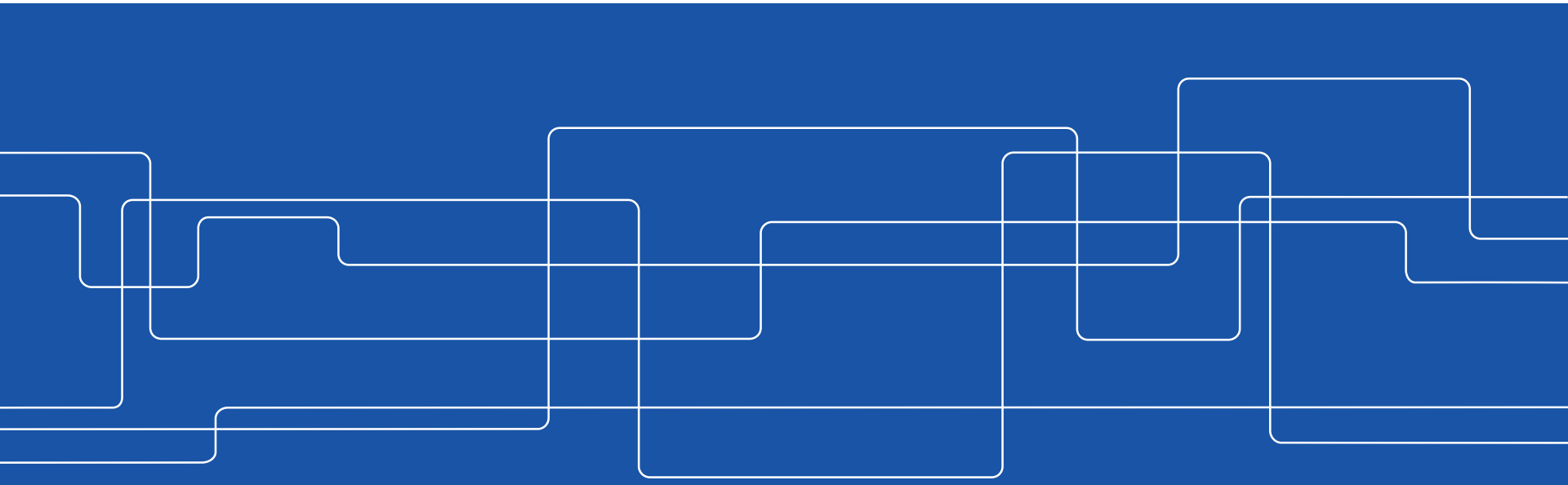
Industrial Safety-Related Considerations to Introducing Full Autonomy in the Automotive Domain

5th Scandinavian Conference on System & Software Safety

Architecture & Safety for Autonomous Systems

Masoumeh Parseh



Introduction

Introduction of autonomous vehicles exposes industrial stakeholders to significant challenges.

SYSTEM ENGINEERING

Four Areas of Considerations

Discussions – Standards & Their Adoption

Standards & Large Transitions:

- Process automation,
- Increase in documentation,
- More and different expert knowledge.

Different perspectives: 1. High expectations 2. checklist

How different perspective deal with transition?

- ❑ Natural transition (1)
- ❑ Legal and market forces to change (2)

Discussions – Dealing with Complexity

How this collaborative relationship will overcome contradictory beliefs among experts?

Two distinct contradictory views on how to handle complexity:

- ❑ New techniques & methods
- ❑ Increase the effort put into current practices

Why should companies invest time, energy and money searching for novel methods?

- ✓ Solution: *New arenas*; fresh and unbiased perspectives.

Discussions – New Methods

Gaps between academy and industry:

- Industry unware of advantages of academic methods.
- Academia unaware of the applicability of methods in industry.

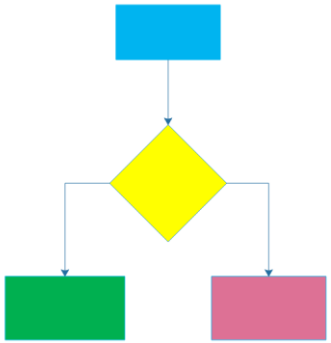
→ promising techniques being rejected, unwillingness of the engineers to learn, resistance.

Solution: involving engineers in decision making, introducing the change gradually.

Conclusion

How to deal with organizational changes and introduction of new roles?

Consolidate new & old methods, roles & processes.



New & old methods be compatible.

People accept the change

Future Work

Facets of complexity drive safety engineering:
environments, algorithms/data/compute platforms, organization

Safety case (ISO): Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development.

Future Work

The Safety Case can be treated ***Dynamically***.

Dynamic: Process/system characterized by constant change/progress.

Future Work

- Safety case is defined before deployment,

Complex safety critical systems:

behavior can dynamically change during deployment,

making safety argument in the safety case invalid.

- New assurance techniques to continuously update the safety arguments based on run-time data: Dynamic safety case

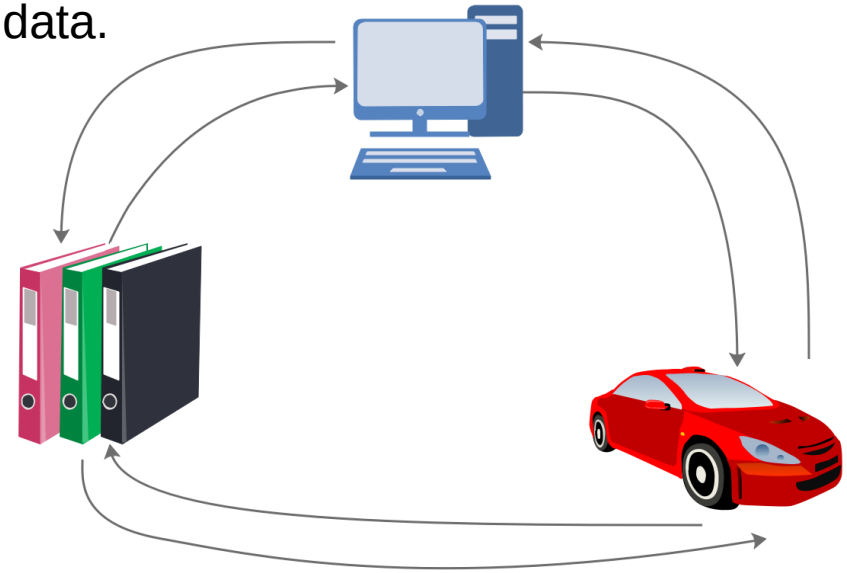
Four stages: 1. Identify, 2. Monitor, 3. Analyze, 4. Respond

Inspired by “Dynamic Safety Case Through-life Safety Assurance” by Ewen Denny , NASA.

Future Work – Interpretations and usage

Dynamic safety case:

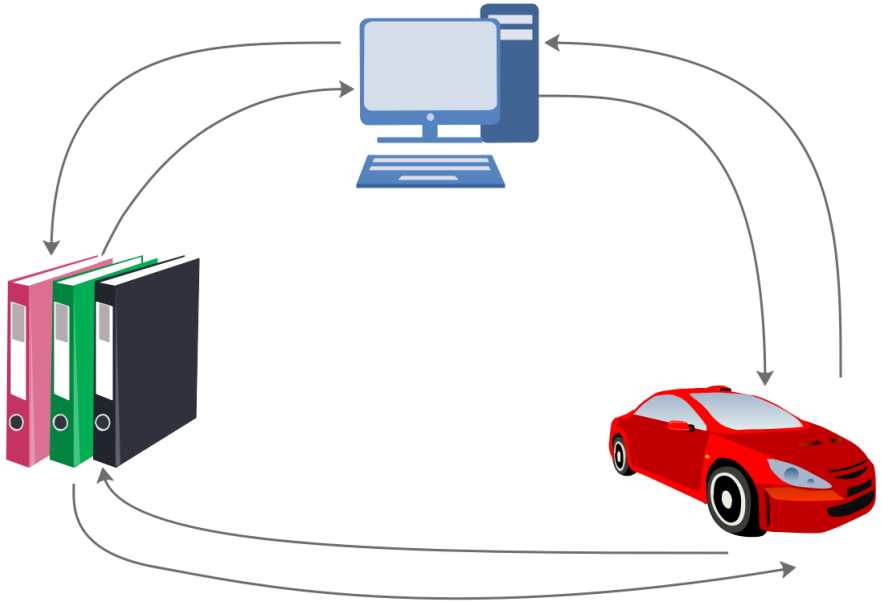
1. Having different safety cases referring to different run-time situations
2. Continuously updating the safety case based on the information obtained from the field data.



Future Work – Interpretations and usage

3. Unknown/unknowns: update the safety case based on what is learned from the data.

- Re-design, re-implementation, V&V and product updates as needed
- Dealing with uncertainty as a cross-cutting aspect



Future Work

1. How well the concept of Dynamic Safety Case is known and applied?
2. Do we need them?
3. How to effectively introduce a dynamic safety case for full automation?
4. What is the impact of Dynamic safety cases on safety analysis?
5. What are barriers for introducing Dynamic safety cases?
6. Is dynamic safety case suitable for all types of systems?

THANK YOU