SafetyLens: Visual Data Analysis of Functional Safety of Vehicles

Arpit Narechania
anarechania3@gatech.edu

Ahsan Qamar
aqamar2@ford.com

Alex Endert
endert@gatech.edu

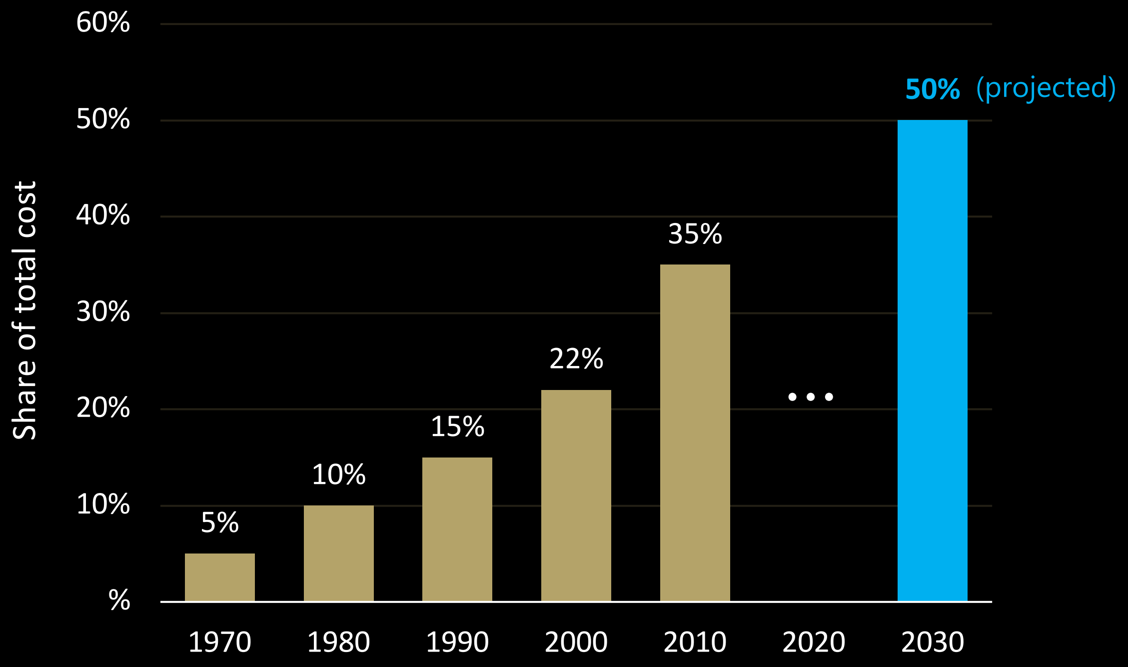
Vehicles - complex electronic and software systems

Lane Change Assist

Adaptive Cruise Control

Parking Assist

Cost of electronics as a percentage of the total cost of an automobile.



Source: I. Wagner, "Automotive electronics cost as a percentage of total car cost worldwide from 1950 to 2030", 2019, Statista.com.

Vehicle safety is important.

2018, United States

6.7M
Vehicle crashes

- **0.6%** Fatalities
- **28%** Injuries
- **71.4%** Damages to Property

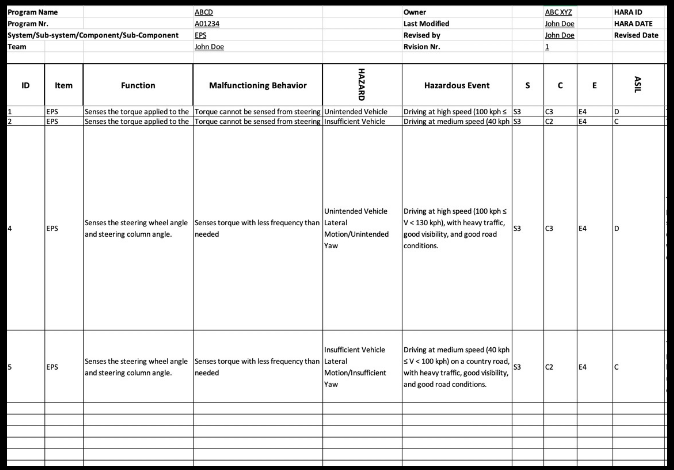
914
Vehicle Recalls

- **29.3M** # Vehicles
- **$20B+** Total Cost

Sources:
National Statistics, 2019, Traffic Safety Facts Annual Report Tables, National Highway Traffic Safety Administration, U.S,
https://www.automotive-fleet.com/329104/recalls-rise-13-affected-vehicles-fall-in-2018.

Automotive Systems Engineering & VIS

Automotive systems engineering processes involve large amounts of data in

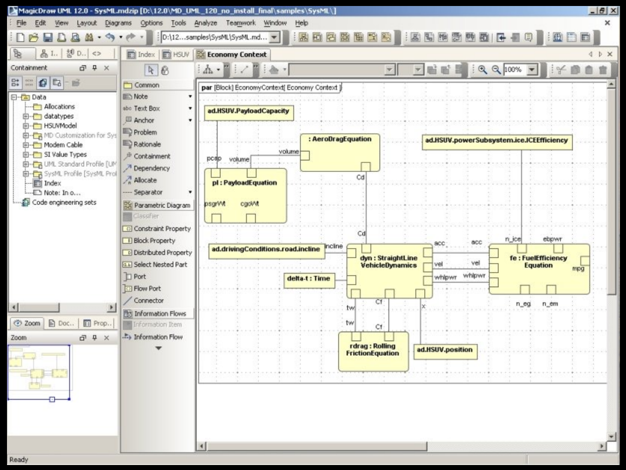


Program Name	ABCD	Owner	ABC XYZ	HARA ID
Program Nr.	A01234	Last Modified	John Doe	HARA DATE
System/Sub-system/Component/Sub-Component	EPS	Revised by	John Doe	Revised Date
Team	John Doe	Rvision Nr.	1	

ID	Item	Function	Malfunctioning Behavior	HAZARD	Hazardous Event	S	C	E	ASIL
1	EPS	Senses the torque applied to the	Torque cannot be sensed from steering	Unintended Vehicle	Driving at high speed (100 kph ≤	S3	C3	E4	D
2	EPS	Senses the torque applied to the	Torque cannot be sensed from steering	Insufficient Vehicle	Driving at medium speed (40 kph	S3	C2	E4	C
4	EPS	Senses the steering wheel angle and steering column angle.	Senses torque with less frequency than needed	Unintended Vehicle Lateral Motion/Unintended Yaw	Driving at high speed (100 kph ≤ V < 130 kph), with heavy traffic, good visibility, and good road conditions.	S3	C3	E4	D
5	EPS	Senses the steering wheel angle and steering column angle.	Senses torque with less frequency than needed	Insufficient Vehicle Lateral Motion/Insufficient Yaw	Driving at medium speed (40 kph ≤ V < 100 kph) on a country road, with heavy traffic, good visibility, and good road conditions.	S3	C2	E4	C

Unstructured documents, e.g. MS Excel

- inconsistent
- error-prone
- may lead to miscommunications



MBSE tools, e.g. MagicDraw

- generally focus on creating information
- lack user interfaces for presenting data
- cannot be customized for new tasks

What is Functional Safety?

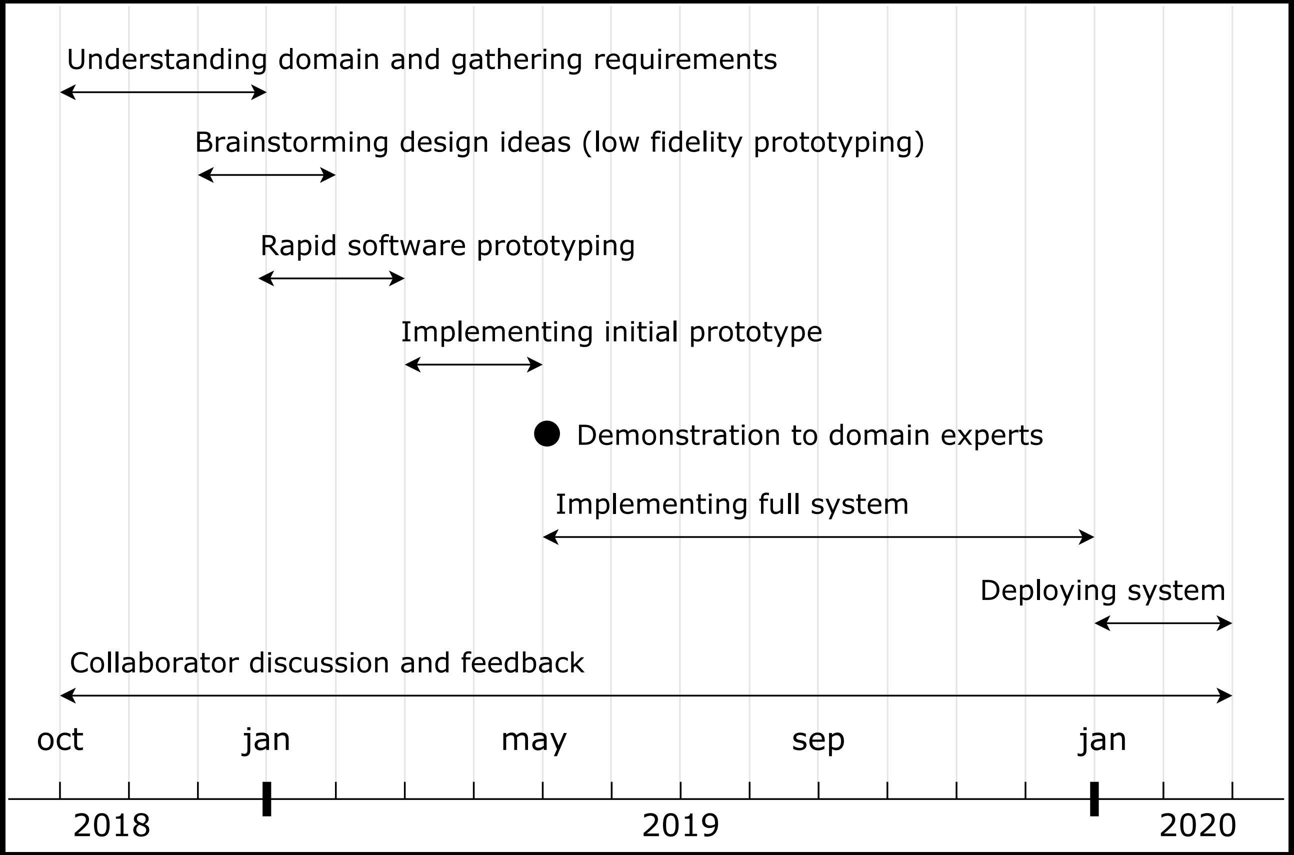
A technique in which domain experts

- **identify and assess hazards due to malfunctioning of automotive EE systems**
- **set goals to minimize unreasonable risk due to these hazards, and**
- **define requirements to achieve these goals**

Source: https://www.iso.org/standard/68383.html

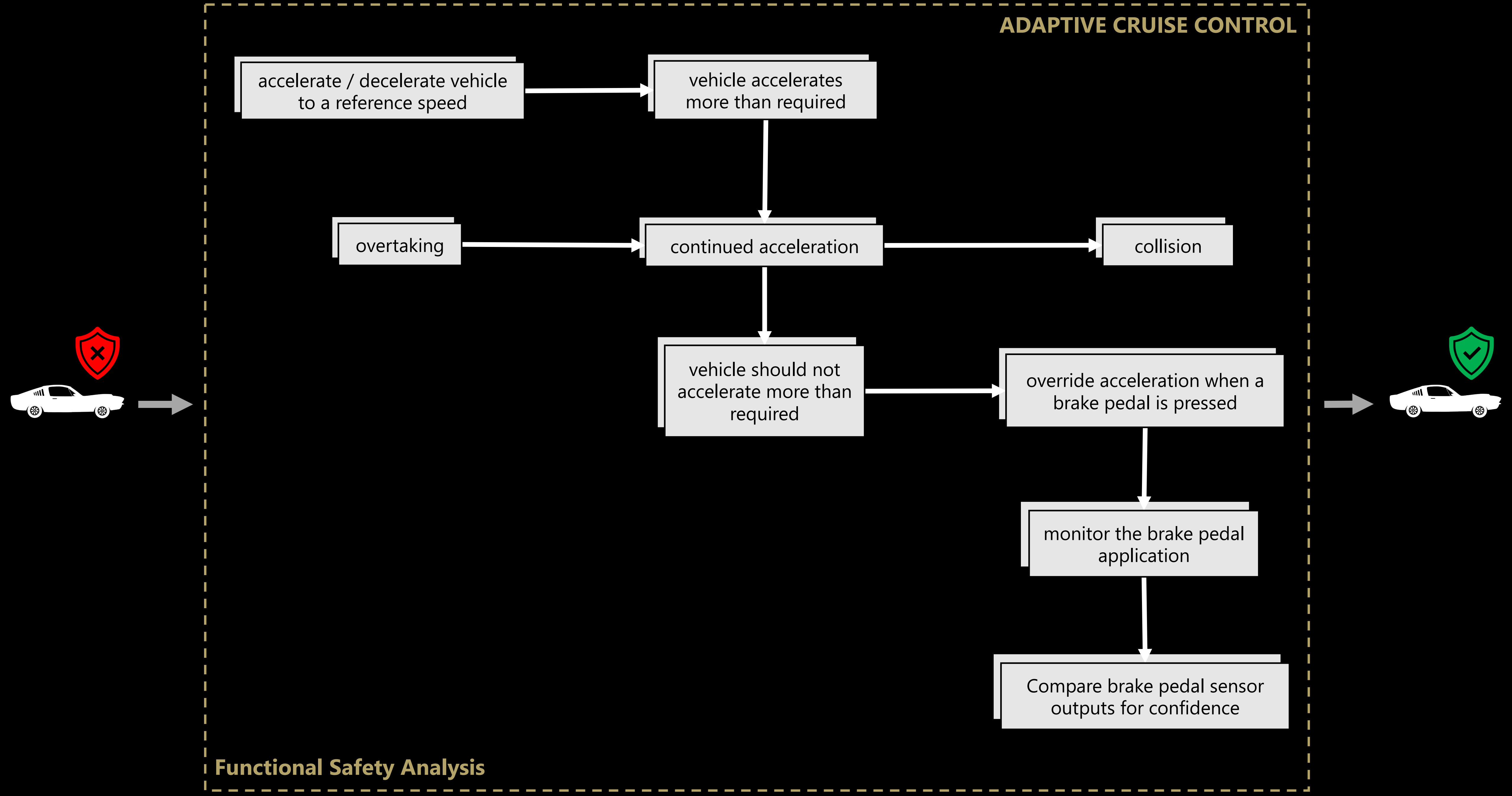
Design Study

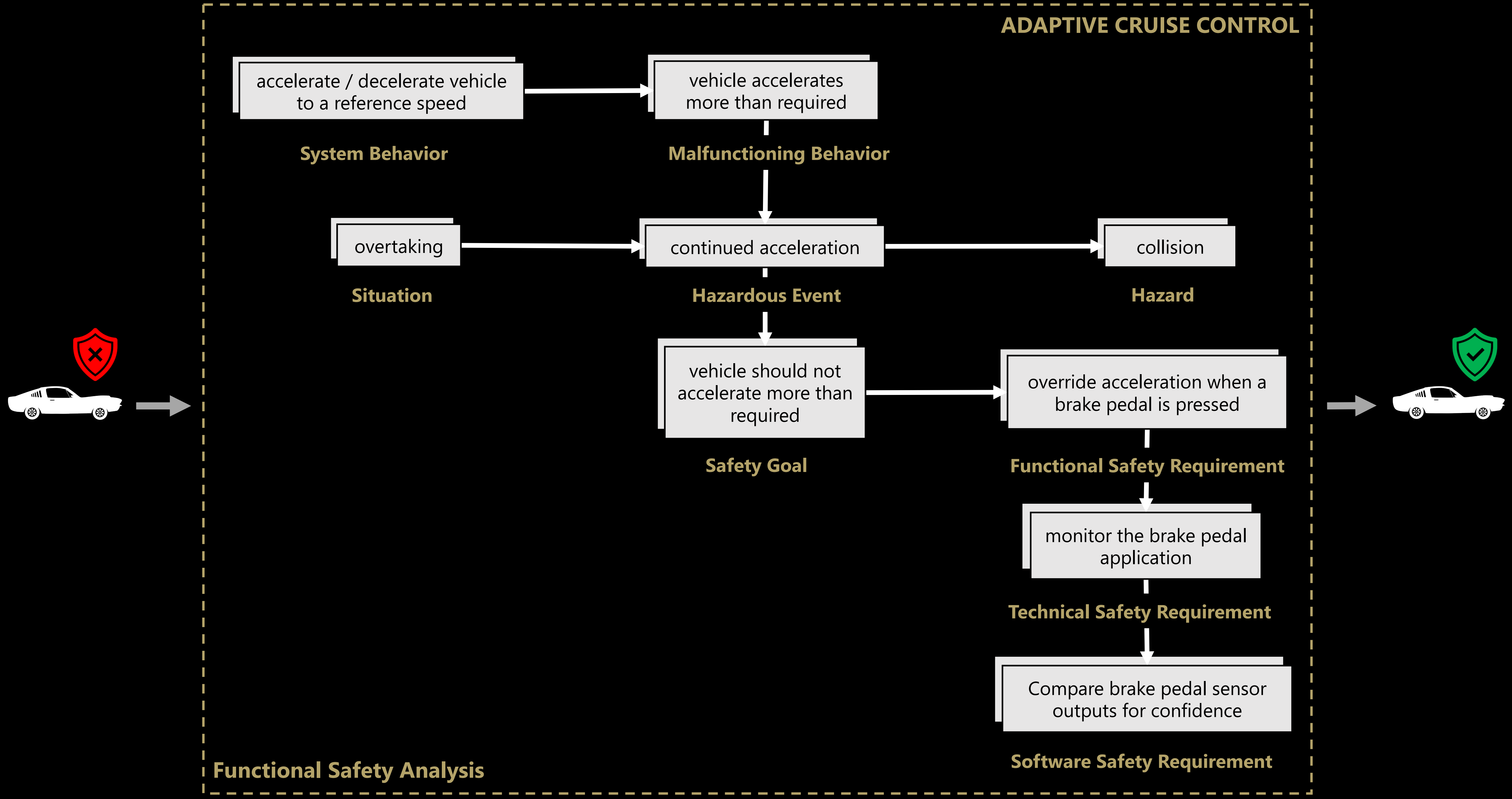
User-centered process with 1-4 domain experts through 1-hour weekly sessions.



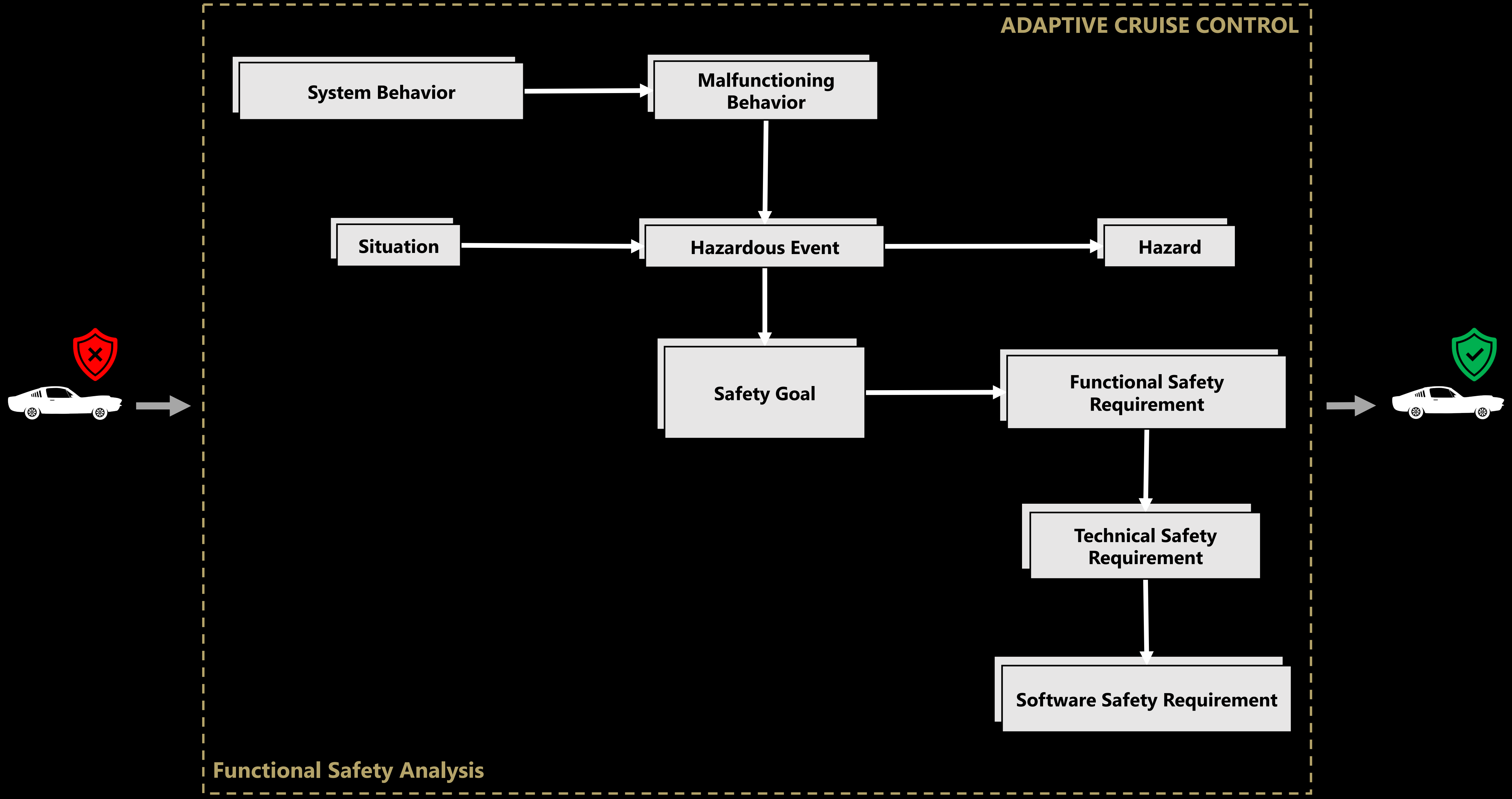

Unreasonable
Risks
Functional Safety
Analysis
Minimum
Risks

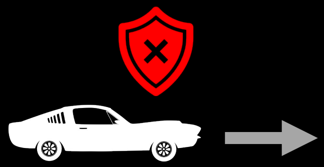
Functional Safety Analysis


ADAPTIVE CRUISE CONTROL
accelerate / decelerate vehicle to a reference speed
vehicle accelerates more than required
overtaking
continued acceleration
collision
vehicle should not accelerate more than required
override acceleration when a brake pedal is pressed
monitor the brake pedal application
Compare brake pedal sensor outputs for confidence
Functional Safety Analysis

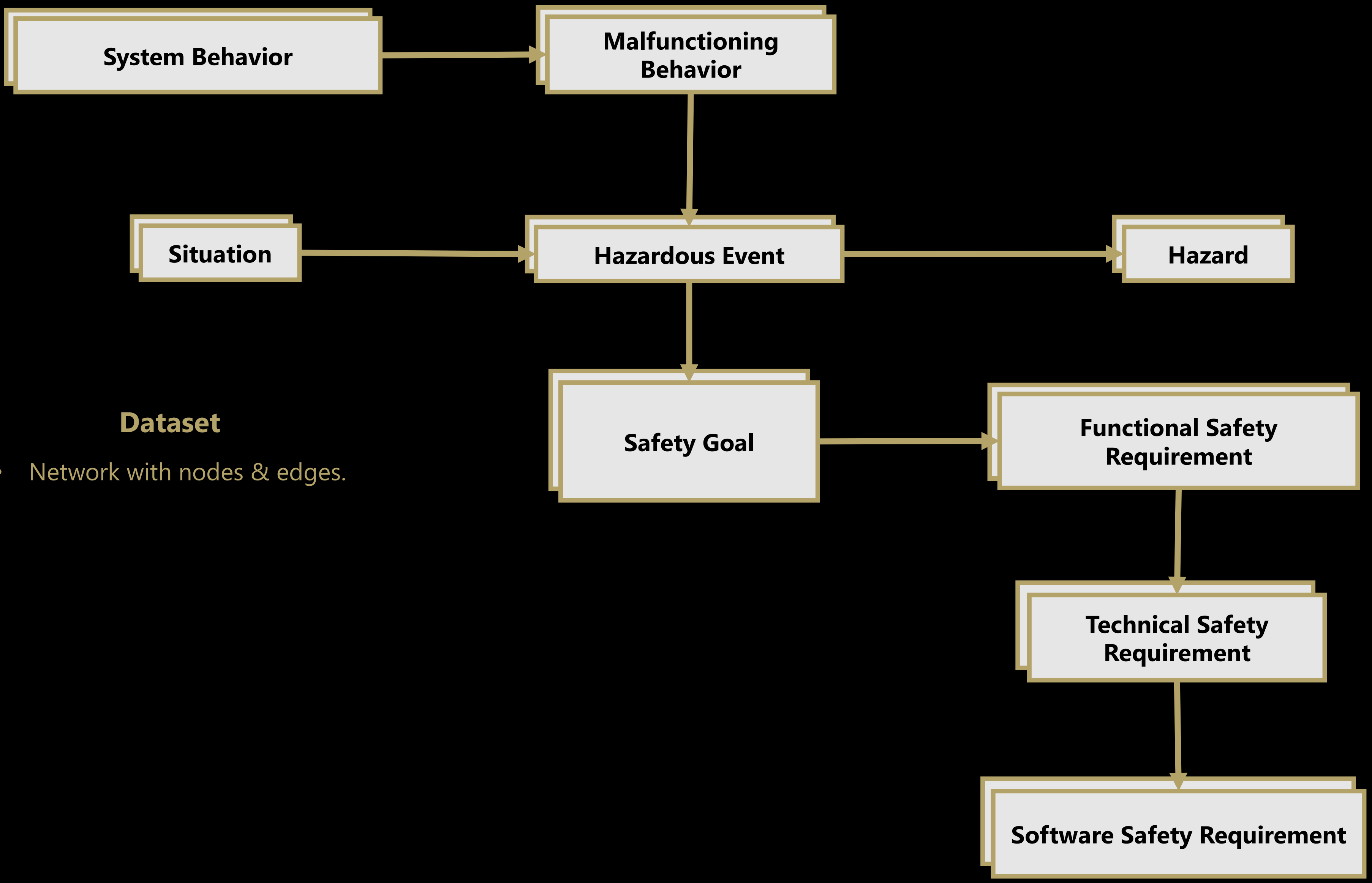


ADAPTIVE CRUISE CONTROL
accelerate / decelerate vehicle to a reference speed
System Behavior
vehicle accelerates more than required
Malfunctioning Behavior
overtaking
Situation
continued acceleration
Hazardous Event
collision
Hazard
vehicle should not accelerate more than required
Safety Goal
override acceleration when a brake pedal is pressed
Functional Safety Requirement
monitor the brake pedal application
Technical Safety Requirement
Compare brake pedal sensor outputs for confidence
Software Safety Requirement
Functional Safety Analysis


ADAPTIVE CRUISE CONTROL
System Behavior
Malfunctioning Behavior
Situation
Hazardous Event
Hazard
Safety Goal
Functional Safety Requirement
Technical Safety Requirement
Software Safety Requirement
Functional Safety Analysis



ADAPTIVE CRUISE CONTROL

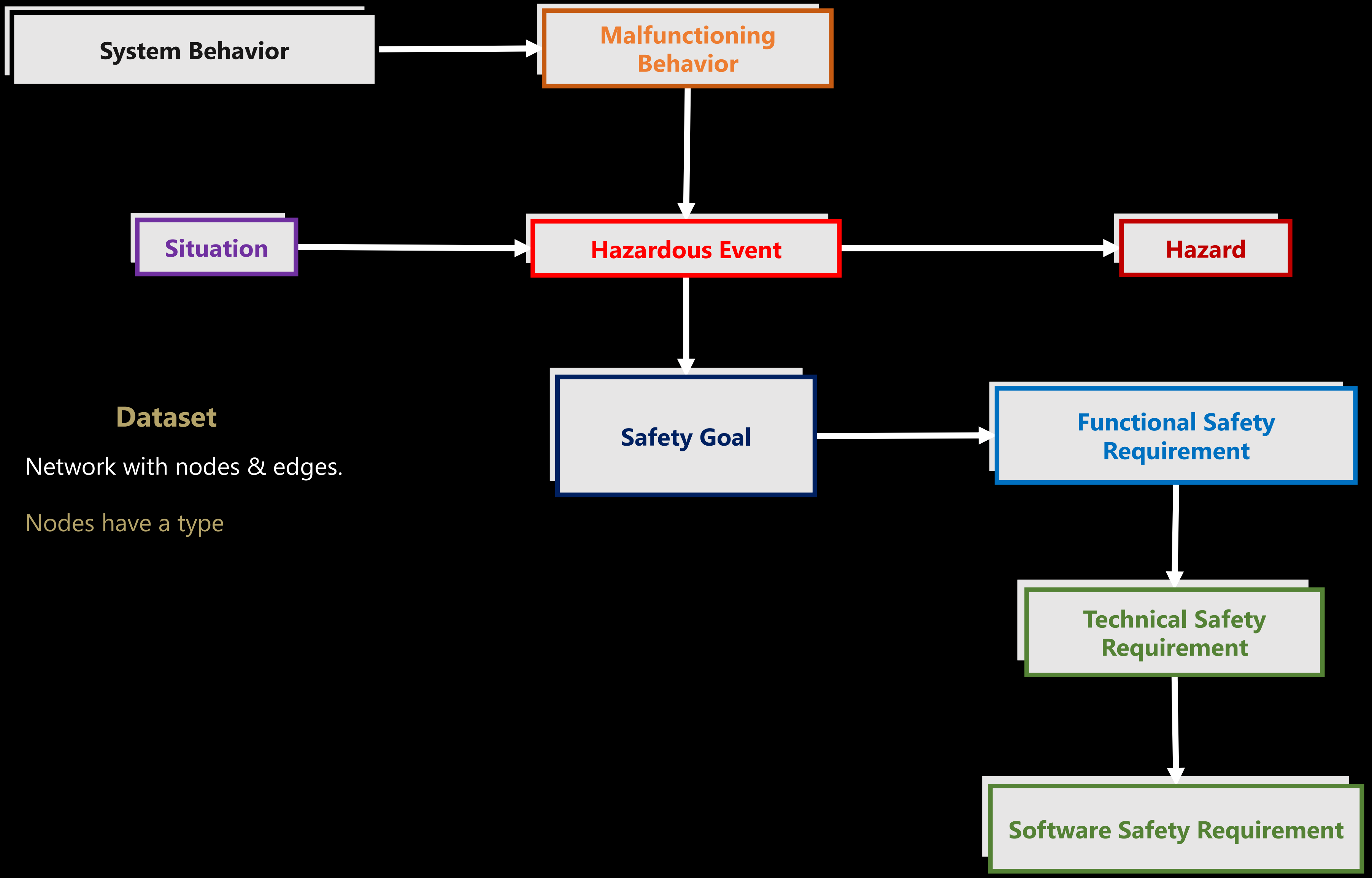


Dataset

- Network with nodes & edges.

Functional Safety Analysis

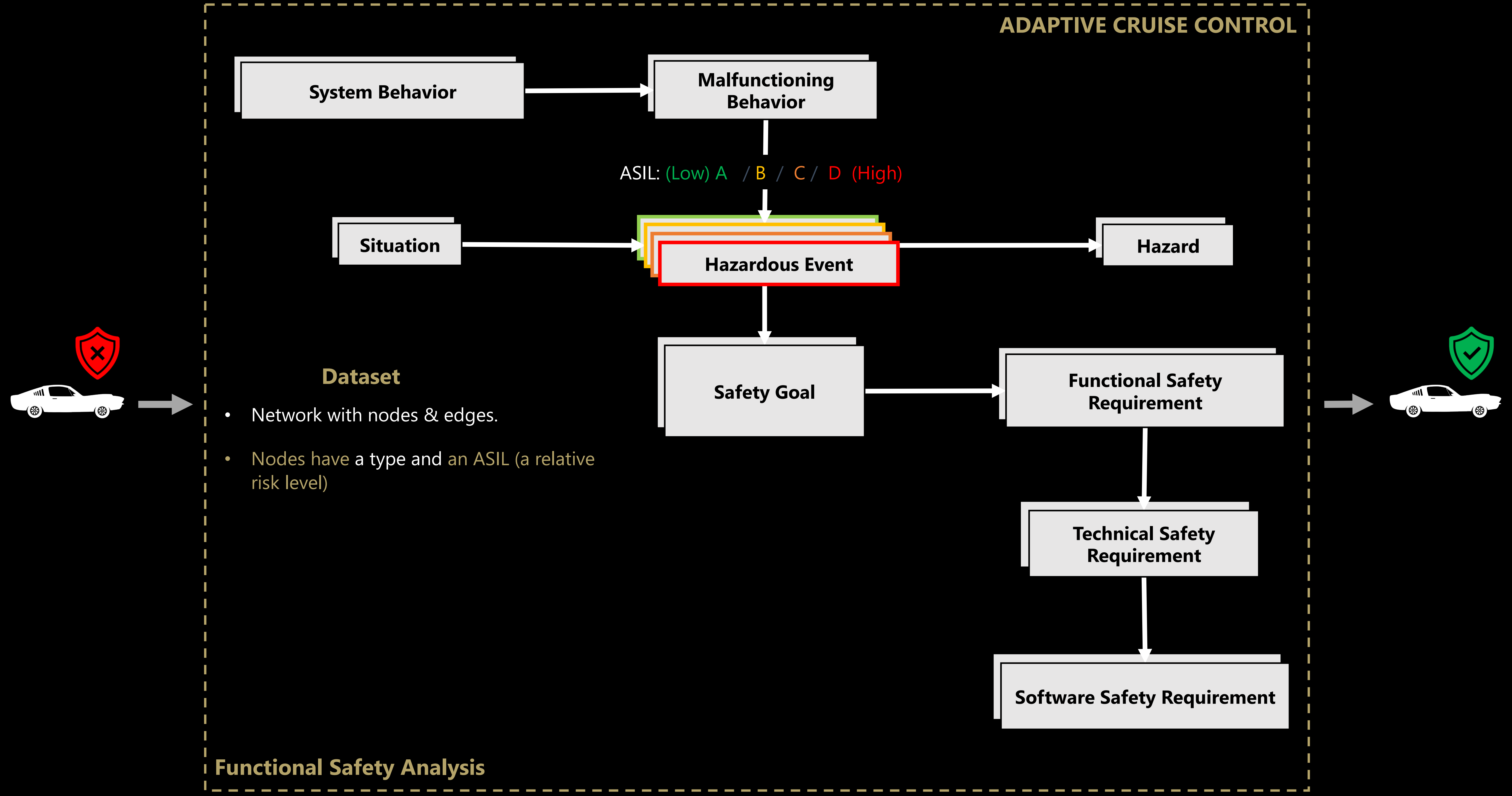
ADAPTIVE CRUISE CONTROL



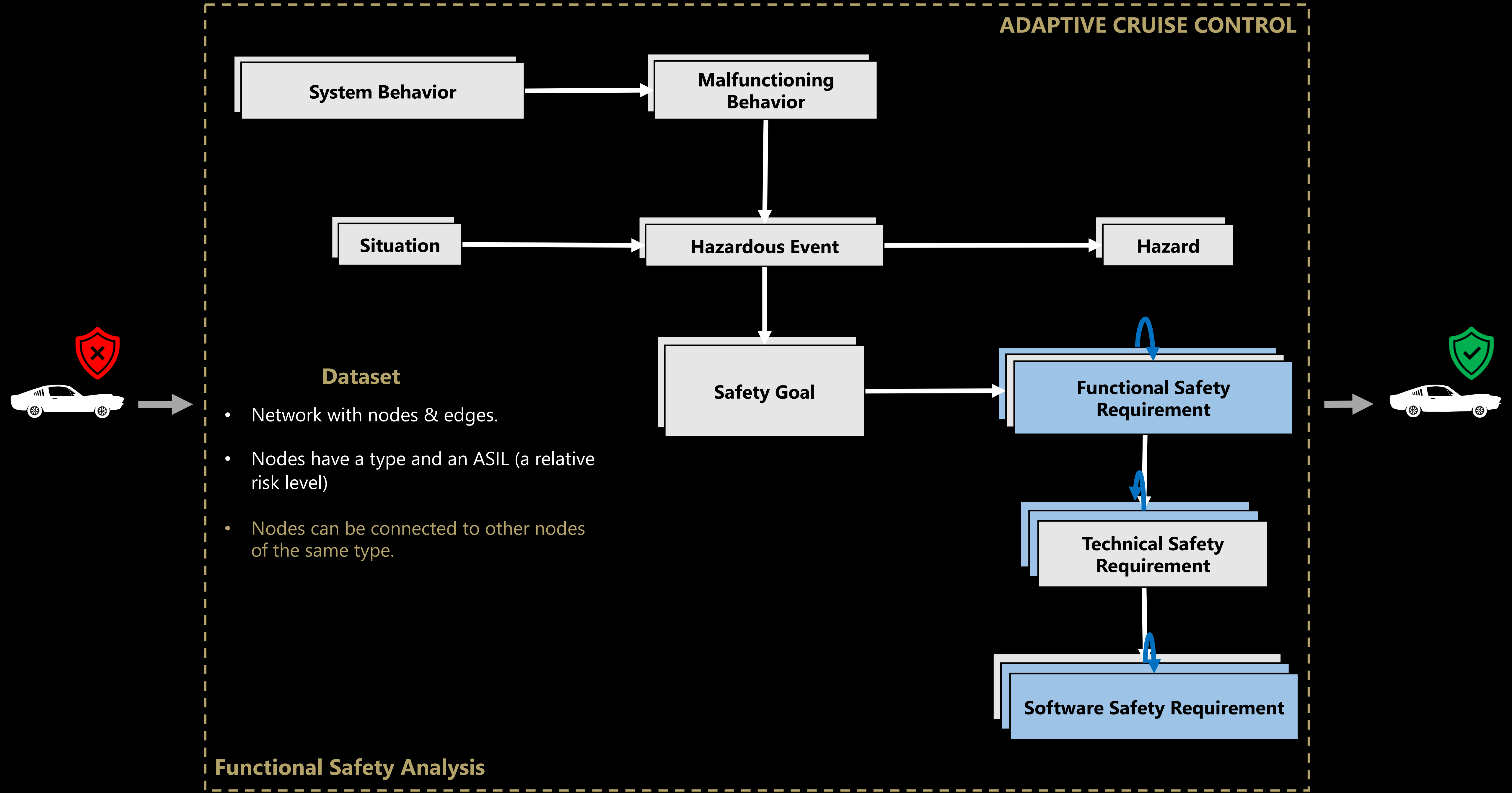
Dataset

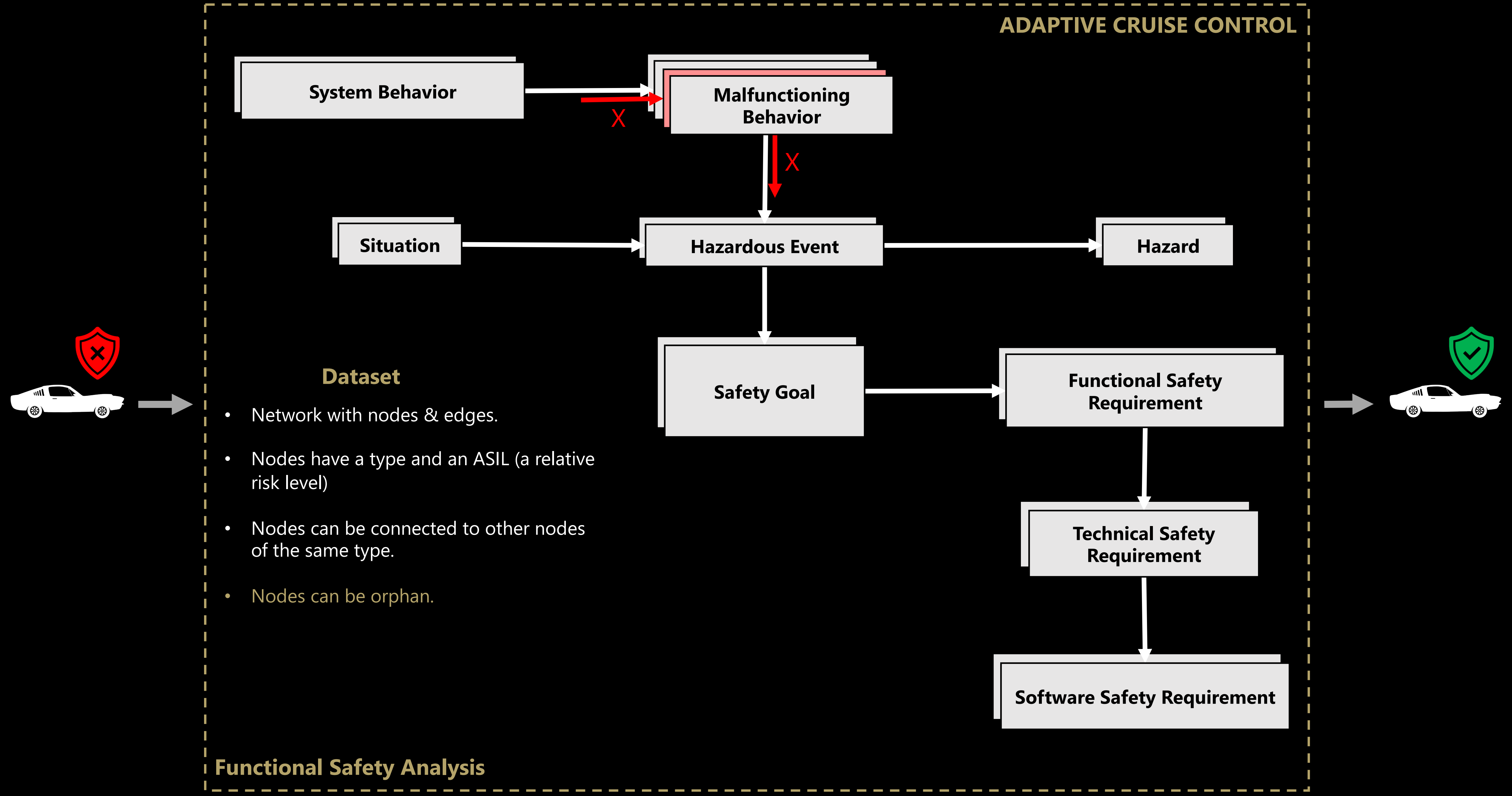
- Network with nodes & edges.
- Nodes have a type

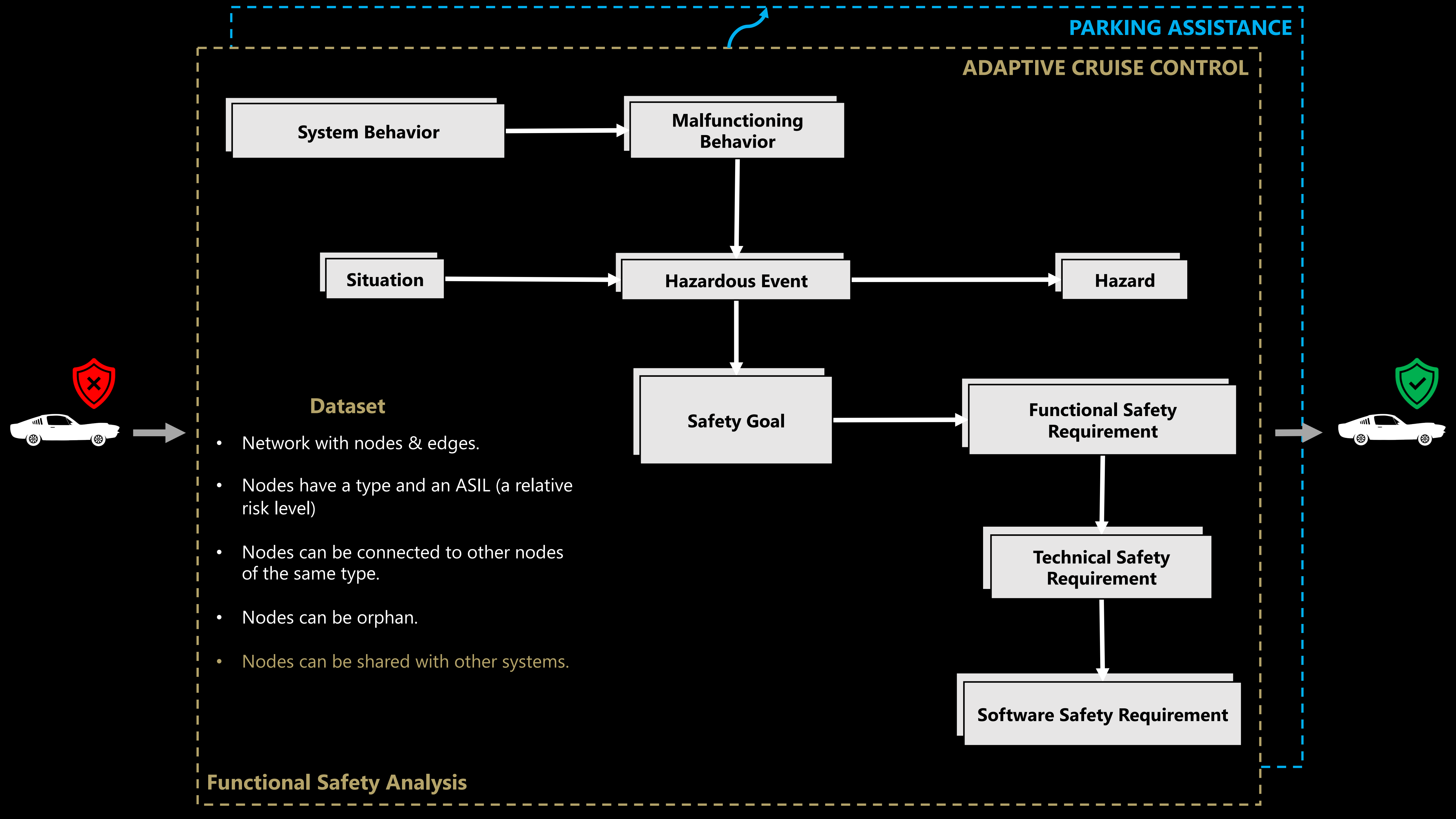
Functional Safety Analysis



ADAPTIVE CRUISE CONTROL
System Behavior
Malfunctioning Behavior
ASIL: (Low) A / B / C / D (High)
Situation
Hazardous Event
Hazard
Safety Goal
Functional Safety Requirement
Technical Safety Requirement
Software Safety Requirement
Dataset
• Network with nodes & edges.
• Nodes have a type and an ASIL (a relative risk level)
Functional Safety Analysis


ADAPTIVE CRUISE CONTROL
System Behavior
Malfunctioning Behavior
Situation
Hazardous Event
Hazard
Safety Goal
Functional Safety Requirement
Technical Safety Requirement
Software Safety Requirement
Dataset
• Network with nodes & edges.
• Nodes have a type and an ASIL (a relative risk level)
• Nodes can be connected to other nodes of the same type.
Functional Safety Analysis


ADAPTIVE CRUISE CONTROL
System Behavior
Malfunctioning Behavior
X
X
Situation
Hazardous Event
Hazard
Safety Goal
Functional Safety Requirement
Technical Safety Requirement
Software Safety Requirement
Dataset
• Network with nodes & edges.
• Nodes have a type and an ASIL (a relative risk level)
• Nodes can be connected to other nodes of the same type.
• Nodes can be orphan.
Functional Safety Analysis


PARKING ASSISTANCE
ADAPTIVE CRUISE CONTROL
System Behavior
Malfunctioning Behavior
Situation
Hazardous Event
Hazard
Safety Goal
Functional Safety Requirement
Technical Safety Requirement
Software Safety Requirement
Dataset
• Network with nodes & edges.
• Nodes have a type and an ASIL (a relative risk level)
• Nodes can be connected to other nodes of the same type.
• Nodes can be orphan.
• Nodes can be shared with other systems.
Functional Safety Analysis

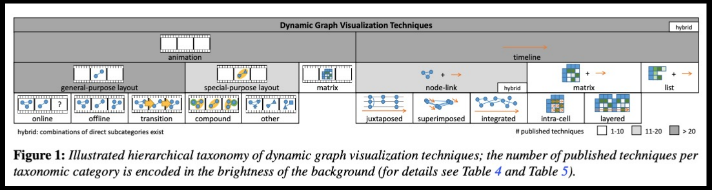
Important user tasks

Functional Safety	VIS
“Which are this node’s connections? Are there any missing connections? Are there nodes that are NOT assigned an ASIL?”	Network exploration; Direct manipulation
“Are the risks associated with a Malfunctioning Behaviour (sufficiently) addressed?”	Network route tracing
“Instead of re-defining certain node and link definitions, can I re-use those from previous projects?”	Network comparison and diffs; Set visualization

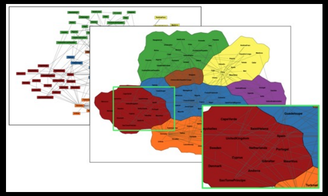
Designing SafetyLens

VIS

- Network exploration; Direct manipulation
- Network route tracing
- Network comparison and diffs; Set visualization

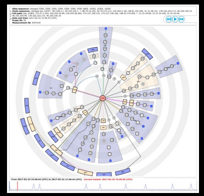


Beck et al, 2017

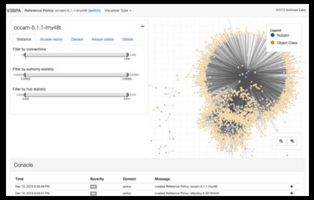


Saket et al, 2016

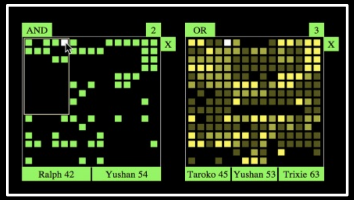
VisTracer, 2012



Radian, 2018



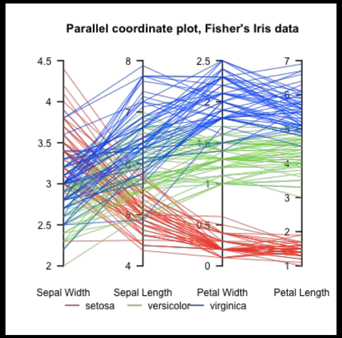
V3SPA, 2016



Onset, 2014

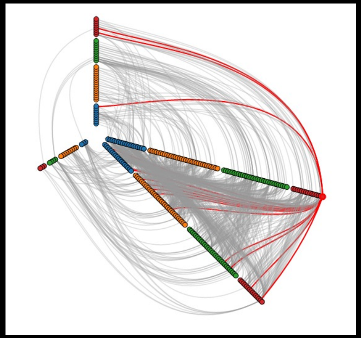
UpSet, 2014

Designing SafetyLens



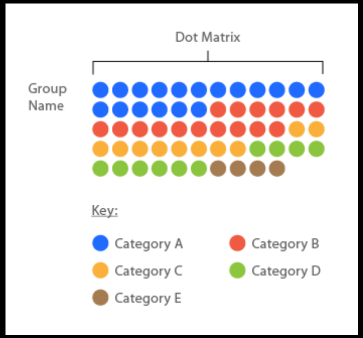
Parallel coordinates chart

- Nodes can be connected to more than two types.
- Discovering patterns is difficult due to linear positioning of nodes



Hive plot

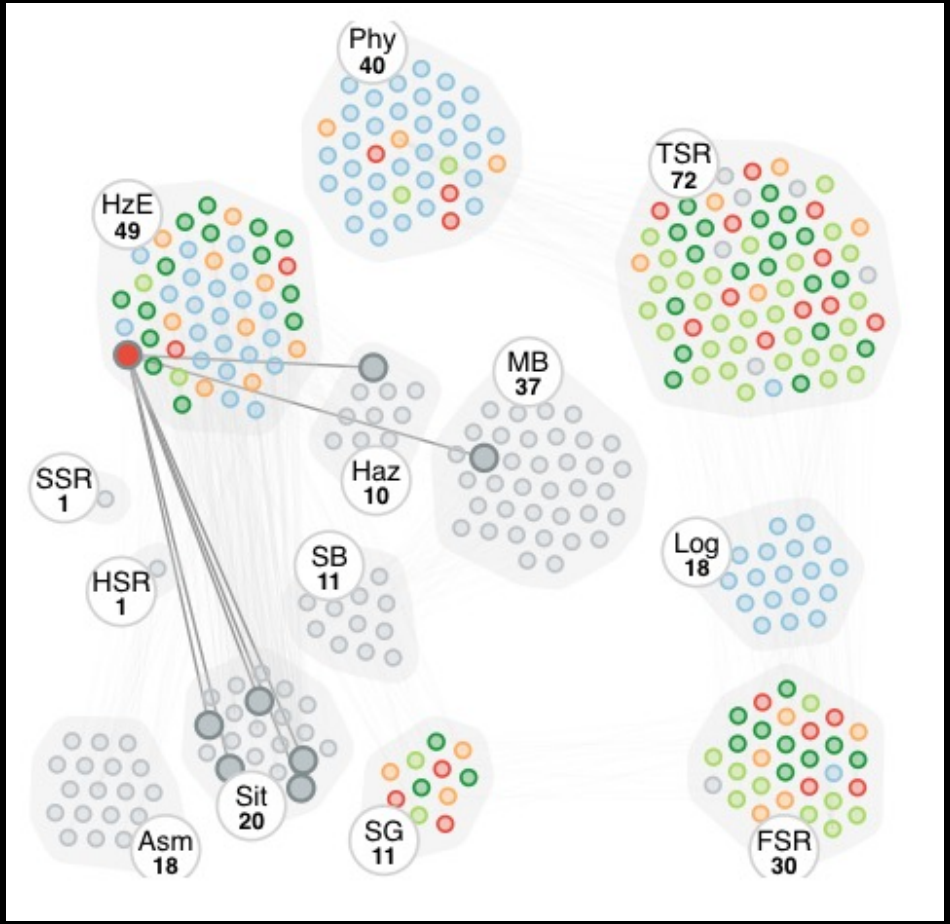
- Discovering patterns is difficult due to linear positioning of nodes



Dot matrix chart

- The spatial positioning of nodes seem of significance but that is not the case.

Designing SafetyLens



Node-link-group Visualization

- Nodes of the same type are clustered using the:
  - multi-body force,
  - circle packing, and
  - collision detection algorithms.
- Each group
  - is identified with a larger label node, and
  - its extent, defined as a convex hull which is highlighted.
- The node groups, nodes, and the links are interactive.

Task #1

- “Which are this node’s connections? Are there any missing connections? Are there nodes that are NOT assigned an ASIL?”
- “Are the risks associated with a Malfunctioning Behaviour (sufficiently) addressed?”
- “Instead of re-defining certain node and link definitions, can I re-use those from previous projects?”

All Hazardous Events should be assigned an ASIL.

Dashboard Compare Summary

Data has been obfuscated due to security issues.

Details

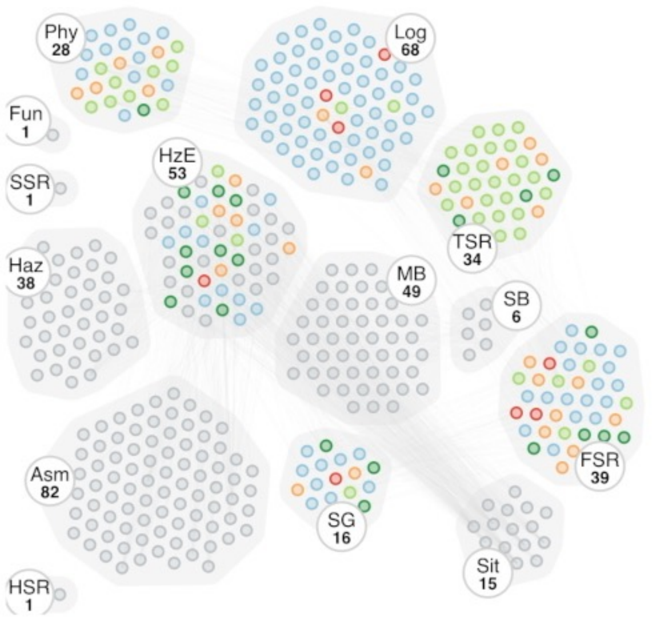
Project

Type

ASIL

Connected Neighbors ()

P1 Project-A



Nodes Links Trace

Name	Type	ASIL

Task #2

- ❖ "Which are this node's connections? Are there any missing connections? Are there nodes that are NOT assigned an ASIL?"
- ❖ "Are the risks associated with a Malfunctioning Behaviour (sufficiently) addressed?"
- ❖ "Instead of re-defining certain node and link definitions, can I re-use those from previous projects?"

- "Verify if a path exists from the MB → HzE → SG → FSR → TSR ?"
- "Verify if the ASILs are all defined and consistent along that path?"

Dashboard Compare Summary

Data has been obfuscated due to security issues.

Details

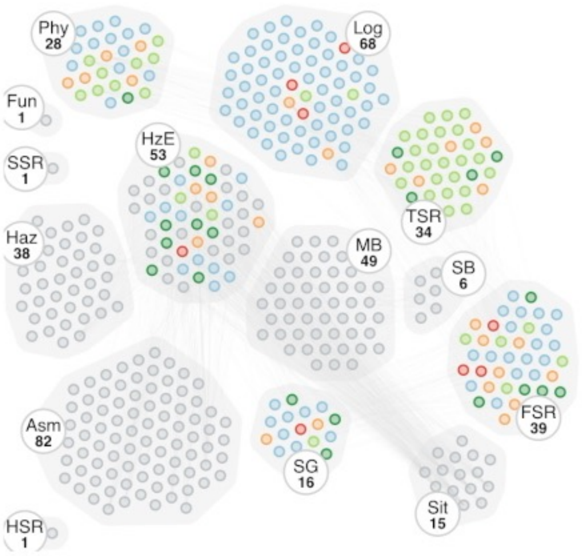
Project

Type

ASIL

Connected Neighbors ()

P1 Project-A



Nodes Links Trac

Name	Type	ASIL

Task #3

- “Which are this node’s connections? Are there any missing connections? Are there nodes that are NOT assigned an ASIL?”

- **“Are the risks associated with a Malfunctioning Behaviour (sufficiently) addressed?”**

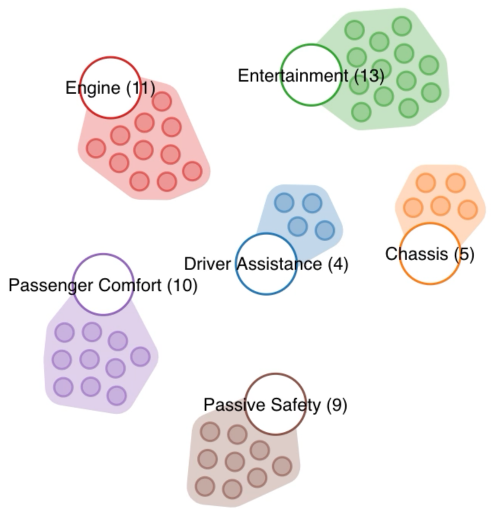
- “Instead of re-defining certain node and link definitions, can I re-use those from previous projects?”

- Verify if a node (e.g. MB) is already defined in older projects and reuse its node-link definitions.

Dashboard Compare Summary *Data has been obfuscated due to security issues.*

Projects

Cluster by Department



S	Project	Department	System	Incharge	Facility
	Project-A	Driver Assistance	Driver Assist	Bob	USA
	Project-B	Driver Assistance	Lane Assist	Vernon	Asia Pacific
	Project-C	Driver Assistance	Park Assist	Amanda	Asia Pacific
	Project-D	Driver Assistance	Adaptive Cruise Control	John	USA
	Project-E	Chassis	Anti-lock Braking System	Paul	USA
	Project-F	Chassis	Brake Assist	Mike	Asia Pacific
	Project-G	Chassis	Electronic Damper	Raj	USA
	Project-H	Entertainment	Vehicle Audio	Jenny	EU
	Project-I	Entertainment	Navigation	Jenny	EU
	Project-J	Engine	Electronic Control Unit	Gary	EU

« 1 2 3 4 5 6 »

Feedback and Going Forward

The overall feedback was **Positive.**

Comments:

- "This let's me see projects quickly and spot problems… but sometimes things don't look right, **can I edit right here?**"

- "How do I only see **what's changed in the visualization from the last time** I logged in? How do I know if this ASIL C has undergone revisions, e.g. was previously D?"

- "What do these (so many node) **colors** represent? What do the **spatial positions** of nodes mean?"

SafetyLens: Visual Data Analysis of Functional Safety of Vehicles

Arpit Narechania* — Georgia Institute of Technology
Ahsan Qamar † — Ford Motor Company
Alex Endert‡ — Georgia Institute of Technology

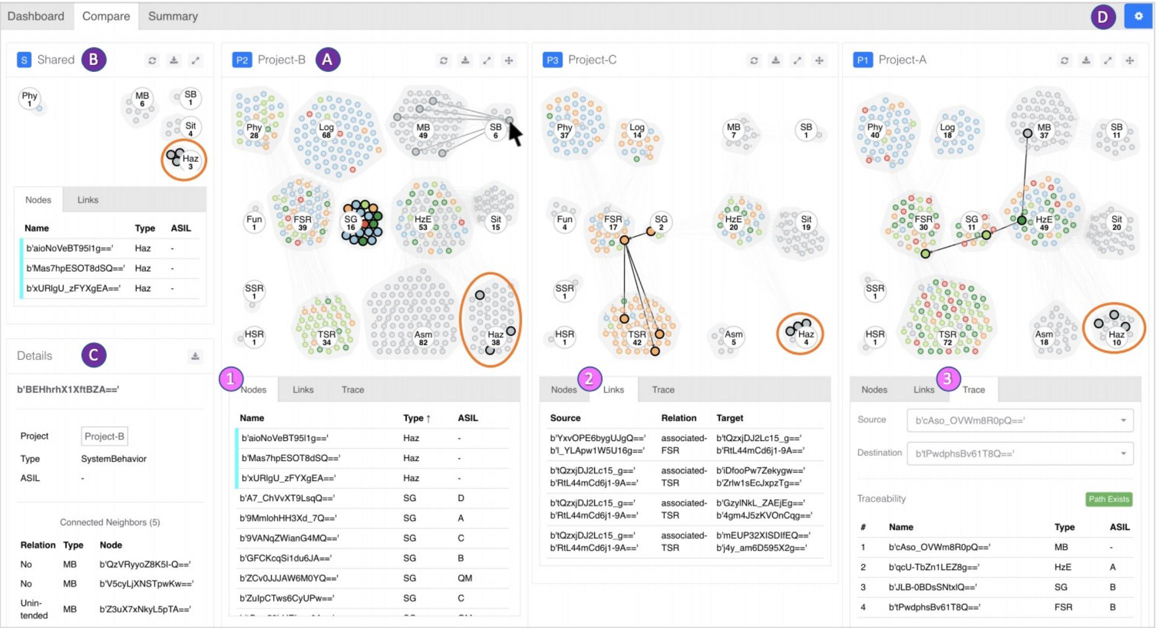


Fig. 1. The SafetyLens Compare view: **(A)** Project Panel comprising the visualization canvas and three tabs: (1) Nodes, (2) Links, and (3) Trace, **(B)** Shared Nodes Panel with three nodes (*Hazards*) selected and highlighted across all three projects (ellipses), **(C)** Detail View Panel showing details of a node (*System Behavior*) hovered in *Project-B* (), and **(D)** opens into a Control Panel comprising search and filter controls.

Abstract— Modern automobiles have evolved from just being mechanical machines to having full-fledged electronics systems that enhance vehicle dynamics and driver experience. However, these complex hardware and software systems, if not properly designed, can experience failures that can compromise the safety of the vehicle, its occupants, and the surrounding environment. For example, a system to activate the brakes to avoid a collision saves lives when it functions properly, but could lead to tragic outcomes if the brakes were applied in a way that's inconsistent with the design. Broadly speaking, the analysis performed to minimize such risks falls into a systems engineering domain called Functional Safety. In this paper, we present SafetyLens, a visual data analysis tool to assist engineers and analysts in analyzing automotive Functional Safety datasets. SafetyLens combines techniques including network exploration and visual comparison to help analysts perform domain-specific tasks. This paper presents the design study with domain experts that resulted in the design guidelines, the tool, and user feedback.

Index Terms—Visual data analysis, Design study, Network visualization, Functional safety, Automotive engineering.

For more information, read our paper at

b.gatech.edu/31PcXUE

Reach out to us directly

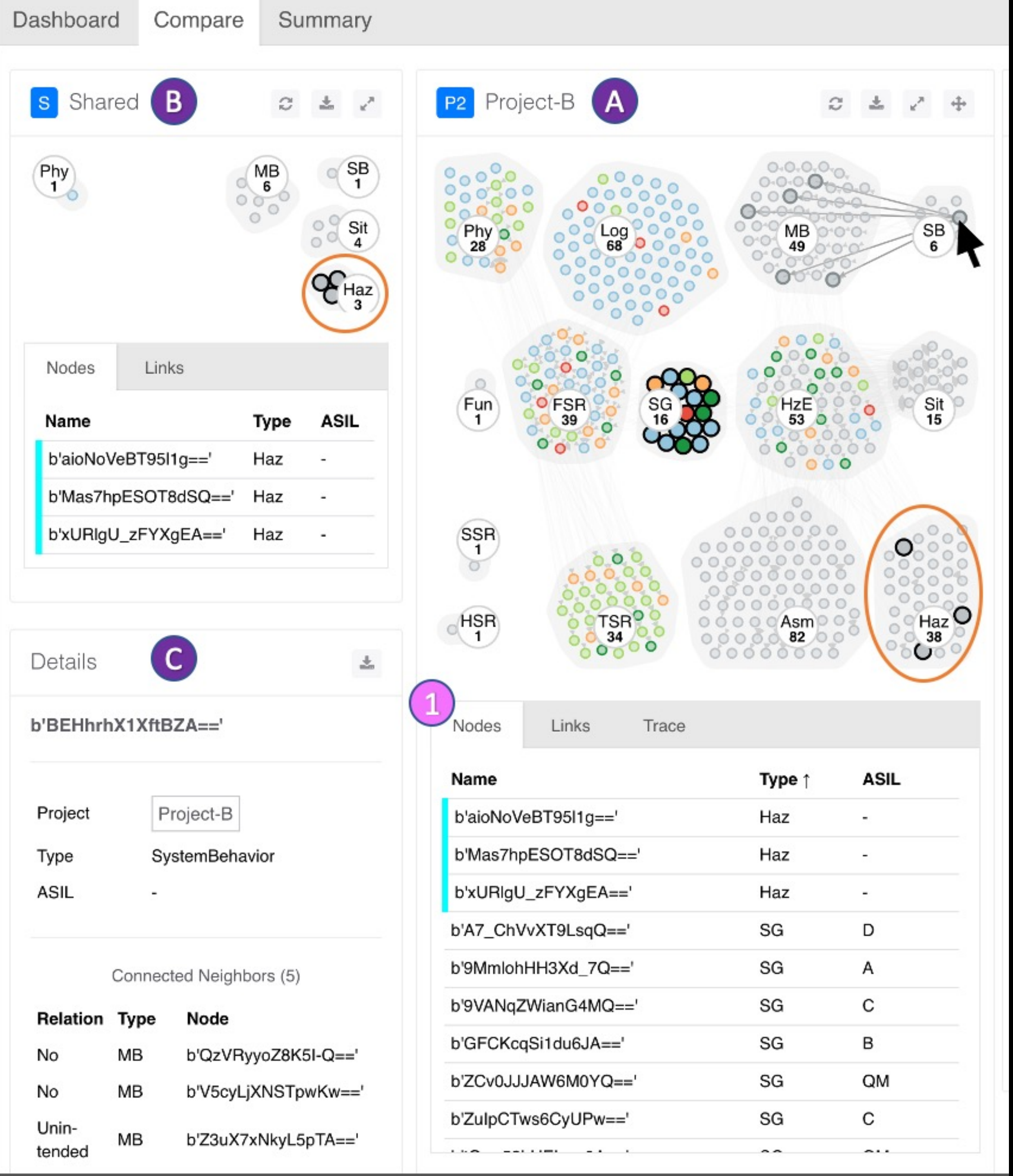
Arpit Narechania
anarechania3@gatech.edu

Ahsan Qamar
aqamar2@ford.com

Alex Endert
endert@gatech.edu



Thank you!



SafetyLens: Visual Data Analysis of Functional Safety of Vehicles

Arpit Narechania
anarechania3@gatech.edu

Ahsan Qamar
aqamar2@ford.com

Alex Endert
endert@gatech.edu



Read the paper at
b.gatech.edu/31PcXUE

Know more about **Functional Safety** at
youtu.be/PrcJn_dWGwA