

USING HAZARD ANALYSIS TO MAKE EARLY ARCHITECTURE DECISIONS FOR AN AUTONOMOUS AUTOMOTIVE APPLICATION

SATURN 2015

Joakim Fröberg



Architecture Analysis for an Autonomous Hauler



A Safe Autonomous Machine: Early Architecture Decisions

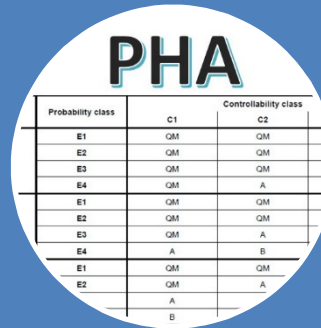


- Functional safety and ASIL? Do we have any hazards?
- Redundancy – Costly and possibly certifiable, So how to do?
- Partitioning – Different criticality separated. How so?

Combining three things



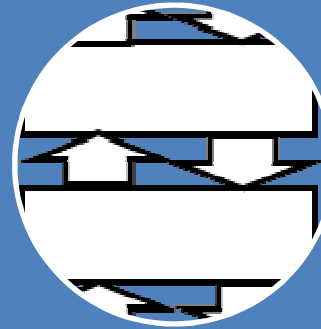
Autonomous
Hauler
Application



PHA

| Probability class | Controllability class | |
|-------------------|-----------------------|----|
| | C1 | C2 |
| E1 | QM | QM |
| E2 | QM | QM |
| E3 | QM | QM |
| E4 | QM | A |
| E1 | QM | QM |
| E2 | QM | QM |
| E3 | QM | A |
| E4 | A | B |
| E1 | QM | QM |
| E2 | QM | A |
| | A | |
| | B | |

Preliminary
Hazard
Analysis



System
Architecture



Study



Autonomous
application scope
and usage

Logic function block
architecture

Preliminary hazard
analysis – ISO26262

Early architecture
design synthesis

Wanted: Method to make early decisions right



Applications of autonomy



- Very different functionality and qualities

Autonomy: scope change



Application – Automated Hauler

- Production – loading and tipping, crusher, piles



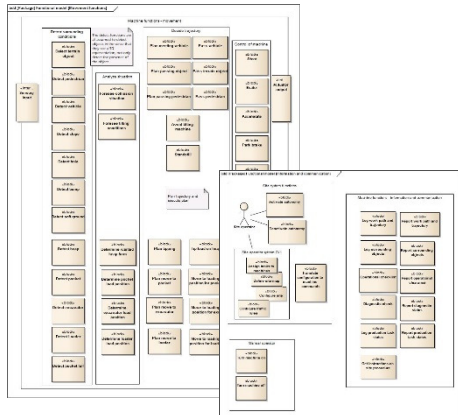
- Scope: Quarry usage
- Site operator at control desk
- Mixed fleet
- People and vehicles

Preliminary Hazard Analysis

| Function | Hazard | Severity | Exposure | Controllability | ASIL |
|-------------------|-----------------|----------|----------|-----------------|------|
| Detect pedestrian | Fatal collision | S3 | E2 | C3 | C |
| | | | | | |
| | | | | | |
| | | | | | |

Presentation Example

Function blocks for system

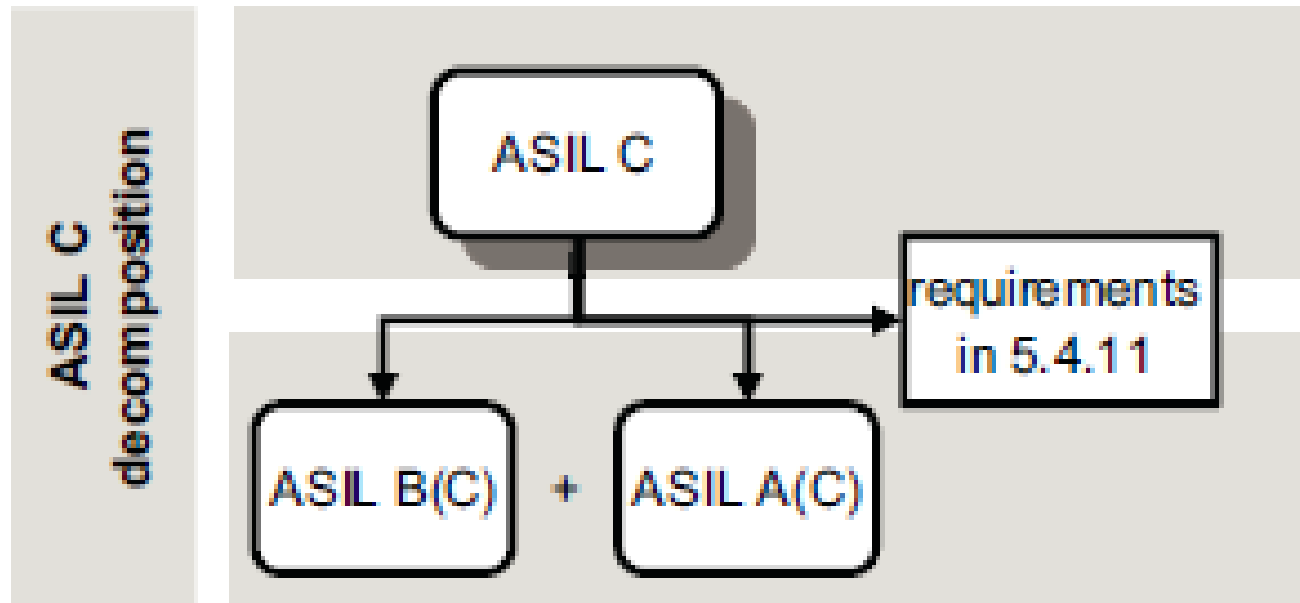


Result
Hazards classified - ASIL

| Function/Block | Source | Failure | Severity | Exposure | Controllability | ASIL | ASIL | ASIL | ASIL |
|----------------|--------|---------|----------|----------|-----------------|------|------|------|------|
| Function/Block | | | | | | | | | |
| Function/Block | | | | | | | | | |
| Function/Block | | | | | | | | | |
| Function/Block | | | | | | | | | |

About 100 Hazards classified

Decomposition - Redundancy



ISO 26262

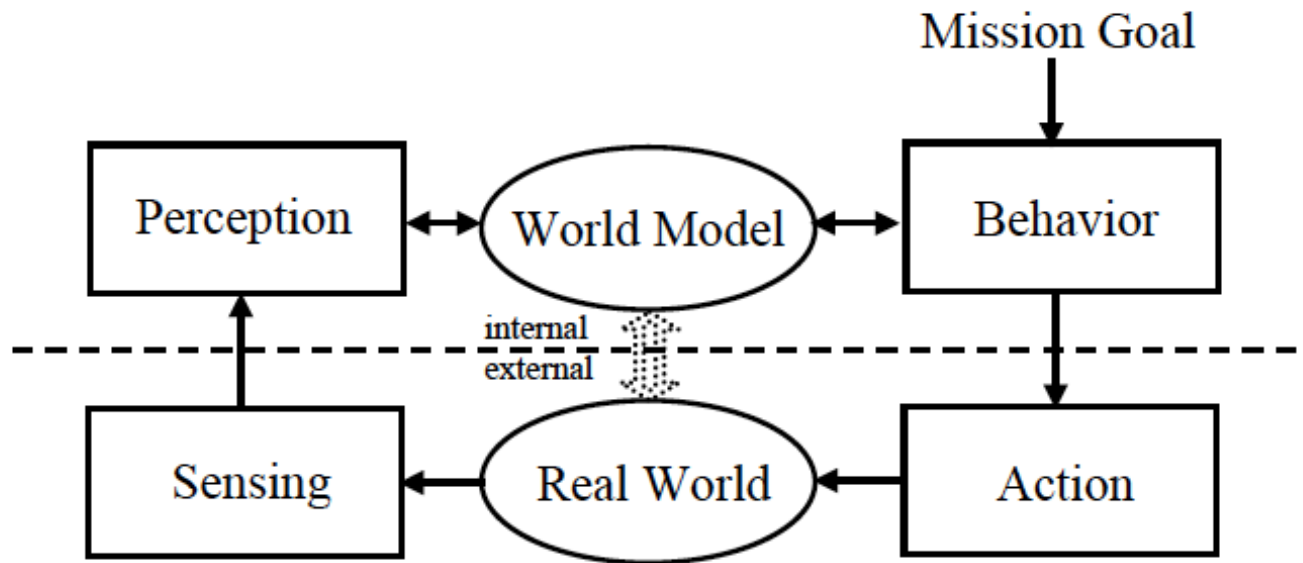
Road vehicles – Functional safety –

Part 9:

Automotive Safety Integrity Level (ASIL)-

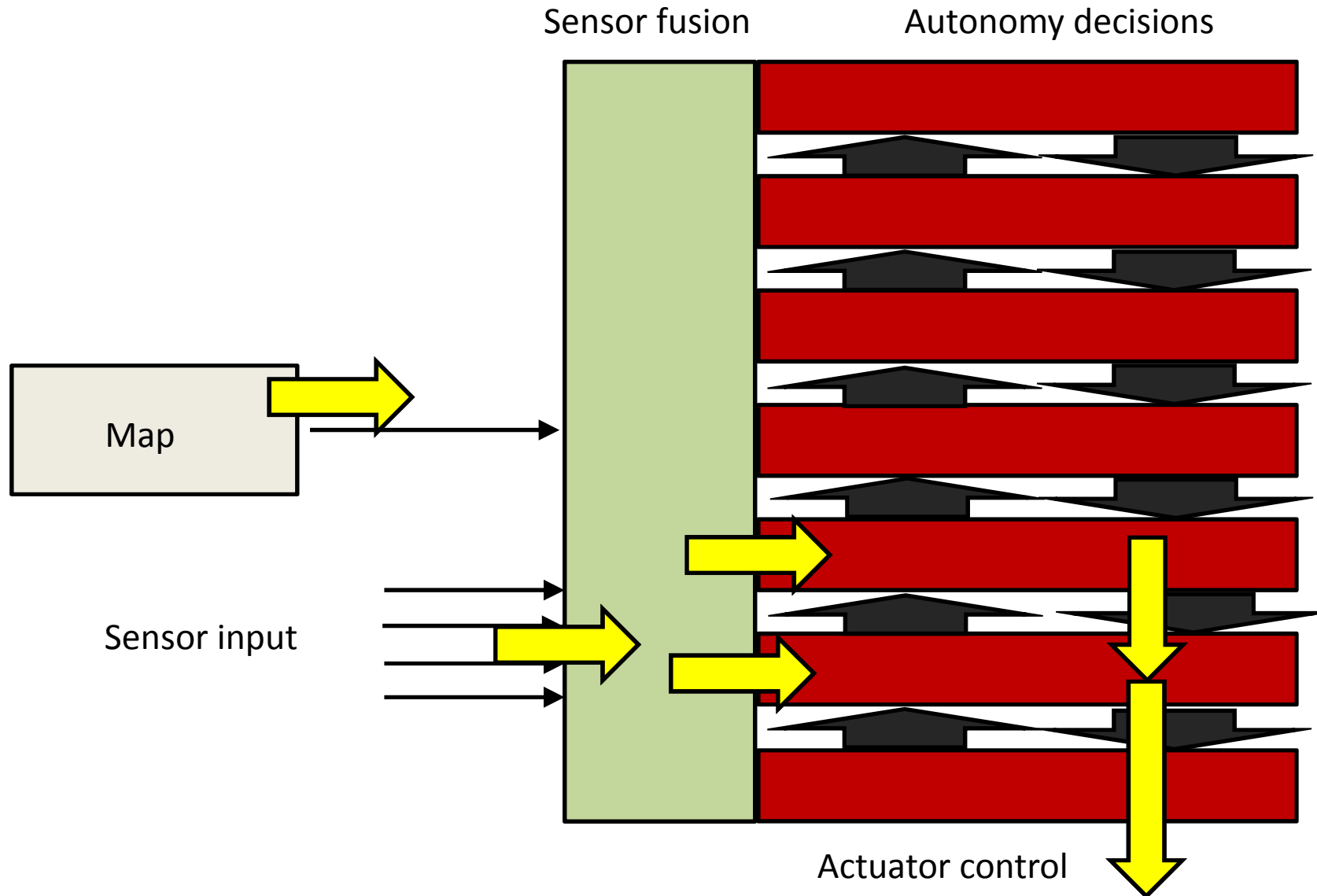
Oriented and safety-oriented analyses

Architecture

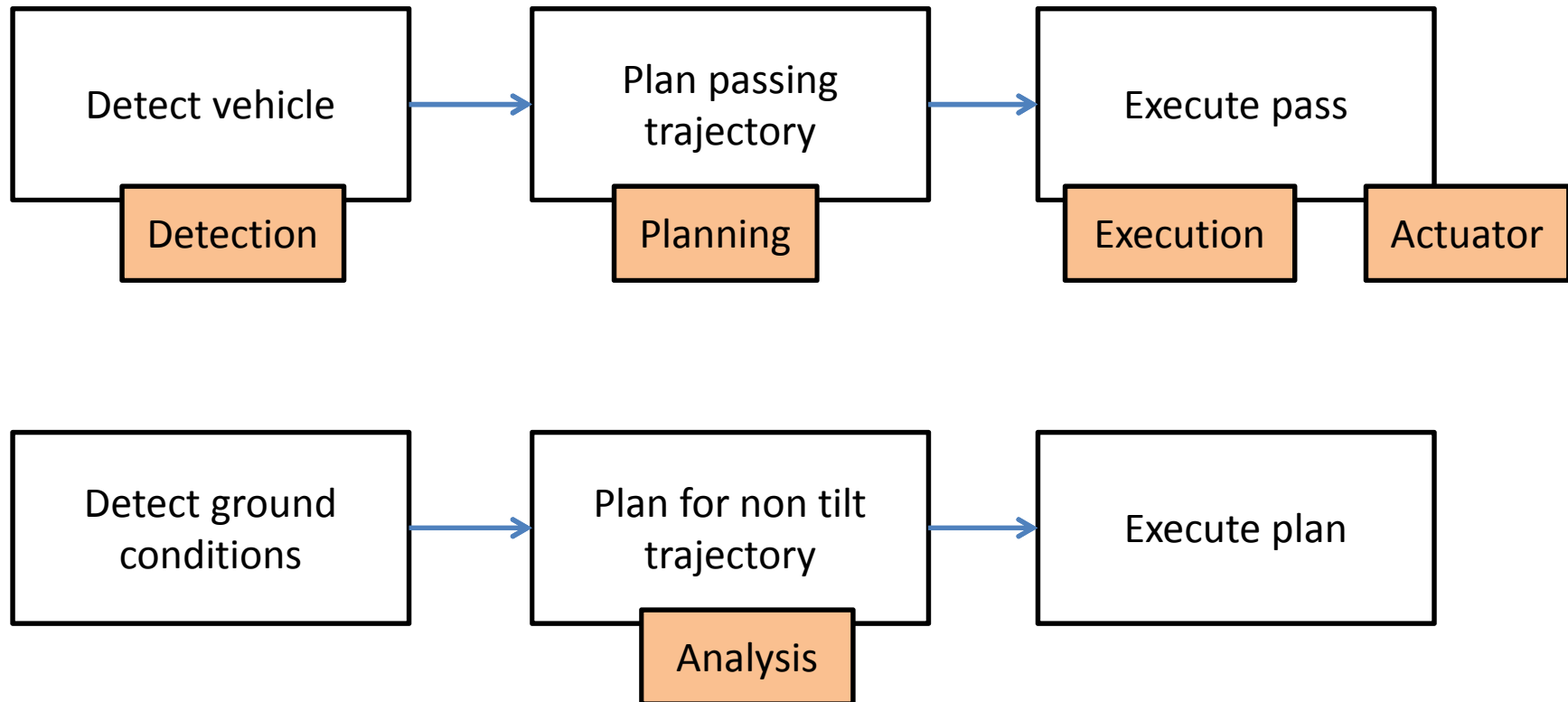


J. Albus et. al. 4D/RCS: "A reference model architecture for unmanned vehicle systems version 2.0," National Institute of Standards and Technology, Gaithersburg, Maryland.

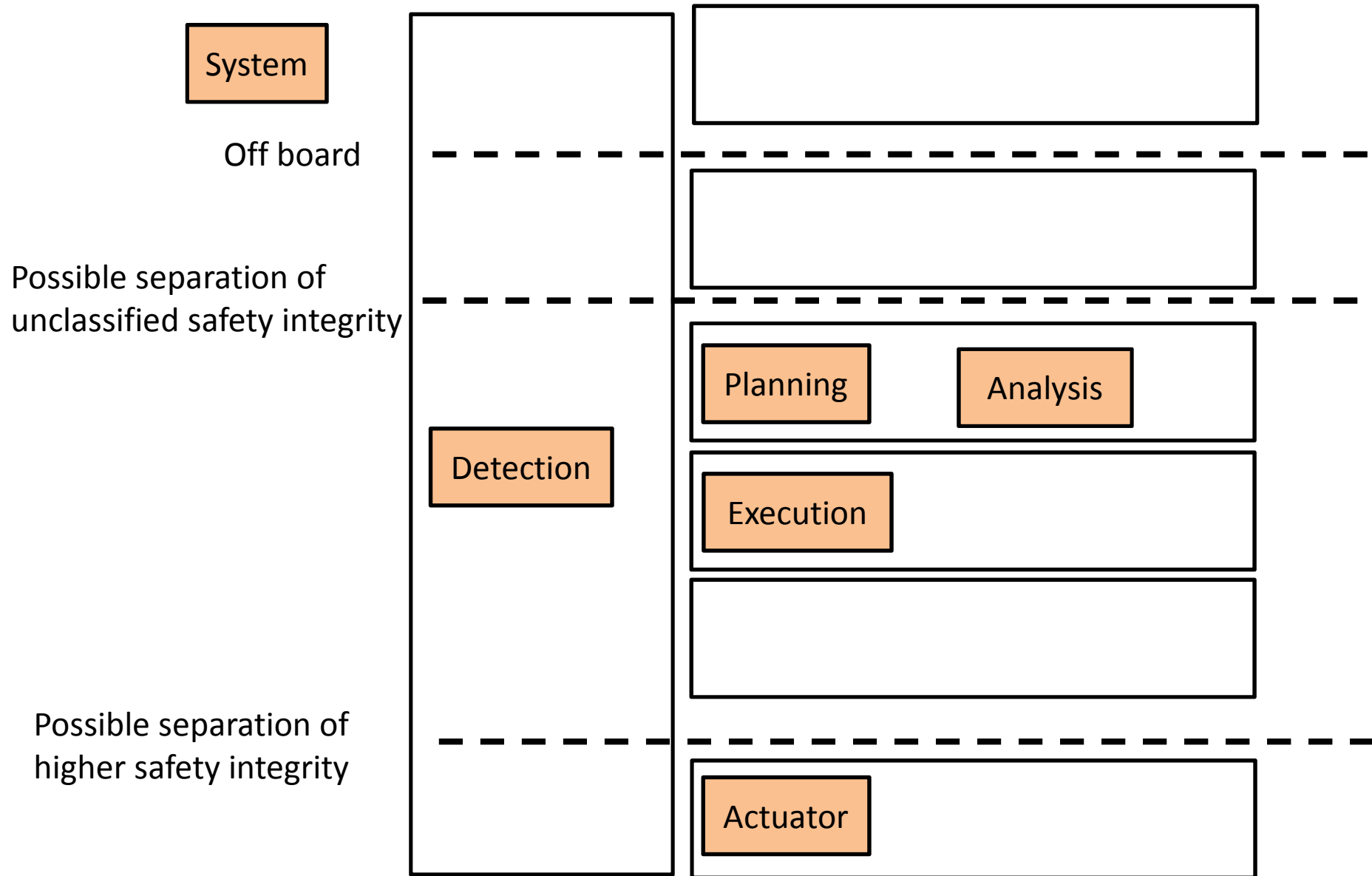
System architecture – a decision stack



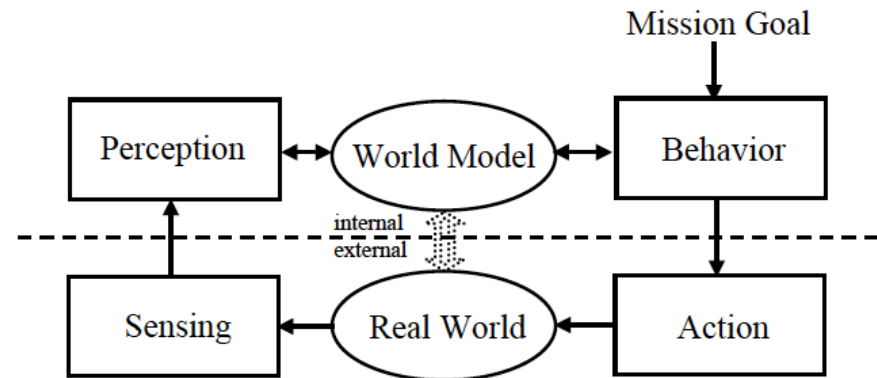
Example



Implications for architecture



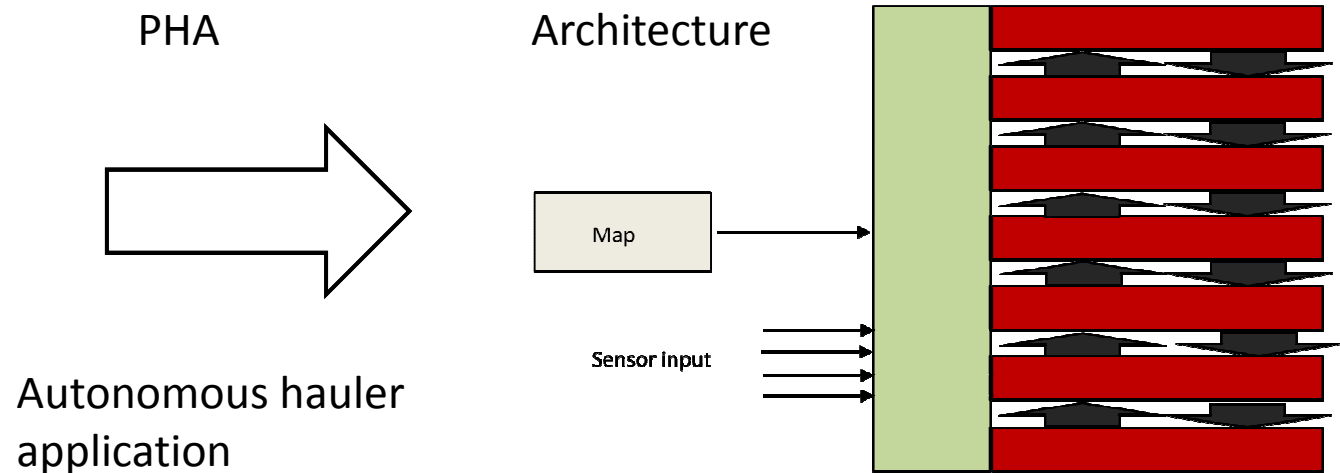
Redundancy & Partitioning



- Redundancy can be employed at perception – difficult at behaviour
- Restrict classified functions to lower layers

Conclusion

- A PHA can aid architecture decisions early
- Separating critical subsystems
- Redundancy suited for perception functions



Contact & Questions

- joakim.froberg@sics.se, joakim.froberg@mdh.se

