

Appropriate Reactions in Embedded Systems

Automotive 2008


Jens Liebehenschel



Dirk Herrmann



About iocon

- Core competencies
Architecture – Design – Methodology
- We offer
 - **Solutions** – supporting your organization's system and software development
 - **Consulting** – teaming up with you to help your development projects succeed, including architecture evaluation according to  **square-m**
 - **Training** – augmenting your knowledge and improving your competence

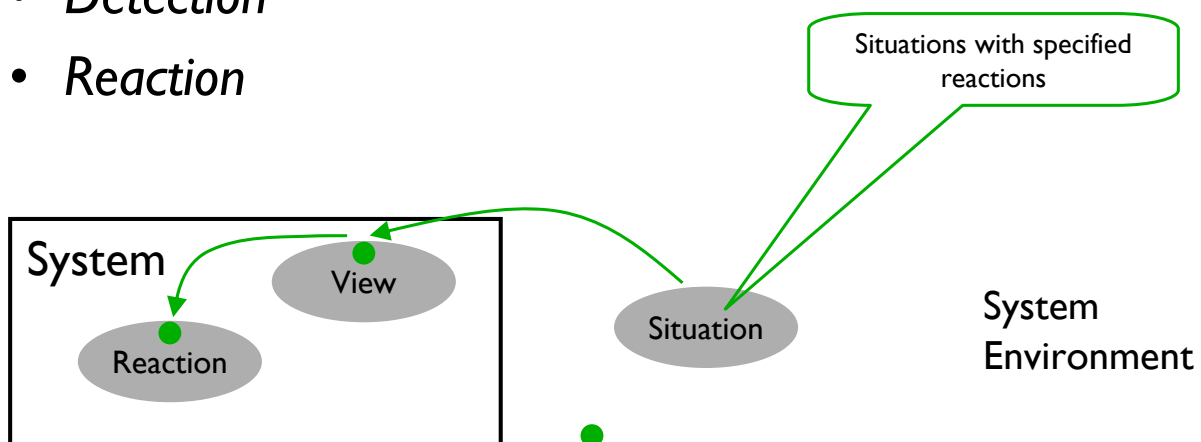
Contents

- Introduction
- Motivation
- Example
- Difficulties
- Approaches
- Summary

3

Introduction

- Requirement: Situation \rightarrow Reaction
- *Situation*
- *View*
- *Detection*
- *Reaction*



4

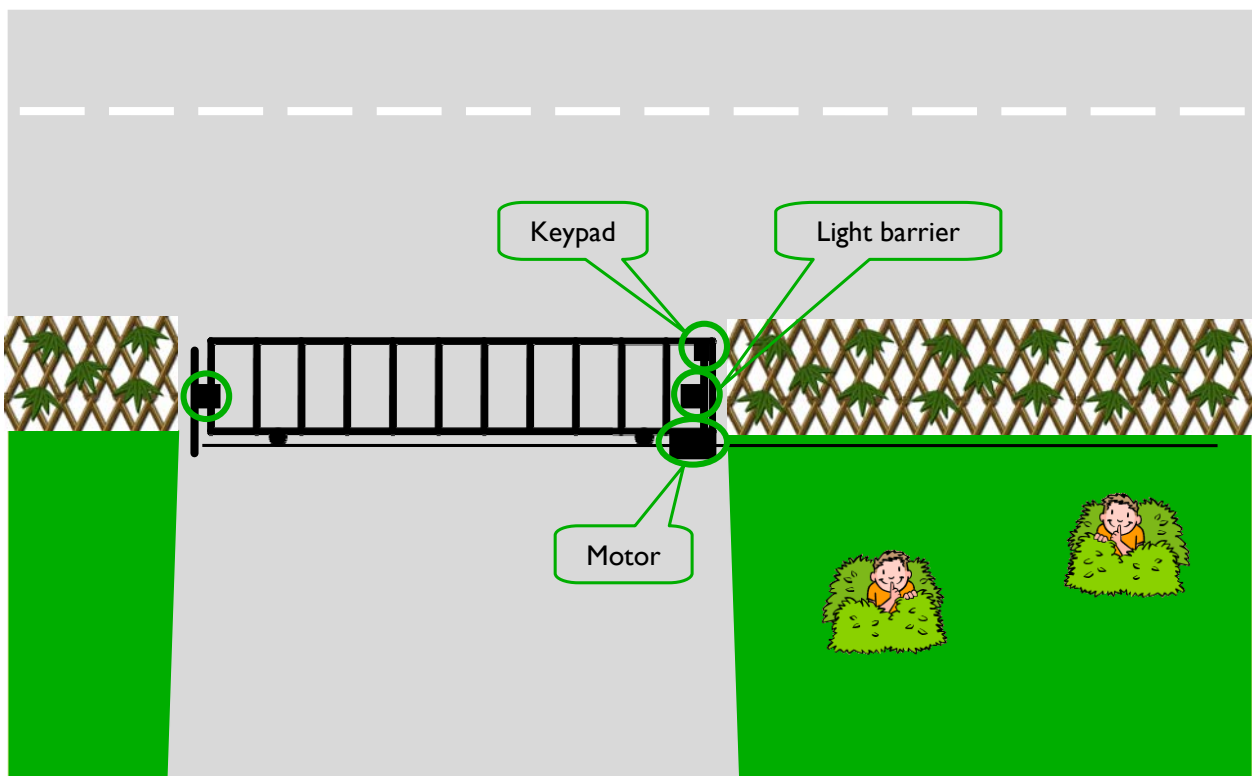
Motivation

Problems in the field (source: internet)

- A small adult is recognized as a child restraint seat. The airbag is deactivated.
- Under certain circumstances the engine accelerates for a short moment.
- Under certain conditions the ABS blocks the wheels on one axis.

5

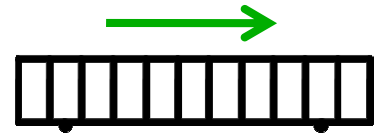
Example: Rolling gate



6

Scenario 1

- Environment: Gate is opening
- Stimulus: Child plays where the gate moves while opening
- Reaction: Gate continues opening
- Problem:

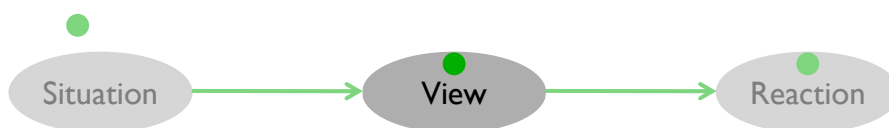


- Situation unexpected or neglected

7

Scenario 2

- Environment: Gate is open
- Stimulus: Child blocks light beam with leaves
- Reaction: Gate will not be closed
- Problem:

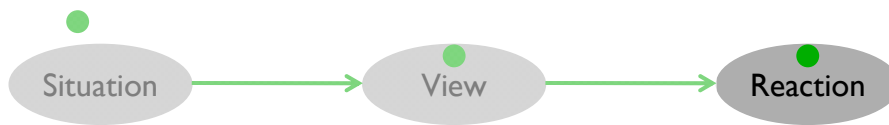
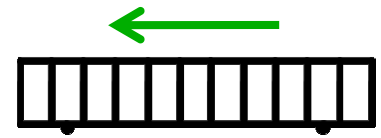


- Leaves and obstacles not distinguishable

8

Scenario 3

- Environment: Gate is closing
- Stimulus: Child puts arm through the gate and interrupts the light beam
- Reaction: Gate reopens
- Problem:



- Reaction not appropriate for all possible situations

Improvement of the gate

- Requirements



- Reaction in case of a detected blocking:
Reverse for a short time, then wait, after
timeout continue initial movement

- Design



- Additional blocking detection by current
measurement
- Blocking detection also while opening

Difficulties in designing reactions



- Which situations to consider
- Probabilities often unknown



- Limited sensory information available
- Several situations map to a single view



- Reaction must fit to all situations for view

11

Consideration of requirements

Checklist

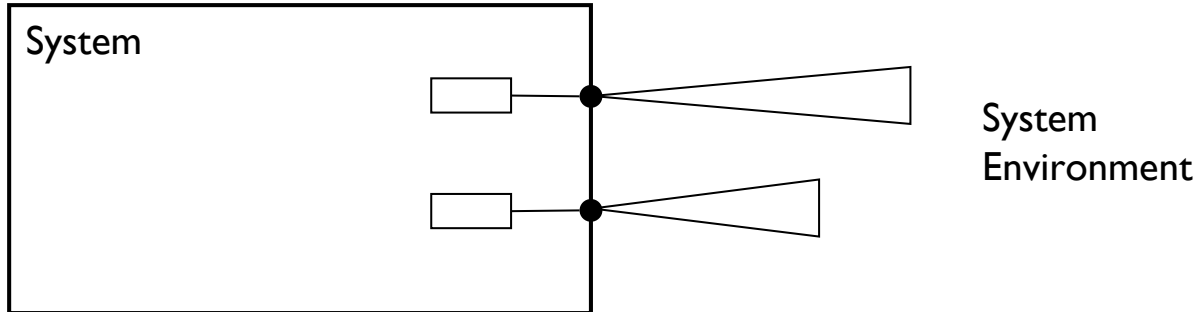
- Requirements complete?
 - All relevant situations considered?
 - Situations resulting from system structure?
- Reactions appropriate?
 - Changes of system mode
 - Reaction time and duration
 - Driver information and diagnostics






12

Limited information

Problem: Mapping situations and views

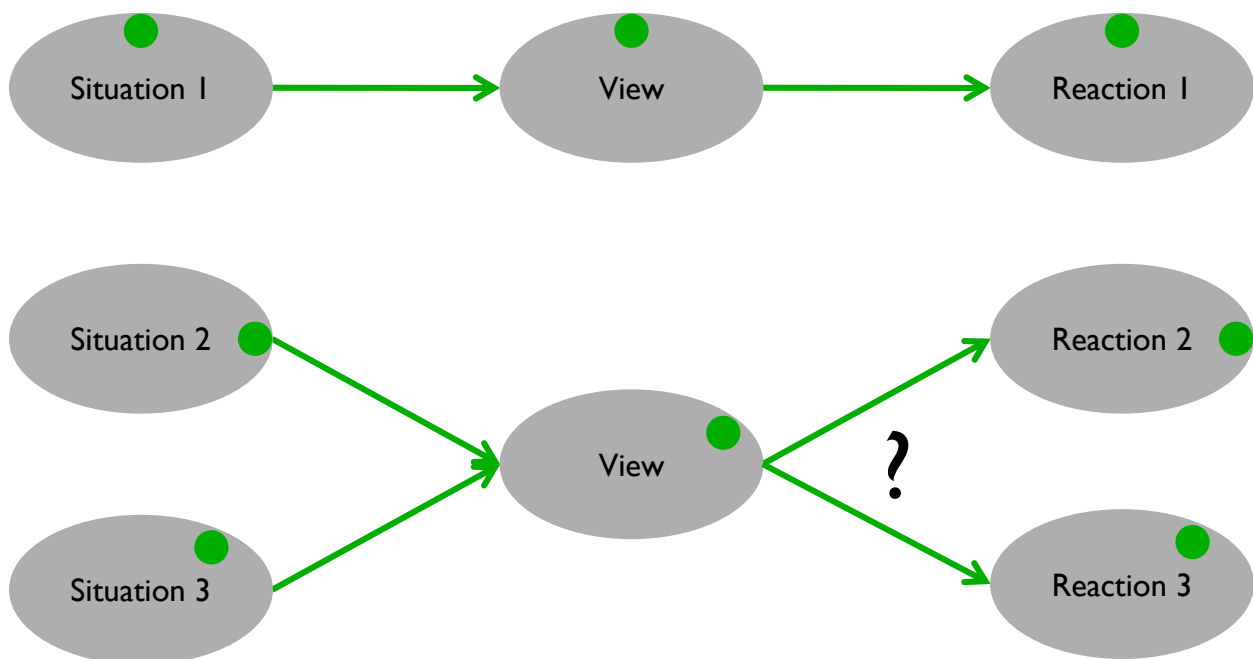


Legend:

-  Sensor and area of surveillance
-  Connection
-  Current sensory data

13

Limited information

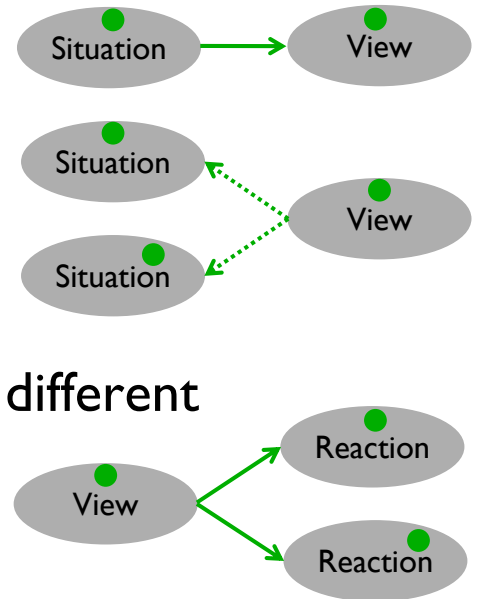


14

Limited information

Determine

1. situations by means of views
2. all situations for given views
3. situations with the same view and different reactions

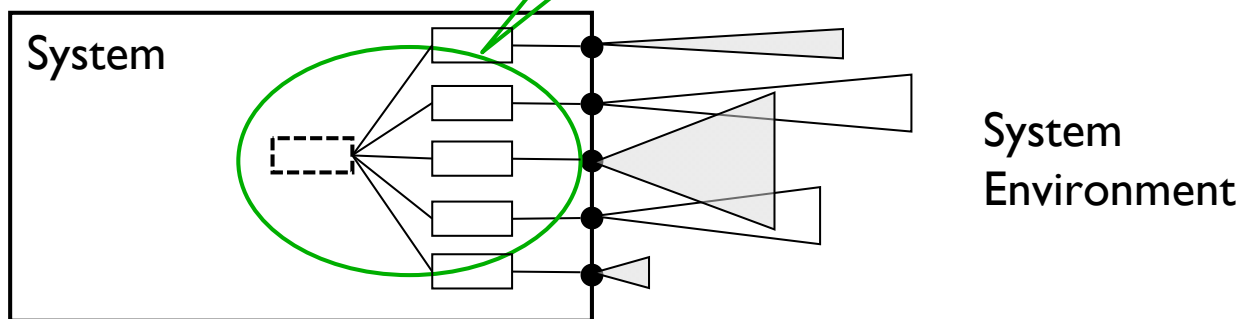


What if sensory view not sufficient?

Limited information

Mechanisms

Models

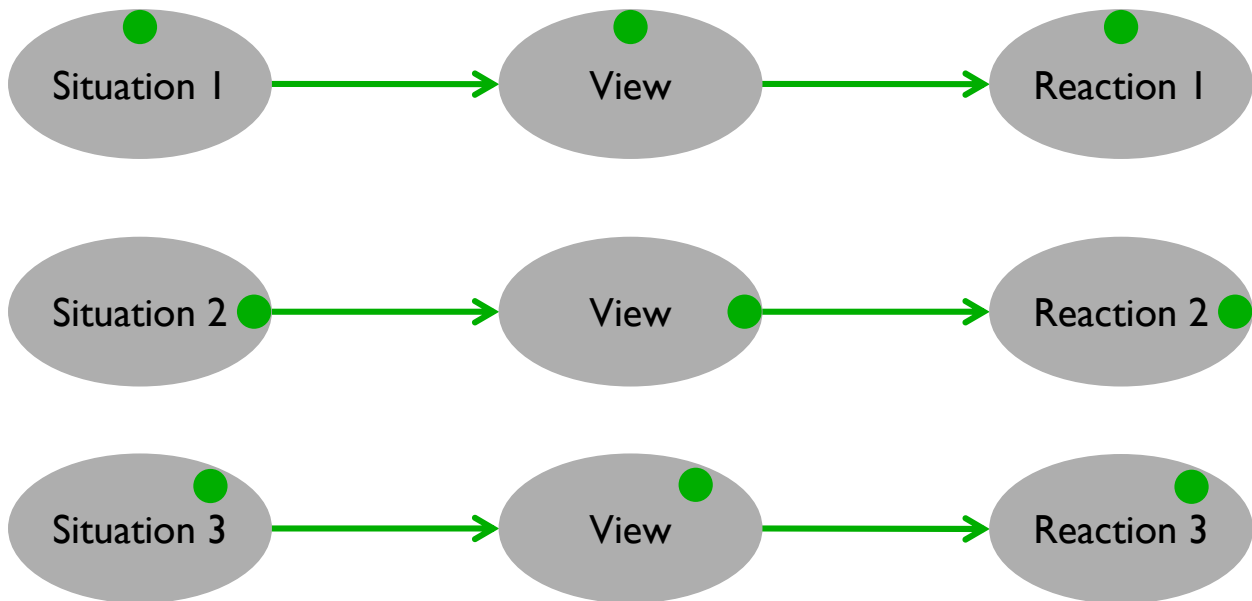


Legend:

-  Calculations (historic data, plausibility checks, ...)
-  Additional / other sensors and area of surveillance

Limited information

More situations can be distinguished now



17

Probabilities

Checklist

- Practically irrelevant scenarios?
- Conditional probability considered?
- Impact and likeliness of false positives or false negatives?



18

Reactions

Checklist



- Reaction fits to situation?
 - Only view of situation present
- Reactions too pessimistic?
 - More safety / security than required
 - Availability reduced

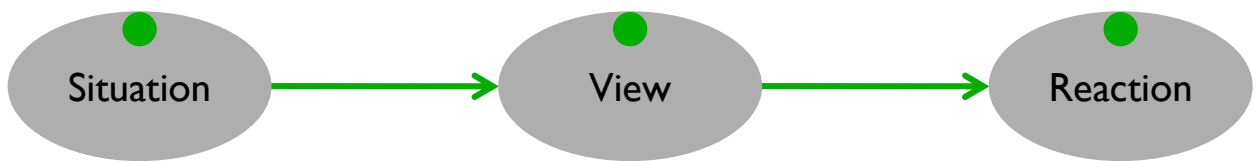
Keep it simple

Scenario

- Situation
 - Small probability
 - Difficult to detect
 - High complexity and cost for detection
 - Reduced safety / security
- Ignoring this situation implies better system

Summary

- Create awareness for reactions



- Approaches for designing reactions
- Come closer to optimal trade-off between safety, security, and availability

Thank you!

