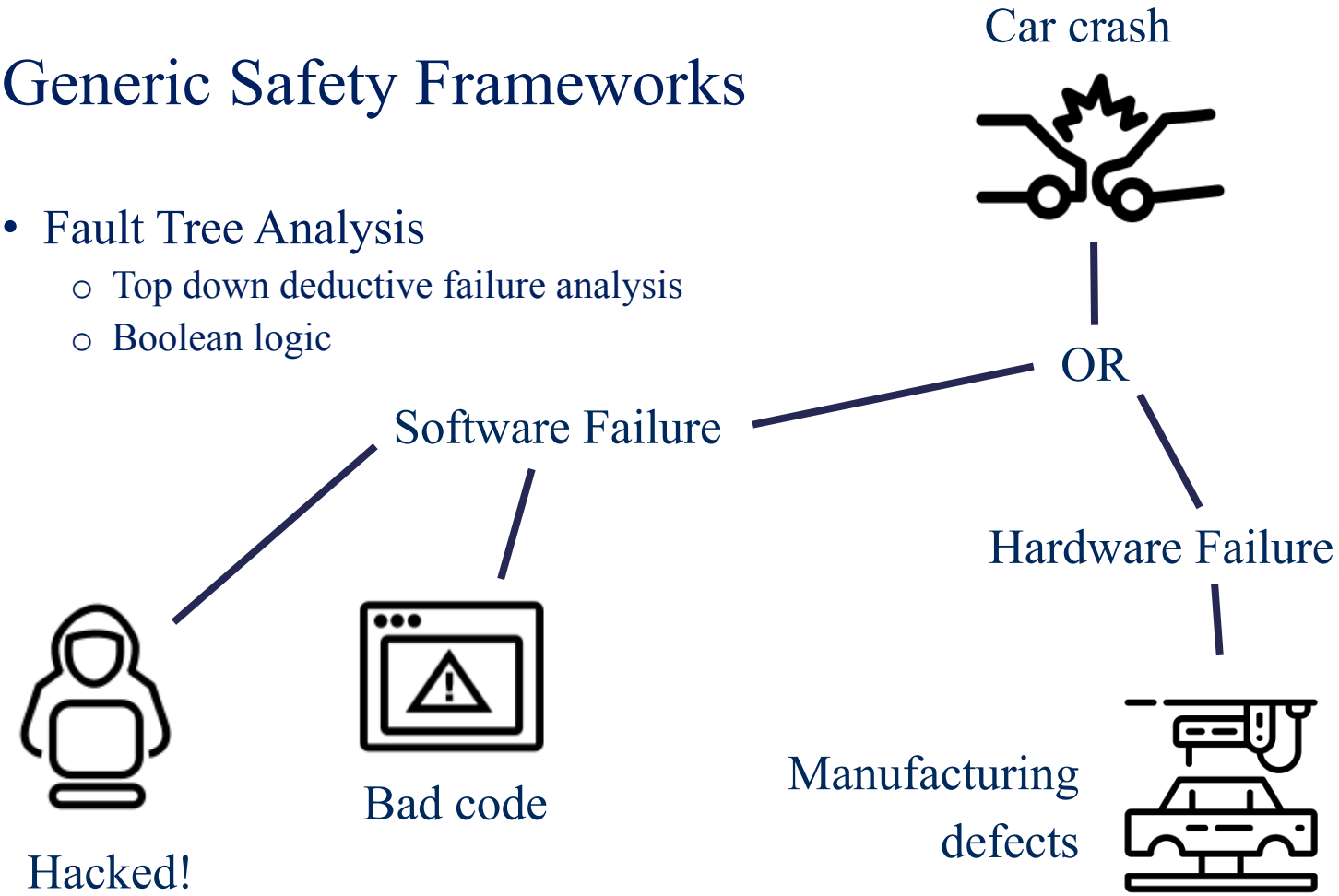
In this lesson, we will cover

- **Generic Safety Frameworks**
  - **Fault Trees, FMEA, HAZOP**

- Autonomous/Automotive Safety Frameworks
  - Functional Safety, Safety of Intended Functionality

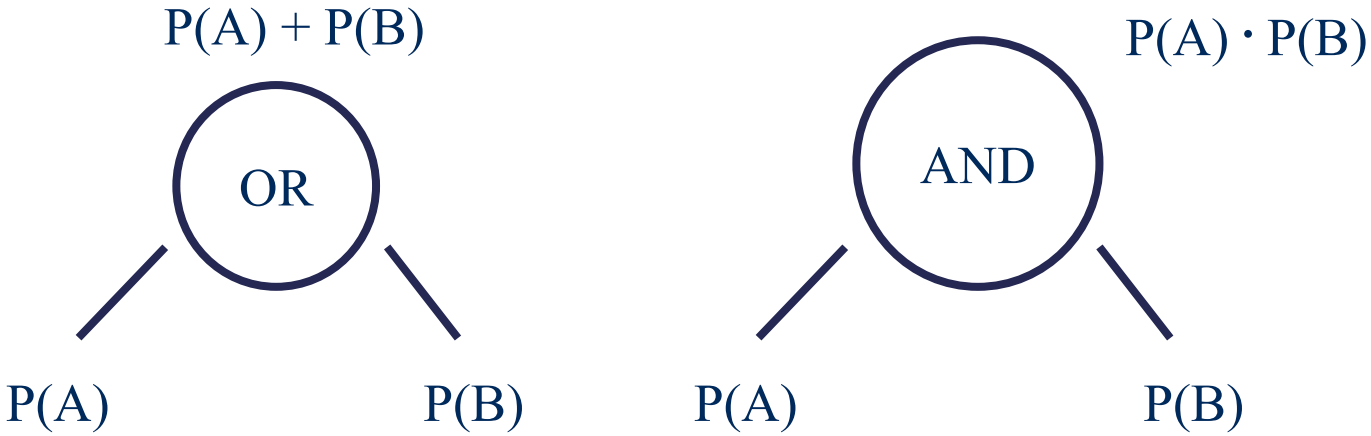
Generic Safety Frameworks

- Fault Tree Analysis
  - Top down deductive failure analysis
  - Boolean logic



Probabilistic Fault Tree Analysis

- Assign probabilities to fault “leaves”
- Use logic gates to construct failure tree



Failure Mode and Effects Analyses (FMEA)

- Bottom up process to identify all the effects of faults in a system

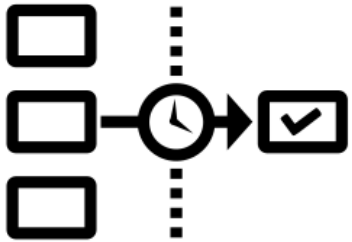
- **Failure Mode**
  Modes or ways in which a component of the system may fail

- **Effects Analysis**
  Analyzing effects of the failure modes on the operation of the system

FMEA: Idea

- Categorize failure modes by priority
  - How serious are their effects?
  - How frequently do they happen?
  - How easily can they be detected?

- Eliminate or reduce failures, starting with top priority



FMEA: Steps

1

Discuss with field experts

Create FMEA table

2

List **failure modes**

3

For each **failure mode**

identify **effects**

Severity? (S)

4

For each **root cause**

Occurrence? (O)

5

For each **prevention method**

Detection? (D)

6

RPN = S · O · D

FMEA: Example

- Consider following failure mode
  - System encounters gravel, controller failure
    - Severity: physical crash (S=10)
    - Occurrence: whenever construction encountered, out of ODD, so somewhat likely (O=4)
    - Detection: can check status monitor to identify if this happens with certainty (D=10)
    - Risk priority number (RPN) = 10x4x10 = 400

FMEA: Example

- Similarly there could be other failure modes, for example:
  - Sign perception failure (RPN = 100)
  - GPS synchronization failure (RPN=300)
  - Incorrect motion prediction (RPN=150)

- Final RPN List:
  - Control failure
  - GPS failure
  - Motion prediction
  - Sign perception

HAZOP – a variation on FMEA

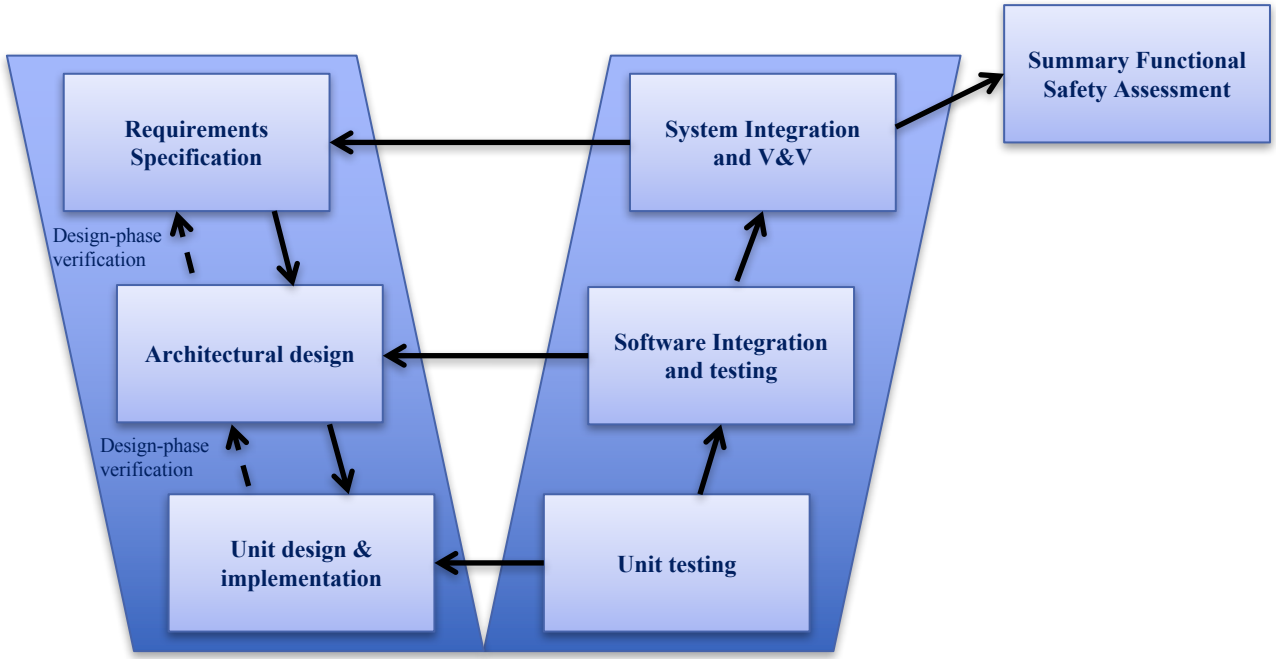
- Hazard and operability study (HAZOP)
- Qualitative brainstorming process, needs “imagination”
- Uses guide words to trigger brainstorming (not, more, less etc.)
- Applied to complex 'processes'
  - Sufficient design information is available, and not likely to change significantly

Automotive Safety Frameworks

- ISO 26262 - Functional Safety Standard
- ISO/PAR 21448.1 – Safety of Intended Functionality

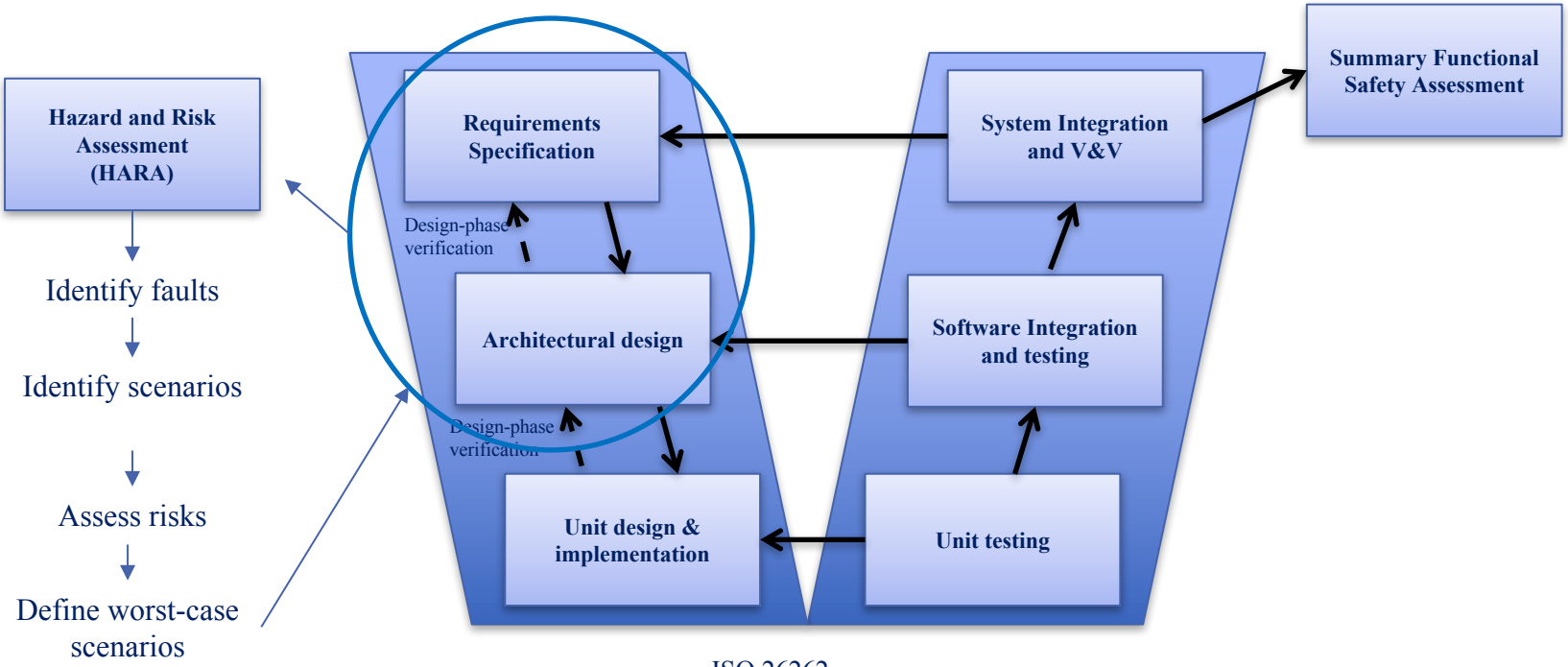
- Functional Safety is defined as:
  - safety due to absence of unreasonable risk
  - only concerned about malfunctioning system
- ISO 26262 defines Automotive Safety Integrity Levels (ASIL)
  - ASIL-D most stringent, ASIL-A least stringent

Functional Safety Process



ISO 26262

Functional Safety Process



ISO 26262

Safety of the Intended Functionality (SOTIF)

- ISO/PAS 21448.1
- Failures due to performance limitations and misuse
  - Sensor limitations
  - Algorithm failures / insufficiencies
  - User misuse – overload, confusion

- Designed for level 0-2 autonomy
- Extension of FuSa
  - V-shaped process
  - Employs HARA

Summary

- Simple analytic frameworks
  - fault trees and probabilistic fault trees
  - Failure modes and effects analysis

- Functional safety frameworks
  - FuSa HARA - safety requirements through risk analysis
  - SOTIF – behavior risk assessment

Module Summary

- Motivation for safety
- Formal definitions for safety concepts
- NHTSA safety recommendations, 2017
- Waymo and GM safety perspectives
- Analytical and data-driven assessment
- Common safety assessment frameworks

Extra

HAZOP: Steps

1 **Define** goals, scope

2 **Prepare**

Template for study outputs?

Guide words?

3 **Examine**

deviations, effects, causes, mitigation

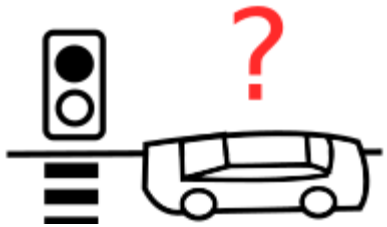
4 **Document**

Implement, follow up

SOTIF: Terms

- Situation Catalog
  - list of all possible situations in our ODD
  - each situation has
    - risk level: normal, near crash, crash
    - demand (or attentiveness): low, medium, high, very high, extreme

- **ORBAP**
  - on road behaviors and performance



SOTIF: Process

(risk analysis)

1 identify requirements

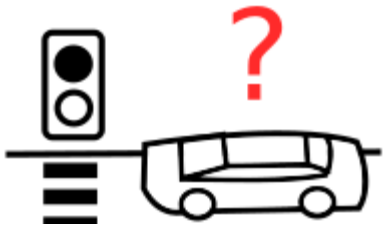
2 ORBAP analysis

3 ORBAP improvement

“situation catalog”

high level requirements

mission requirements



situation analysis

environmental conditions

STPA

- System Theoretic Process Analysis
- hazard analysis technique, very similar to SOTIF
- key insight: accidents happen because of bad control!

1 identify safety requirements

possible accidents?

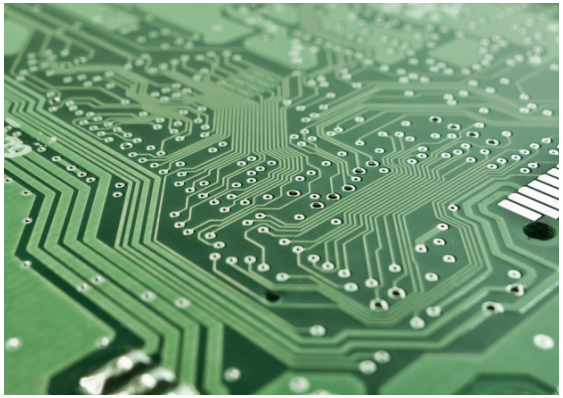
2 identify hazardous actions

3 **for each** hazardous action

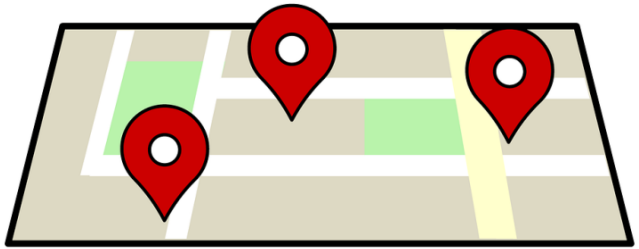
cause?

mitigation measures?

STPA: Example



- cause - controllers don’t work because of bad GPS synchronization, etc
- mitigation measures - automatically disable automation and ask for driver control if sync not working, etc
- degradation over time - perform mandatory board check every year and replace if needed, etc

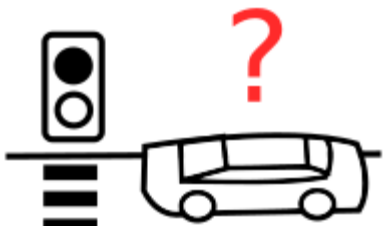


FuSa: HARA Steps

1

identify functional faults

situation catalog? 2



choose situations to address

3

risk assessment

4

results and worst case scenarios

verify?

5

construct **safety requirements**