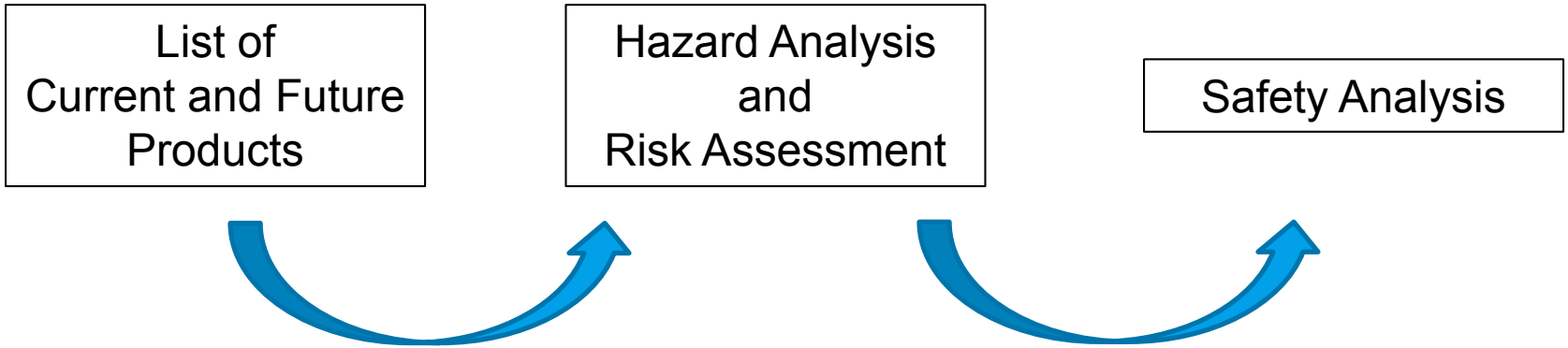

SAE
INTERNATIONAL
GOVERNMENT INDUSTRY MEETING
April 3-5, 2019 | Washington, DC
Safety Analysis of
Heavy-Duty Truck Platooning Systems
Doug Pape
Battelle
*This meeting is co-located with
THE WASHINGTON AUTO SHOW
The Public Policy Show

Safety Analysis of Heavy-Duty Truck Platooning Systems

Battelle is conducting this research for NHTSA



Study Completion: Summer 2020.

A Sampling of Platooning Projects

Volvo

Peloton

Texas A&M Transportation Institute

TARDEC

Safety Analysis of Heavy-Duty Truck Platooning Systems

Hazards

An event that poses danger to people, the system, or the environment

Caused by human error, hardware failure, or software defect (usually)

May be caused by limits of system design (scenario not anticipated)

Identifying Hazards

Preliminary Hazard Analysis (PHA)

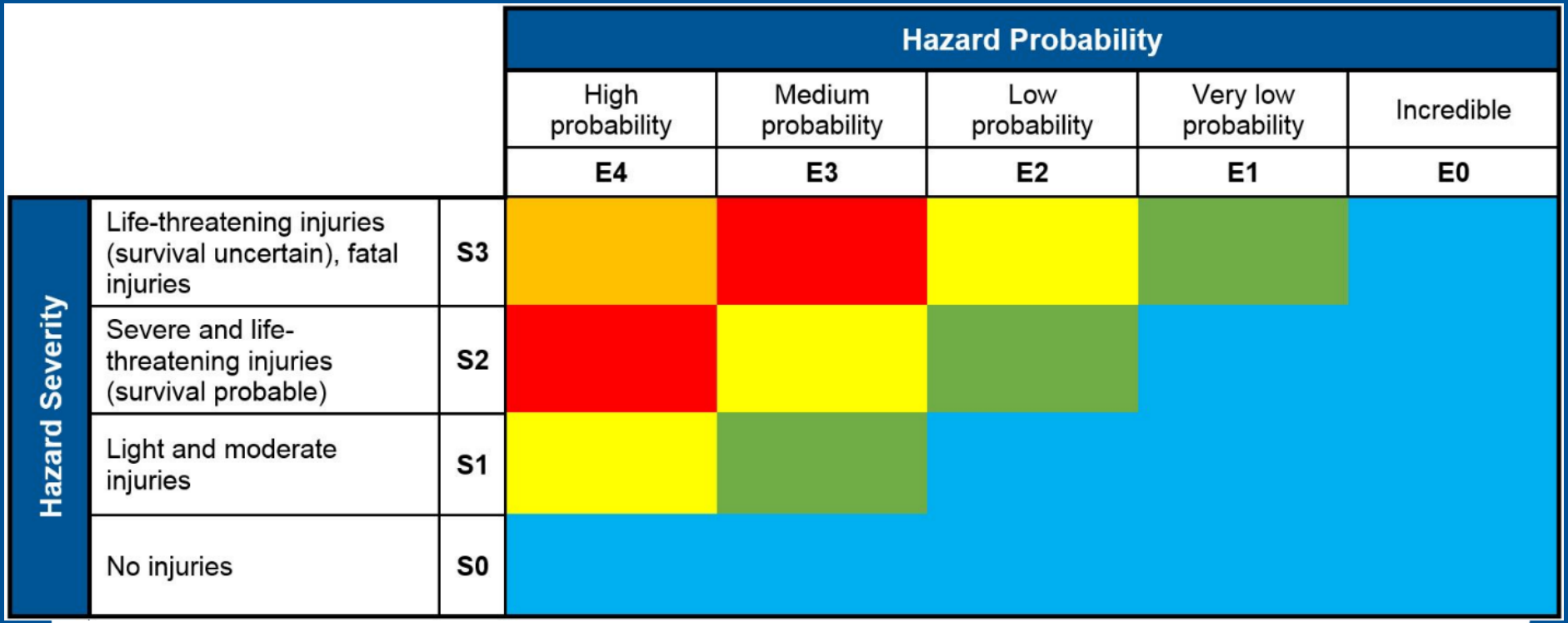
More formalized than brainstorming

Decompose the design to subsystems or blocks

- Identify failures of the function of each block
- Identify failures of the interfaces
- Identify failures from the environment and from human factors

Then characterize the risk of every hazard.

Risk Characterization



Risk Characterization

ISO 26262 adds a third dimension—Controllability

		Controllability		
Severity	Exposure	C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Classes of Hazards We Are Considering

- Communication failures (message lost, delayed, corrupted)
- Component failures (hardware failures, software errors)
- Vehicle factors (brake failures, differences in brake rates)
- Environmental factors (weather, other traffic)
- Driver issues (lack of training, acclimatization with the system)
- Human factors (reliance, fatigue, workload, fumes from close following, trust in the other driver, standardization across brands)

Safety Analysis of Heavy-Duty Truck Platooning Systems

Common Safety Analysis Techniques

Failure Modes & Effects Analysis

FMEA

Bottom → Up

Fault Tree Analysis

FTA

Top → Down

Failure Modes & Effects Analysis

Bottom Up

A Failure Modes & Effects Analysis determines

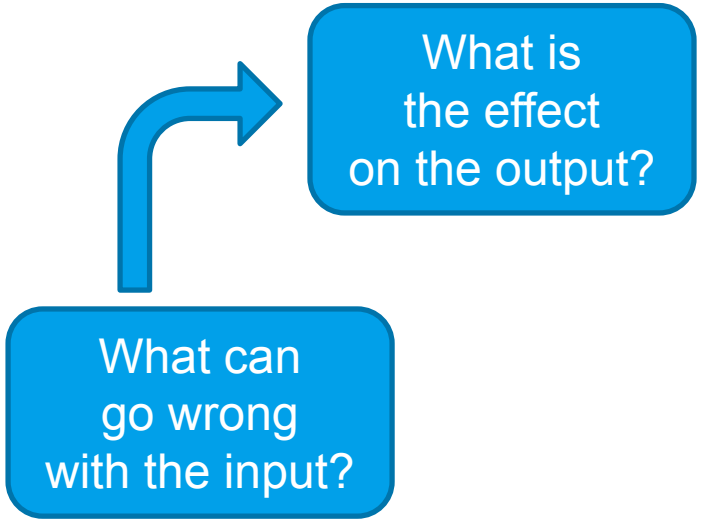
how a system might fail

and the likely effects of particular modes of a failure.

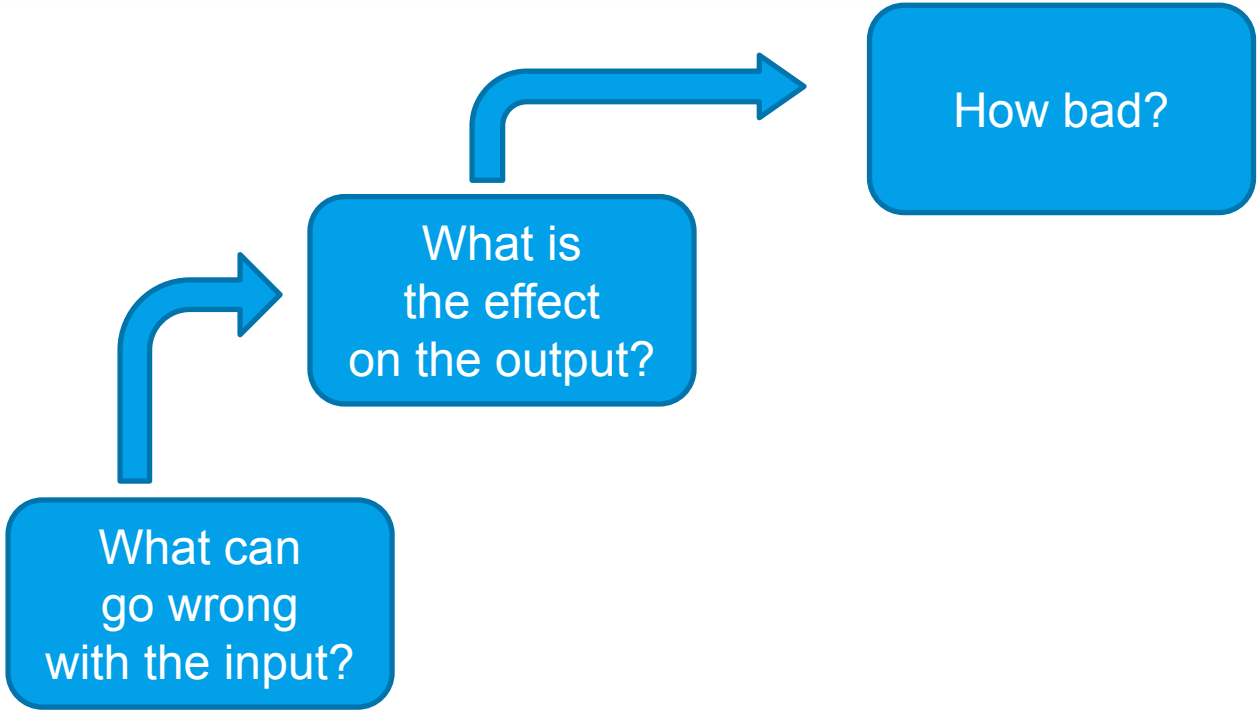
Failure Modes & Effects Analysis

What can go wrong with the input?

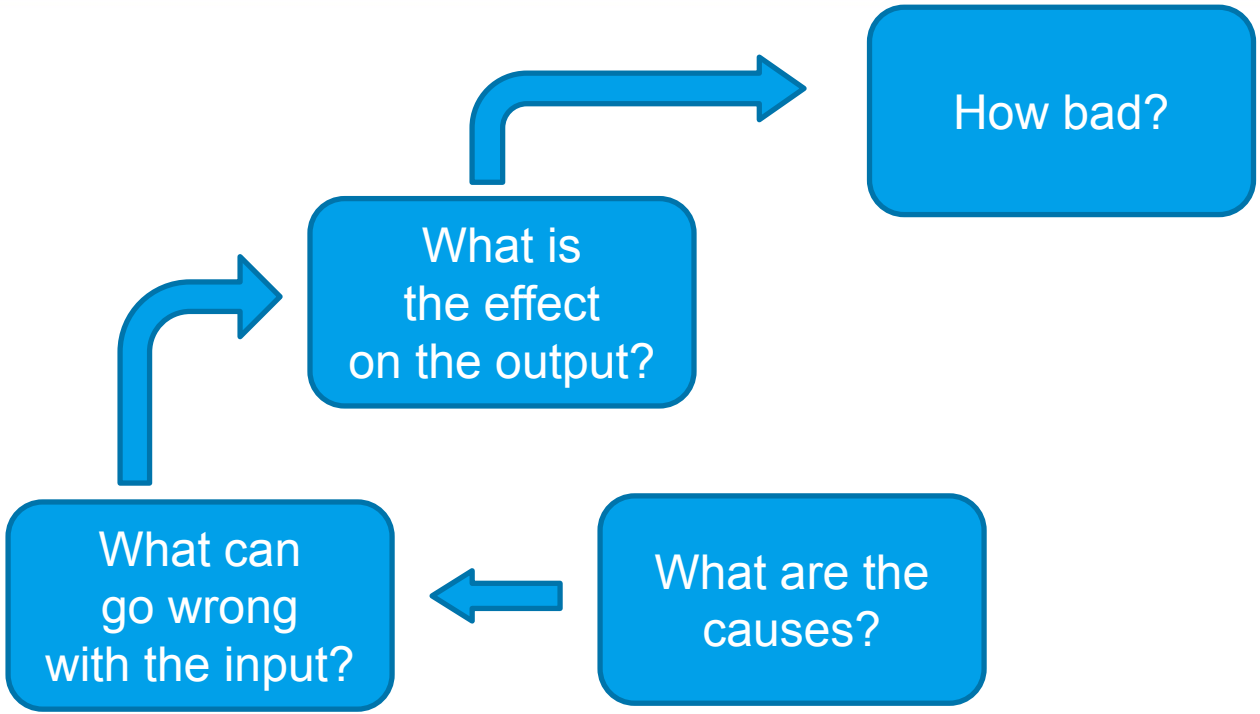
Failure Modes & Effects Analysis



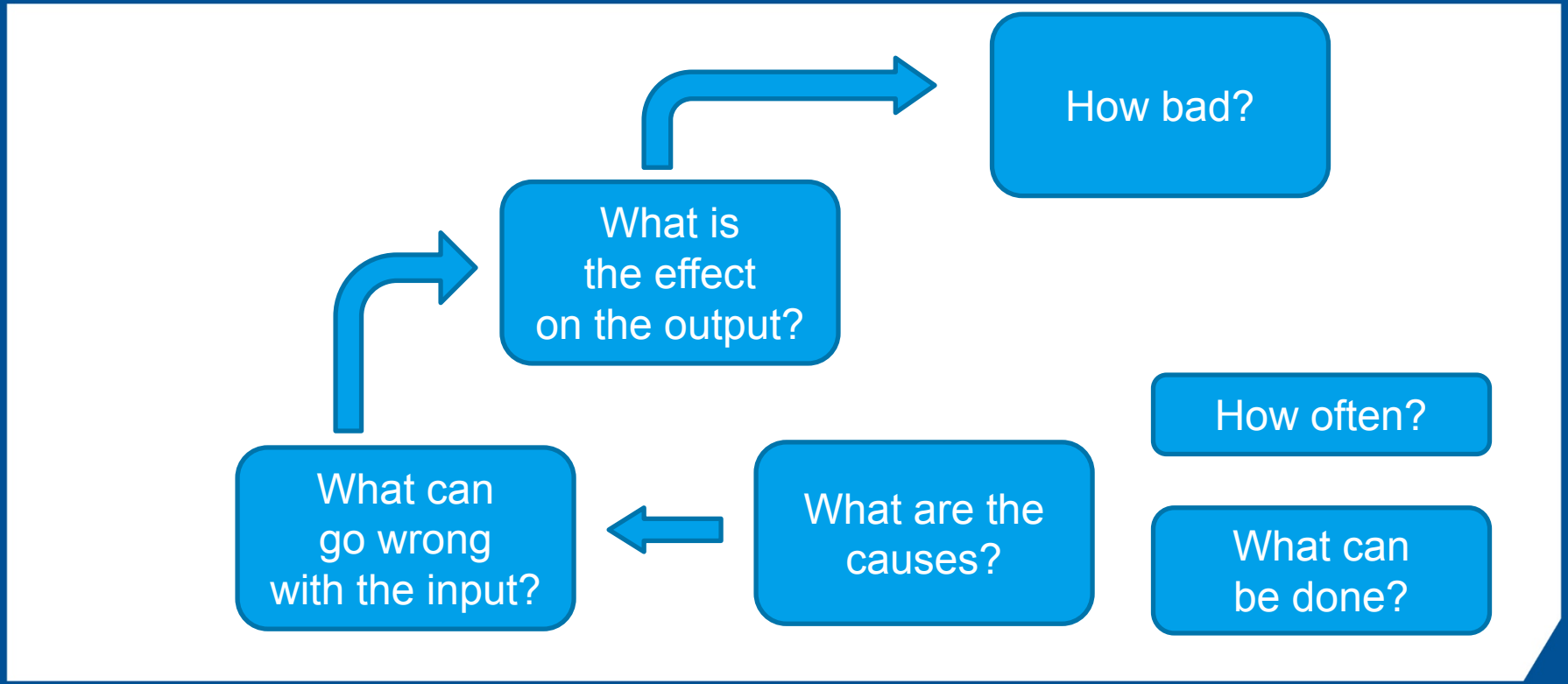
Failure Modes & Effects Analysis



Failure Modes & Effects Analysis



Failure Modes & Effects Analysis



Fault Tree Analysis (FTA)

Top Down

A Fault Tree Analysis is

a deductive analytical technique

where an undesirable state is specified.

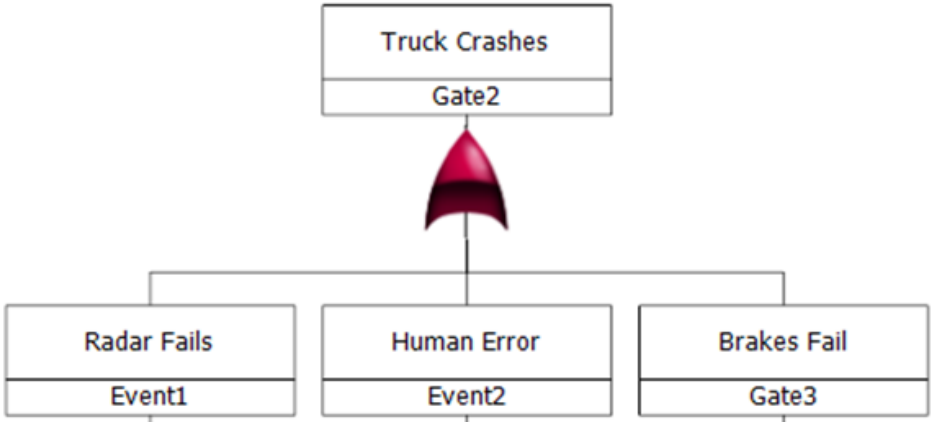
FTA demonstrates how resistant a system is to initiating faults.

FTA of complex systems is labor intensive

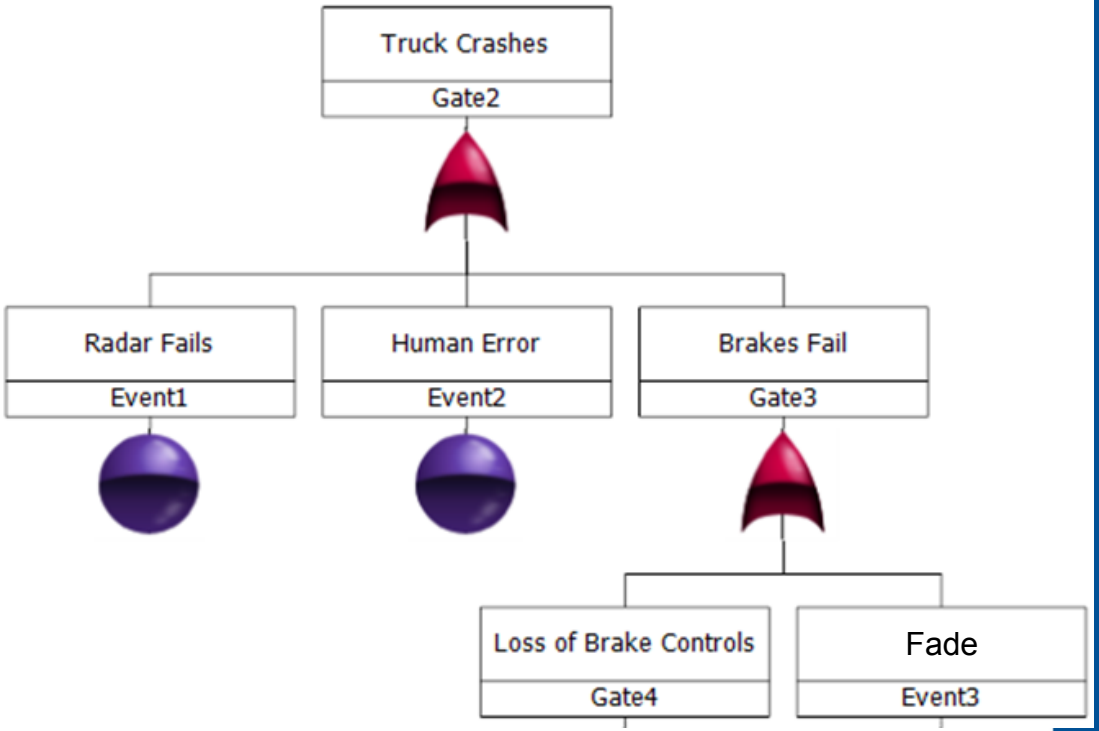
but beneficial.

Top-Down Approach

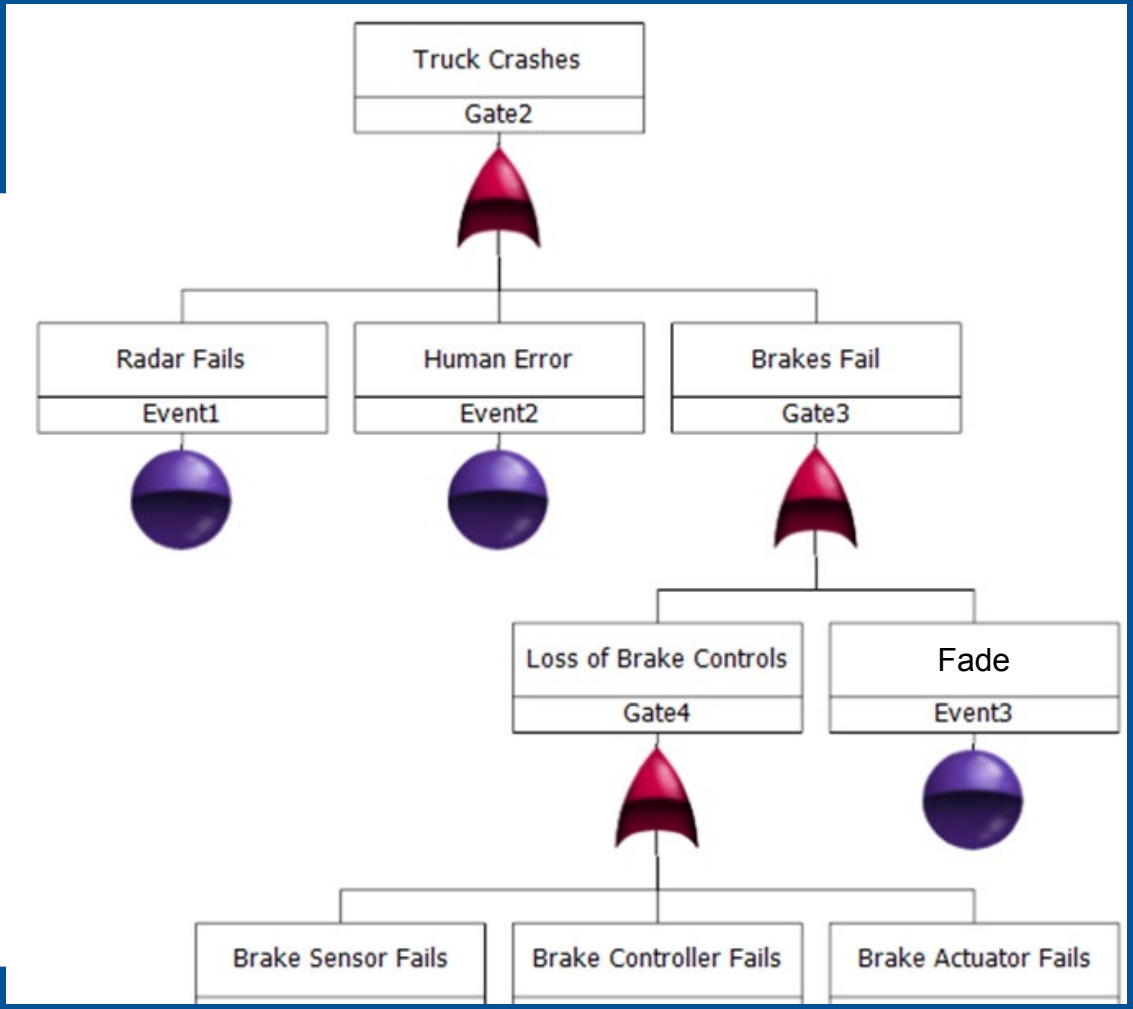
Top-Down Approach



Top-Down Approach



Top-Down Approach



Human Factors

Analysis Techniques

- Task analysis
- Workload assessment
- Activity sequence diagram

Possible Faults

- Distraction or boredom
- Confusing message

Questions

Contact Information:

Doug Pape
pape@battelle.org

NHTSA Program Lead:
Alrik Svenson
Alrik.Svenson@dot.gov