Identification of Item Interactions for Functional Safety

Markus Baumeister, CTPCS, Continental

International VDI-Workshop “Item Definition Based on Product Liability Laws and ISO 26262 of future ADAS”

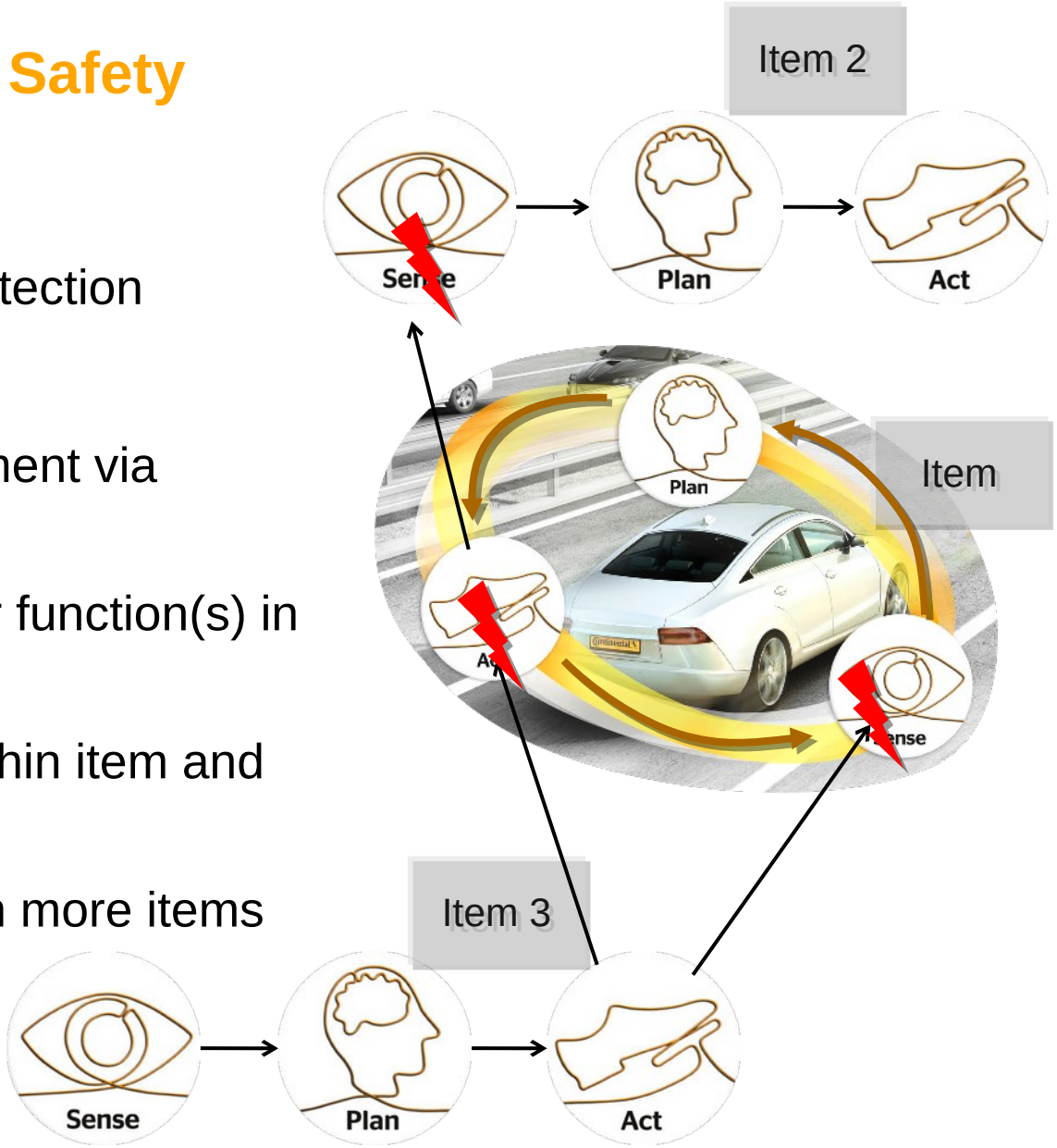
11. May 2015

Contents


Safe and Dynamic Driving
towards VISION ZERO
ZERO ACCIDENTS
ZERO INJURIES
ZERO FATALITIES
Plan
Act
Sense
Continental

Item-based Functional Safety

- Item executes a function
  - E.g. Lane Departure Protection
- Item-environment boundary
  - Interaction with environment via sensors and actuators
- Hazard and risk analysis for function(s) in item
- Safety concept for faults within item and failures in environment
  - Environment can contain more items



Environment of Multi-functional Car Systems

Example: Continental Chassis & Safety ADAS Functions

Normal Driving | **Safety Functions**

- Parking
- Urban Assist
- Predictive Suspension Control
- Intelligent Headlamp Control

- BT Adaptive Cruise Control
- S Lane Keeping Assist
- BST Traffic Jam Assist
- Chauffeur/ Highly Automated Driving
- Overtaking Assist

- B Emergency Brake Assist
- S Lane / Road Departure Protection
- S Lateral Collision Avoidance
- S Emergency Steer Assist
- BT Emergency Stop Assist
- Back-up Assist

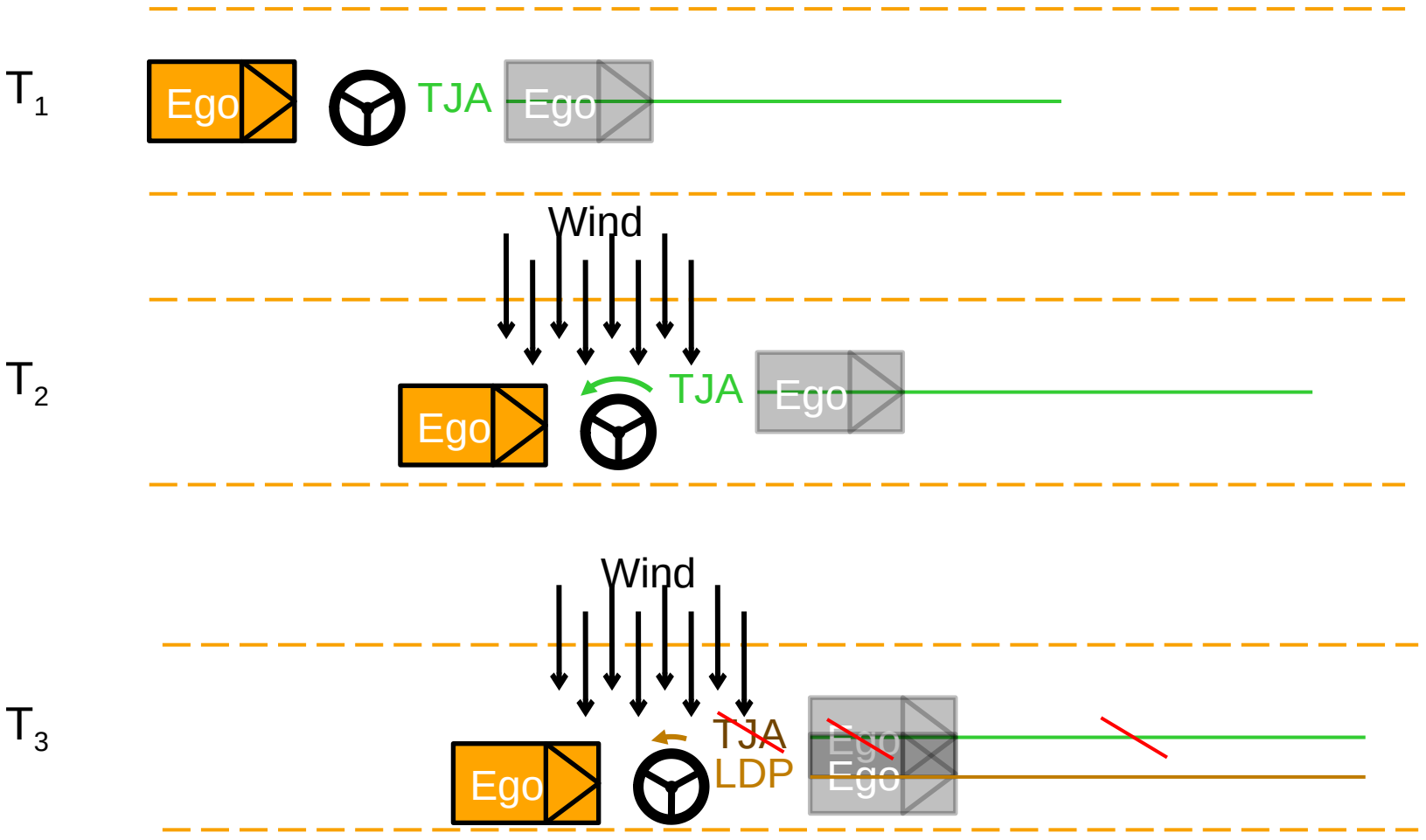
B = Brake
S = Steering
T = Throttle

V2X

› **V2X / ADAS functional integration (Cooperative** ACC)

› **Standalone warning + intervention**
› **V2X / ADAS functional integration (**EBA/ESA)

Potential Interaction: TJA vs. LDP



Item Interaction and Hazards

- Steering over lane markings is a hazard
  - Controlability unclear, so maybe not safety-relevant
- All individual items are working according to spec

⇨ **Hazards can occur due to interaction of *correct* items**

- Solution: Item = Car?
- Better: **Find way to identify interactions and hazards**

Contents

ISO 26262-3 on Item Interactions

ISO 26262 acknowledges item interaction

5 Item definition

5.1 Objectives

The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

But later steps are item-centric in standard (and in practise)

7 Hazard analysis and risk assessment

7.1 Objectives

The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

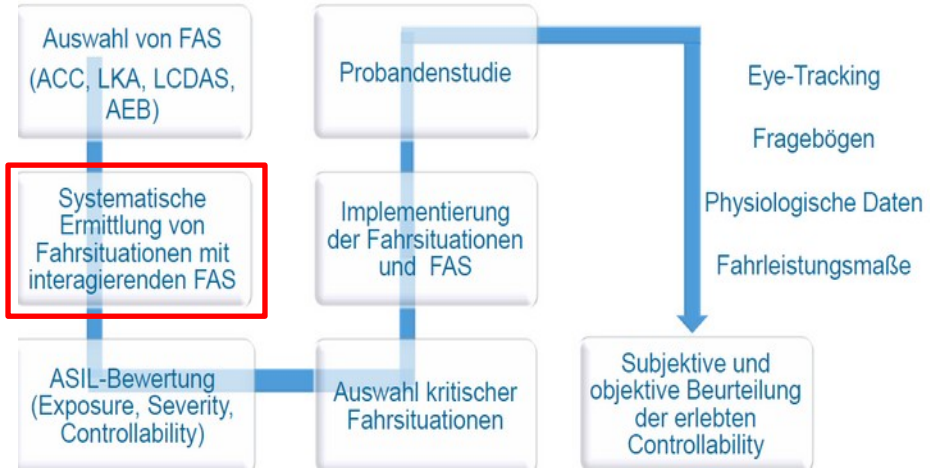
Other Approaches: ConFas (TU Berlin)

Goal: Determine controllability of interactions

Simulation of situations where two system interact

Identification of situations using a catalog of driving scenarios and situations

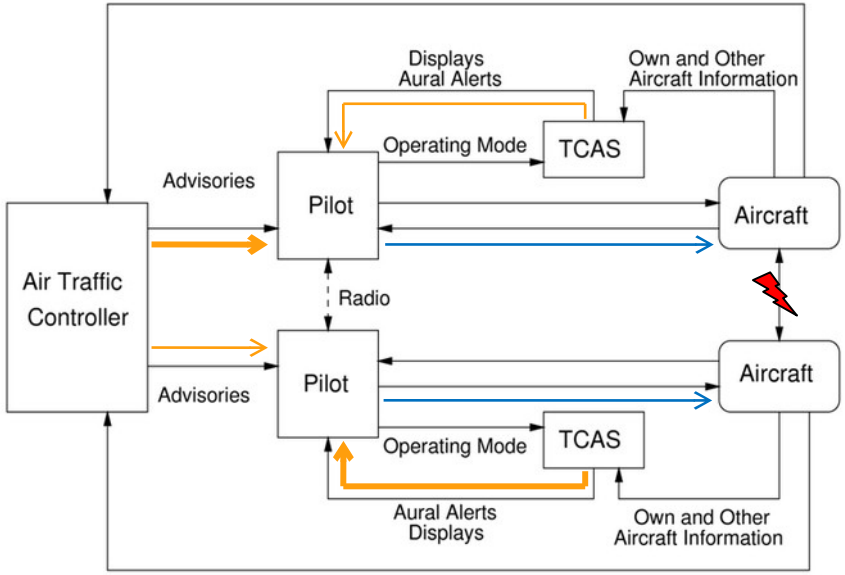
Examined situations had one FAS system hinder the driver in correcting another



(both from O.Schädler, Experimentelle Bewertung der Beherrschbarkeit von interagierenden Fahrerassistenzsystemen anhand kritischer Fahrsituationen; AAET 2015)

Other Approaches: STPA (N. Leveson et al.)

- Assumption: Accidents are caused by inadequate control
- Goal: Define constraints on component behaviour and interactions
- Includes human behaviour, regulations, laws, …
- Keyword-based search for control action (=part of interaction) failures



Systems model for the “Überlingen incident”, from Nancy Leveson, "A new approach to hazard analysis for complex systems" , *International Conference of the System Safety Society*. 2003.

Keywords: Control action
- incorrectly provided
- incorrectly not provided
- provided with incorrect timing
- provided with incorrect duration

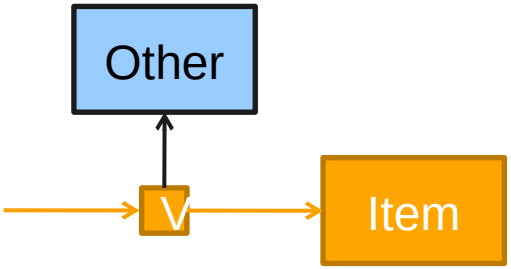
Contents

Interaction Identification Approach

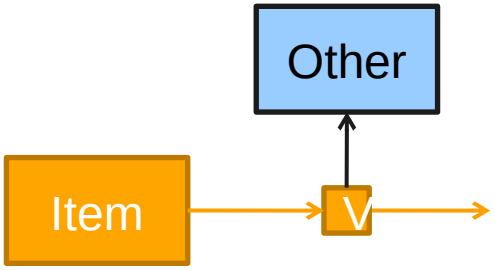
- Once known, interaction can be regulated/prevented
- Items interact via values
  - Functional: Signal (groups)
  - Physical: Physical quantities

- **1. What kinds of interaction exist?**
- 2. How to identify them?

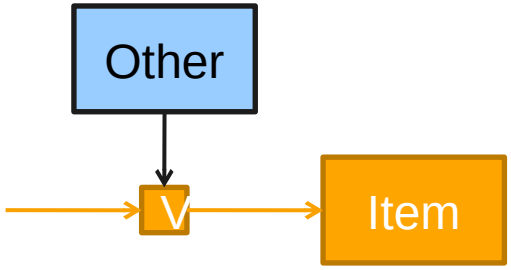
Classification of Interaction Possibilities



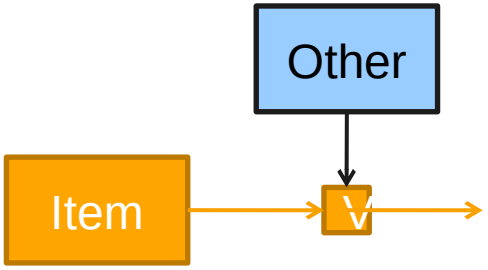
Read Input



Read Outputs



Write Input



Write Outputs

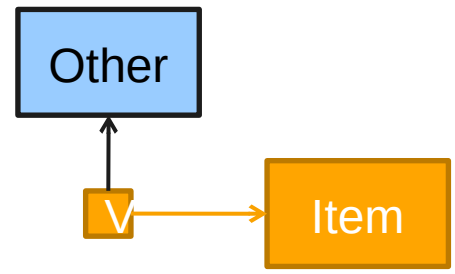
Potential Interaction Consequences

and possible countermeasures

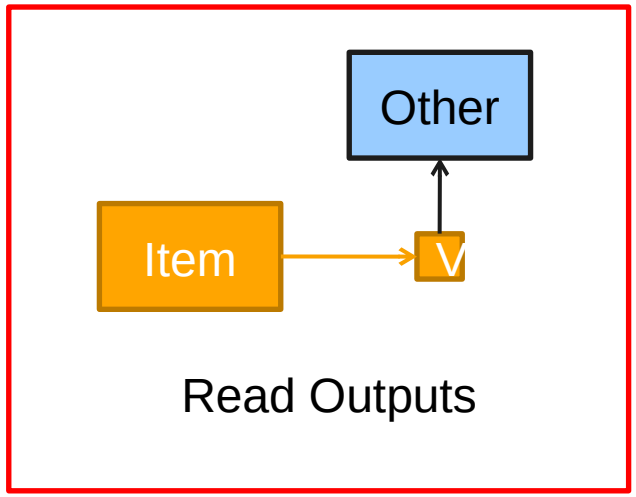
- „Other“ & Item write same outputs
  - Overwrite each other
    - Access Coordination
  - Add up and grow over limits
    - Limiter or Access Coordination
  - Confuse user by sequential actions
    - Dead time
  - Provide action ignoring other‘s (old) intervention

    („TJA vs. LDP“ example)
    - Observe previous actions
    - Dead time

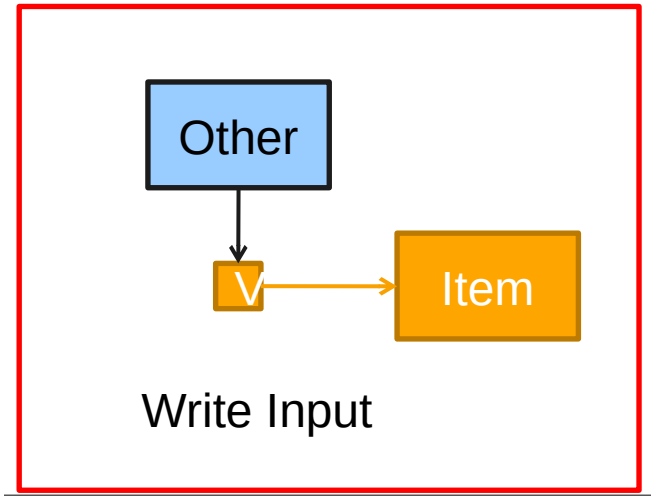
Interaction Possibilities 2



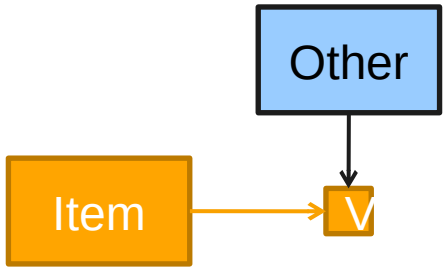
Read Input



Read Outputs



Write Input



Write Outputs

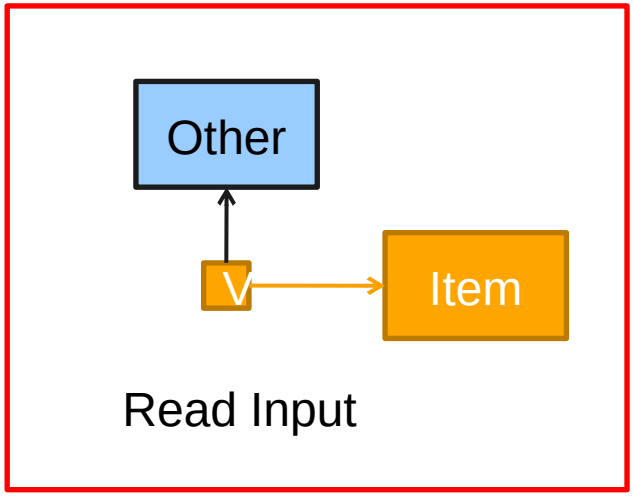
Potential Interaction Consequences 2

and possible countermeasures

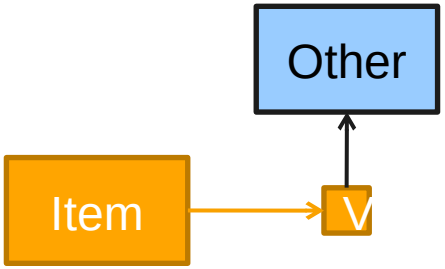
- „Other“ writes Item‘s Inputs
  - Other‘s output misidentified as driver intention
    - Observe other‘s outputs
  - Falsify read values
    - Observe other‘s outputs
  - Unsynchronized Changes
    - Read all data at beginning of time slot
- „Other“ reads Item‘s Outputs

  Analogous but consequences for Other

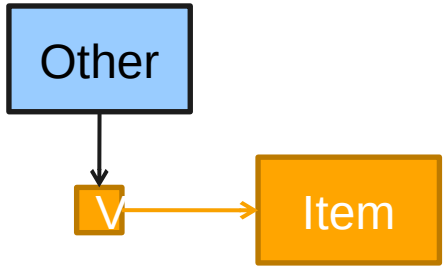
Interaction Possibilities 3



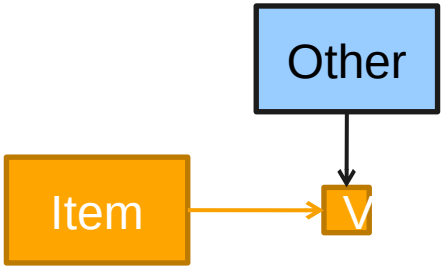
Read Input



Read Outputs



Write Input



Write Outputs

Potential Interaction Consequences 3

and possible countermeasures

- „Other“ & Item read same Inputs
  - (Dead)Lock access to data
    - Deadlock prevetion/detection
  - Bring used sensor into different modes

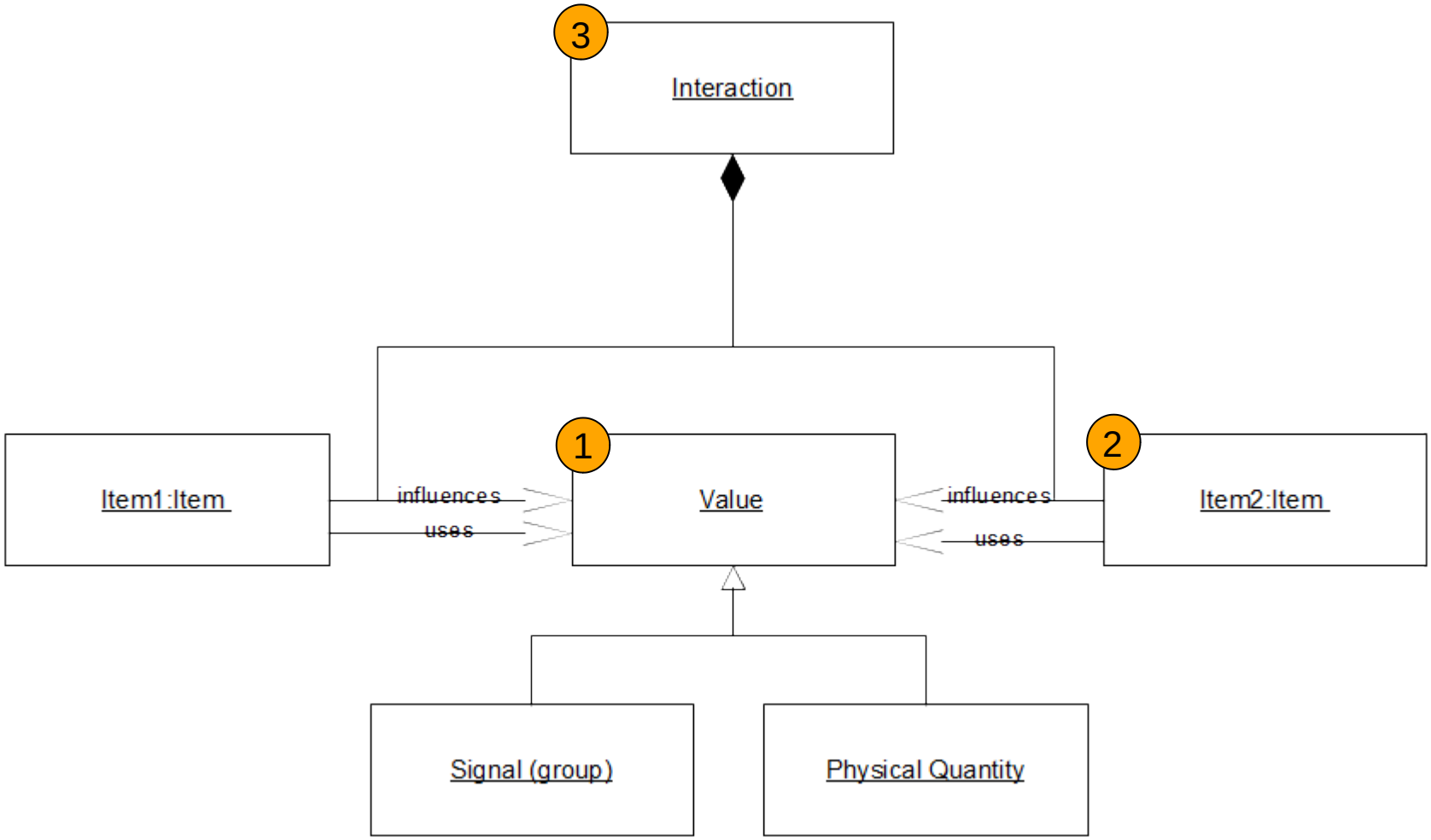
    (e.g. Long-range vs. Short-range evaluation of radar)
    - Central sensor management

Interaction Identification Approach

- Once known, interaction can be regulated/prevented
- Items interact via values
  - Functional: Signal (groups)
  - Physical: Physical quantities

- 1. What kinds of interaction exist?
- 2. How to identify them?

Metamodel of Interactions



Potential Approach

- 1 Identify all interfaces
  - Signal groups as well as physical quantities
- 2 Identify all other items using same interfaces
  - Read/Write Input/Output
    - (Except Read Input)
- 3 For each item & interface identify and evaluate potential interactions
  - Using a keyword list

3 Steps, 3 Excel Pages

Interfaces

Itemname

Functional Interfaces

Inputs

Value or Signal

Outputs

Value or Signal

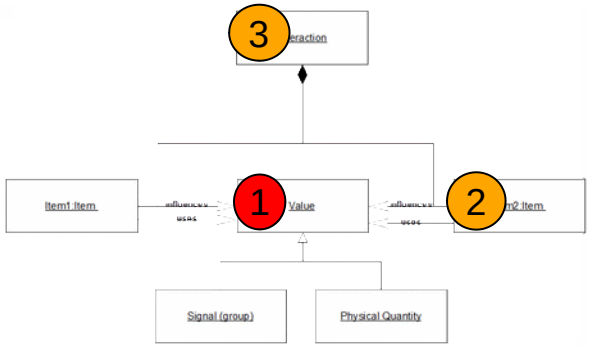
Physical Interfaces

Inputs

Value or Signal

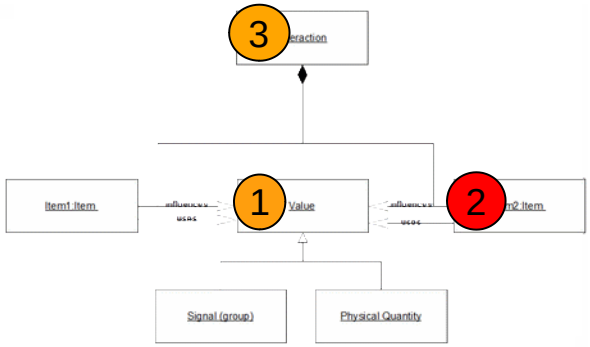
Outputs

Value or Signal



3 Steps, 3 Excel Pages

Other items

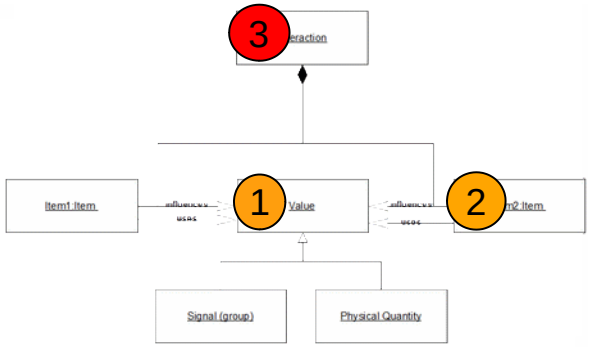


Functions interacting with *Itemname*

Interfaces	**Other Functions**
Reading Inputs (only check for deadlocks, etc.)	
Value or Signal	*Function 1*
Value or Signal	*Function 2*
Reading Outputs	
Value or Signal	*Function 3*
Value or Signal	
Write Inputs	
Value or Signal	*Function 4*
Value or Signal	*Function 1*
Write Output	
Value or Signal	*Function 4*

3 Steps, 3 Excel Pages

Other items



Potential interaction effects of other items with *Itemname*

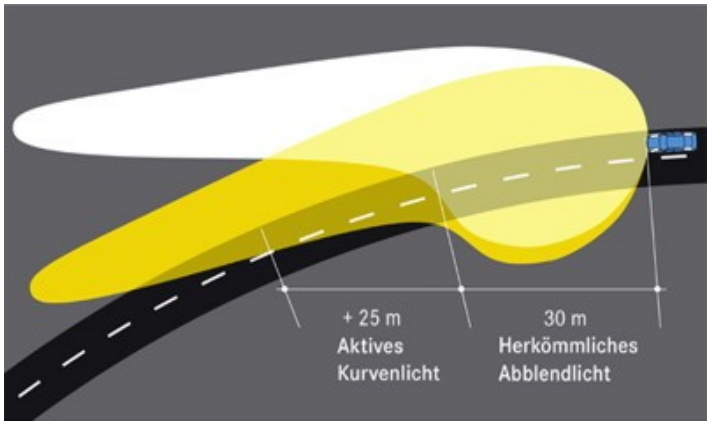
Reading Outputs	**Other function**	**What is the effect if the item changes the output (which is input to the other functions) in the following ways**					**Countermeasures**
		1) more Output is increased (slowly/quickly) over original value	2) less Output is decreased from original value	3) inverse Output gradient changes direction (i.e. increase <-> decrease)	4) before Output is changed before other functions acts	5) after Output is changed after other function acts	
Value or Signal	*Function 1*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	Potential countermeasures against each consequence
Value or Signal	*Function 2*						

Writing inputs	**Other function**	**What is the effect if the other functions changes its output (which is input to the item) in the following ways**					**Countermeasures**
		1) more Output is increased (slowly/quickly) over original value	2) less Output is decreased from original value	3) inverse Output gradient changes direction (i.e. increase <-> decrease)	4) before Output is changed before other functions acts	5) after Output is changed after other function acts	

Contents

Example Systems for Interaction Analysis

› Advanced front-lighting system (“Kurvenlicht”) turning the headlamps



Kurvenlicht_dyn.jpg from www.bs-wiki.de

› Light assistant switching on/off headlights and high beam

from motor-talk.de

› Drift assistant helping to drive through curves oversteering

from www.tmwerkes.ca

Practise

Experiences of practise

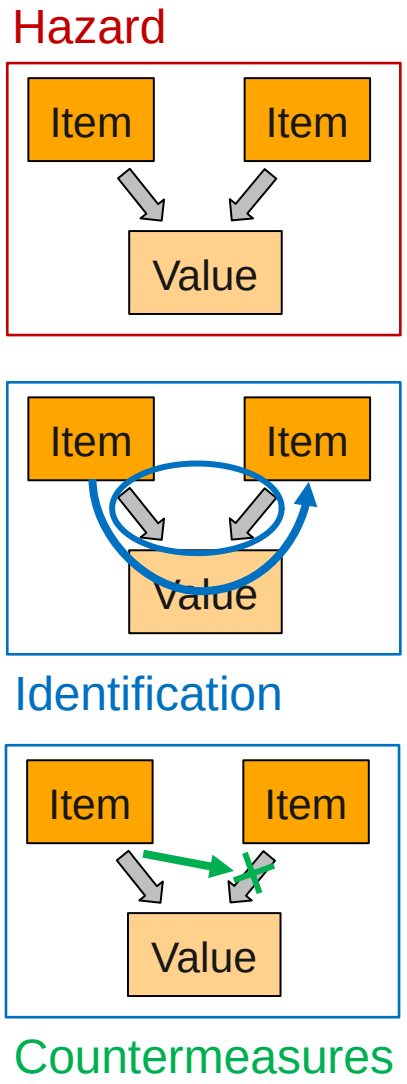
- Things that worked well / badly ?
- Additional keywords?

Limitations of Shown Approach

- Some interactions will not be identified:
- Physical relationsships
  - E.g. two planes cannot be in same airspace simultaneously
  - E.g. braking and steering both use up adhesion
    - Could use „adhesion“ as physical quantity
- Driver limitations
  - E.g. drivers are less experienced with simultaneous steering and braking
- Effects within normal control chains
  - Part of one item

Summary

- Interaction of correctly functioning systems can cause hazards
- Analysis approach
  - Following influenced signals/quantities
  - Keyword-based interaction identification
  - Countermeasures definition



Questions and … Questions

- Your questions!

- My questions:
  - Do **you** analyze item interactions?
    - Example interaction hazards found which can be shared?
  - Systematic approach at identification?
  - Approach to determine controlability?
  - Interactions of items in different cars?

Thank you

for your attention!

Backup Slides

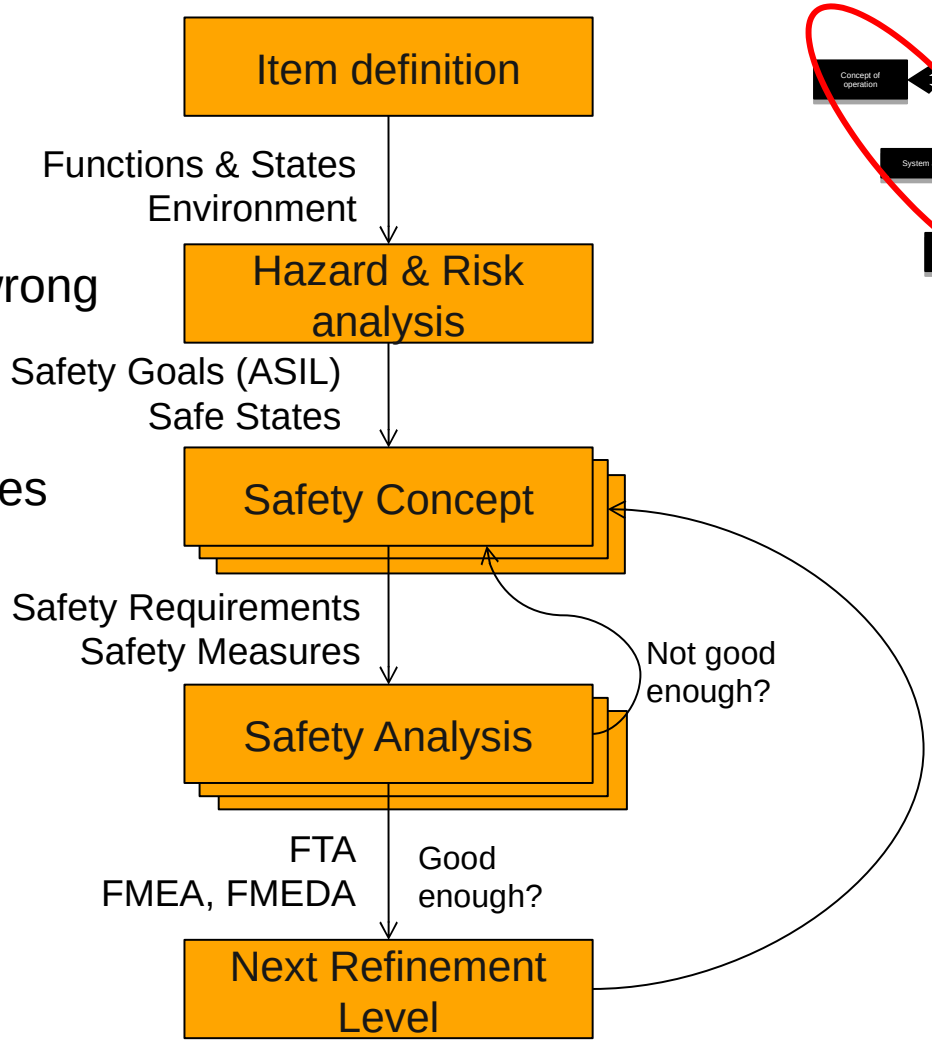
The specification leg of the V-model

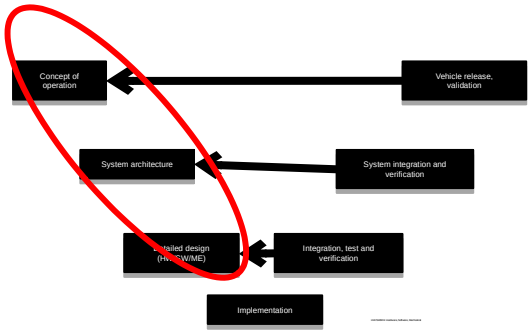
Know what you do

Know what could go wrong

Define countermeasures

Evaluate Sufficiency





Identification of Failure Modes – Systematic Brainstorming

- Hazard and Operability Study (HAZOP)
  - First applied in chemical industry to identify potential hazards caused by deviations from design intent
- Approach
  - Find ways an item/component can fail based on two sets of keywords
  - Primary: Intentions or Functions of component
    - Particular aspect of design or parameter
    - Differ from component to component
  - Secondary: Deviation hints
    - Possible deviations
    - Standard Set of keywords
- Alternative result: Consequences

HAZOP secondary keywords

Keyword	General Meaning	Example Primary Keyword: Steering
No	Function not performed / unachieable	No steering moment; Steering locked
More	Quantitative increase	Too much/too long steering moment
Less	Quantitative decrease	Too few/Too short steering moment
Also	Qualitative increase (something in addition)	Vibration while steering; Steering wheel height modified
Part	Qualitative decrease (something missing)	--
Reverse	Opposite than intended	Steering moment in opposite direction
Other	Not where or how expeced (something different)	No steering moment but braking; Unexpected steering moment
Fluctuation	Not achieved all of the time	Steering moment ‚stutters‘
Early	Function performed too early	Too quick moment buildup
Late	Function performed too late	Steering moment buildup too slow


Safe and Dynamic Driving
towards Vision Zero
SensePlanAct
Chassis & Safety
Continental
Continental

Identification of Item Interactions for Functional Safety

Markus Baumeister, CTPCS, Continental

International VDI-Workshop "Item Definition Based on Product Liability Laws and ISO 26262 of future ADAS"

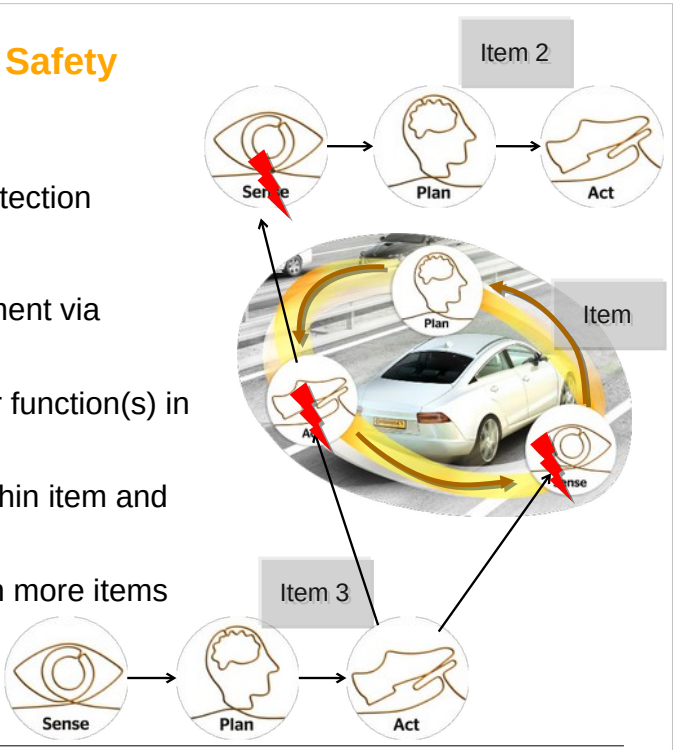
11. May 2015

Contents


Safe and Dynamic Driving
towards VISION ZERO
ZERO ACCIDENTS
ZERO INJURIES
ZERO FATALITIES
Plan
Act
Sense

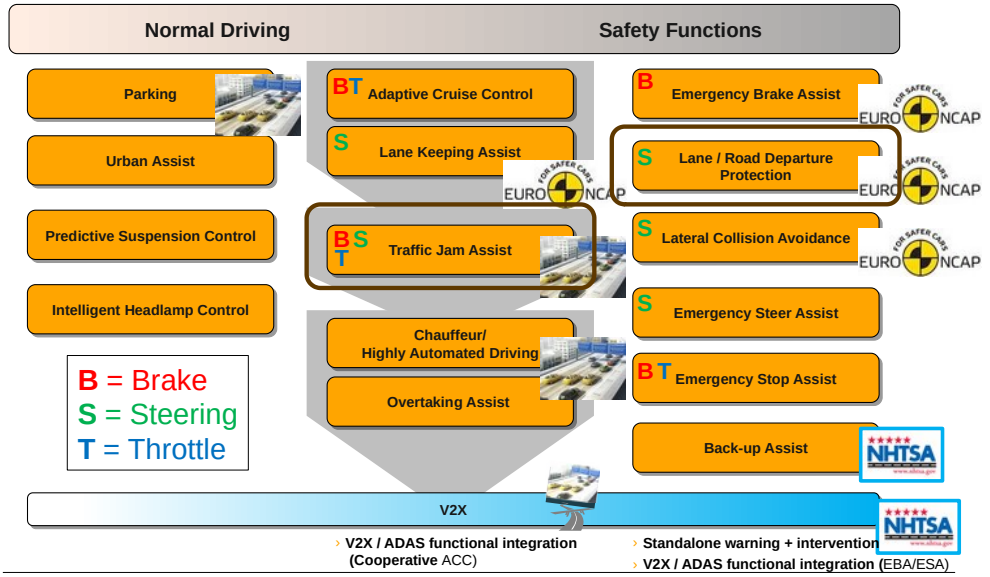
Item-based Functional Safety

- Item executes a function
  - E.g. Lane Departure Protection
- Item-environment boundary
  - Interaction with environment via sensors and actuators
- Hazard and risk analysis for function(s) in item
- Safety concept for faults within item and failures in environment
  - Environment can contain more items

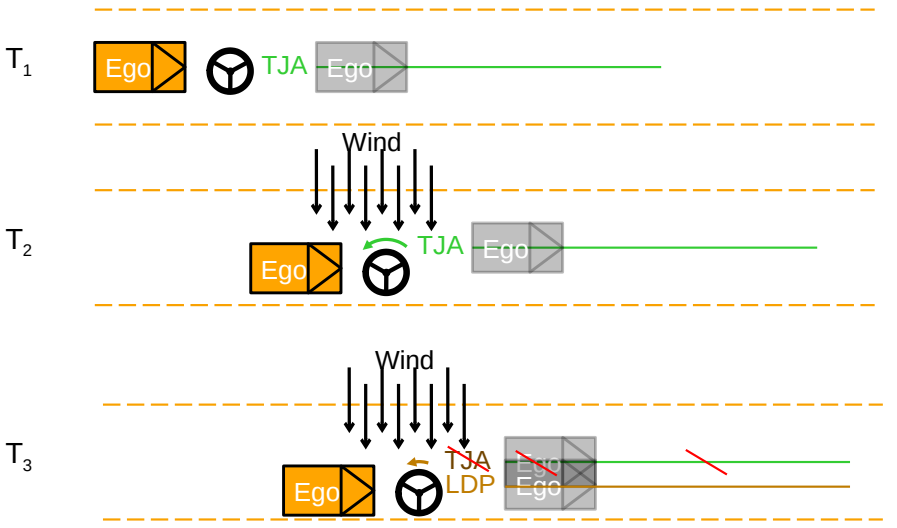


Environment of Multi-functional Car Systems

Example: Continental Chassis & Safety ADAS Functions



Potential Interaction: TJA vs. LDP



Item Interaction and Hazards

- Steering over lane markings is a hazard
  - Controlability unclear, so maybe not safety-relevant
- All individual items are working according to spec

⇨ **Hazards can occur due to interaction of *correct* items**

- Solution: Item = Car?
- Better: **Find way to identify interactions and hazards**

Contents

ISO 26262-3 on Item Interactions

ISO 26262 acknowledges item interaction

5 Item definition

5.1 Objectives

The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

But later steps are item-centric in standard (and in practise)

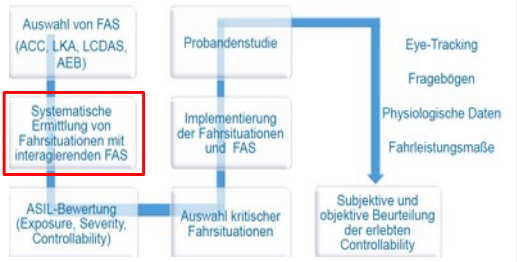
7 Hazard analysis and risk assessment

7.1 Objectives

The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

Other Approaches: ConFas (TU Berlin)

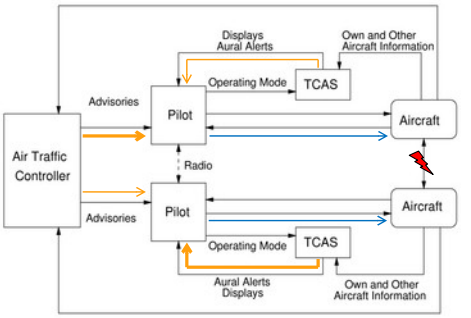
- Goal: Determine controllability of interactions
- Simulation of situations where two system interact
- Identification of situations using a catalog of driving scenarios and situations
- Examined situations had one FAS system hinder the driver in correcting another



(both from O.Schädler, Experimentelle Bewertung der Beherrschbarkeit von interagierenden Fahrerassistenzsystemen anhand kritischer Fahrsituationen; AAET 2015)

Other Approaches: STPA (N. Leveson et al.)

- Assumption: Accidents are caused by inadequate control
- Goal: Define constraints on component behaviour and interactions
- Includes human behaviour, regulations, laws, …
- Keyword-based search for control action (=part of interaction) failures



Systems model for the "Überlingen incident", from Nancy Leveson, "A new approach to hazard analysis for complex systems" , *International Conference of the System Safety Society*. 2003.

Keywords: Control action
- incorrectly provided
- incorrectly not provided
- provided with incorrect timing
- provided with incorrect duration

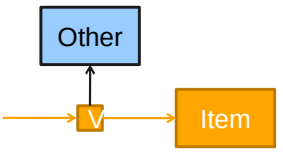
Contents

Interaction Identification Approach

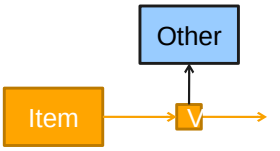
- Once known, interaction can be regulated/prevented
- Items interact via values
  - Functional: Signal (groups)
  - Physical: Physical quantities

- 1. What kinds of interaction exist?
- 2. How to identify them?

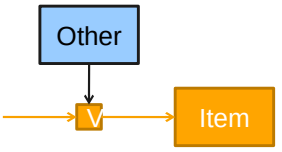
Classification of Interaction Possibilities



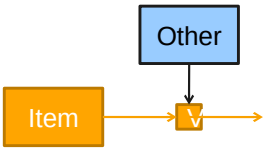
Read Input



Read Outputs



Write Input



Write Outputs

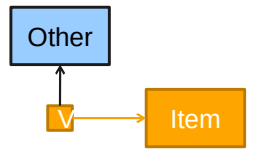
Potential Interaction Consequences

and possible countermeasures

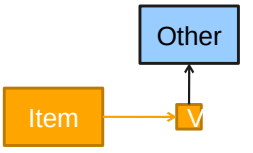
- „Other“ & Item write same outputs
  - Overwrite each other
    - Access Coordination
  - Add up and grow over limits
    - Limiter or Access Coordination
  - Confuse user by sequential actions
    - Dead time
  - Provide action ignoring other‘s (old) intervention

    („TJA vs. LDP“ example)
    - Observe previous actions
    - Dead time

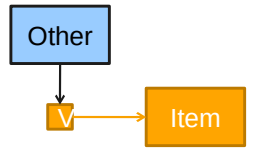
Interaction Possibilities 2



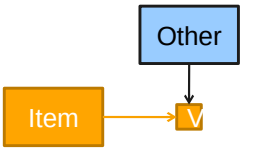
Read Input



Read Outputs



Write Input



Write Outputs

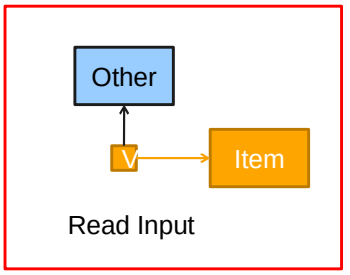
Potential Interaction Consequences 2

and possible countermeasures

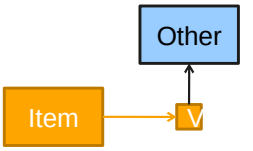
- „Other“ writes Item‘s Inputs
  - Other‘s output misidentified as driver intention
    - Observe other‘s outputs
  - Falsify read values
    - Observe other‘s outputs
  - Unsynchronized Changes
    - Read all data at beginning of time slot
- „Other“ reads Item‘s Outputs

  Analogous but consequences for Other

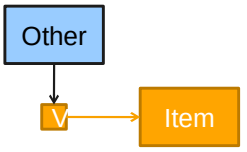
Interaction Possibilities 3



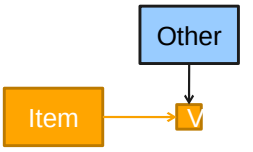
Read Input



Read Outputs



Write Input



Write Outputs

Potential Interaction Consequences 3
and possible countermeasures

- „Other“ & Item read same Inputs
  - (Dead)Lock access to data
    - Deadlock prevetion/detection
  - Bring used sensor into different modes

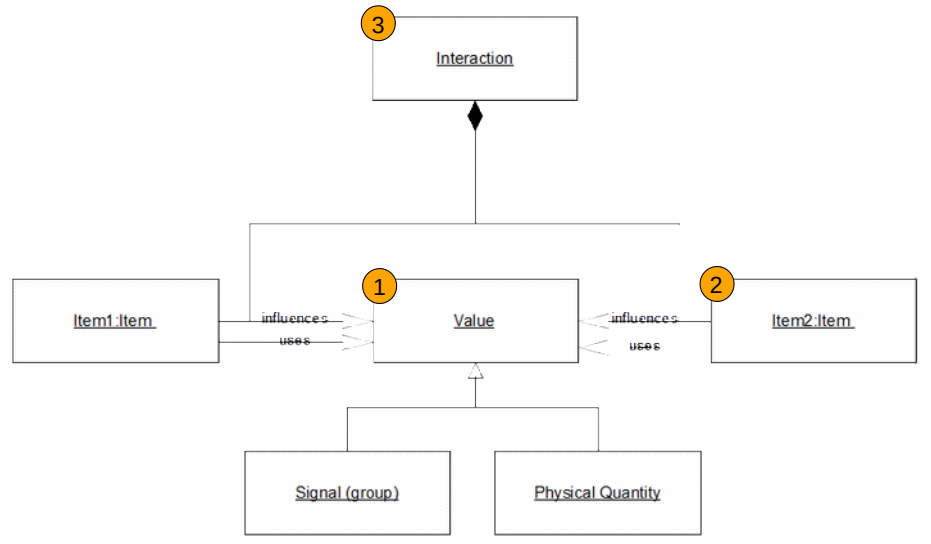
    (e.g. Long-range vs. Short-range evaluation of radar)
    - Central sensor management

Interaction Identification Approach

- Once known, interaction can be regulated/prevented
- Items interact via values
  - Functional: Signal (groups)
  - Physical: Physical quantities

- 1. What kinds of interaction exist?
- 2. How to identify them?

Metamodel of Interactions



Potential Approach

- 1 Identify all interfaces
  - Signal groups as well as physical quantities
- 2 Identify all other items using same interfaces
  - Read/Write Input/Output
    - (Except Read Input)
- 3 For each item & interface identify and evaluate potential interactions
  - Using a keyword list

3 Steps, 3 Excel Pages

Interfaces

Itemname

Functional Interfaces

Inputs

Value or Signal

Outputs

Value or Signal

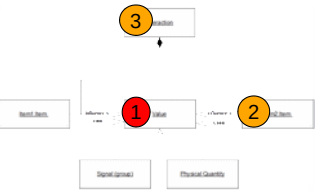
Physical Interfaces

Inputs

Value or Signal

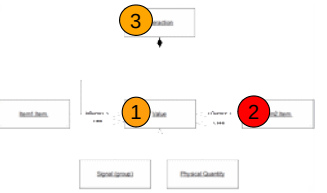
Outputs

Value or Signal



3 Steps, 3 Excel Pages

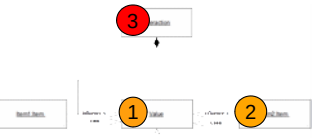
Other items



Functions interacting with *Itemname*

Interfaces	**Other Functions**
Reading Inputs (only check for deadlocks, etc.)	
Value or Signal	*Function 1*
Value or Signal	*Function 2*
Reading Outputs	
Value or Signal	*Function 3*
Value or Signal	
Write Inputs	
Value or Signal	*Function 4*
Value or Signal	*Function 1*
Write Output	
Value or Signal	*Function 4*

3 Steps, 3 Excel Pages
Other items



Potential interaction effects of other items with *Itemname*

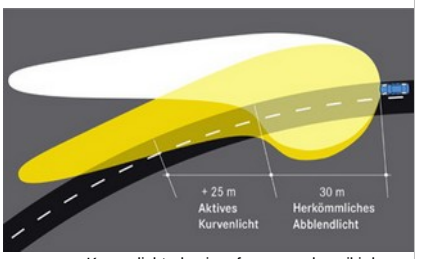
Reading Outputs	**Other function**	**What is the effect if the item changes the output (which is input to the other functions) in the following ways**					**Countermeasures**
		1) more Output is increased (slowly/quickly) over original value	2) less Output is decreased from original value	3) inverse Output gradient changes direction (i.e. increase <-> decrease)	4) before Output is changed before other functions acts	5) after Output is changed after other function acts	
Value or Signal	*Function 1*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	*Interaction and consequence*	Potential countermeasures against each consequence
Value or Signal	*Function 2*						

Writing inputs	**Other function**	**What is the effect if the other functions changes its output (which is input to the item) in the following ways**					**Countermeasures**
		1) more Output is increased (slowly/quickly) over original value	2) less Output is decreased from original value	3) inverse Output gradient changes direction (i.e. increase <-> decrease)	4) before Output is changed before other functions acts	5) after Output is changed after other function acts	

Contents

Example Systems for Interaction Analysis

- Advanced front-lighting system (“Kurvenlicht”) turning the headlamps



Kurvenlicht_dyn.jpg from www.bs-wiki.de

- Light assistant switching on/off headlights and high beam

from motor-talk.de

- Drift assistant helping to drive through curves oversteering

from www.tmwerkes.ca

Practise

Experiences of practise

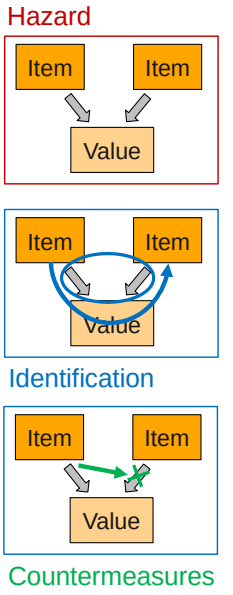
- Things that worked well / badly ?
- Additional keywords?

Limitations of Shown Approach

- Some interactions will not be identified:
- Physical relationsships
  - E.g. two planes cannot be in same airspace simultaneously
  - E.g. braking and steering both use up adhesion
    - Could use „adhesion“ as physical quantity
- Driver limitations
  - E.g. drivers are less experienced with simultaneous steering and braking
- Effects within normal control chains
  - Part of one item

Summary

- Interaction of correctly functioning systems can cause hazards
- Analysis approach
  - Following influenced signals/quantities
  - Keyword-based interaction identification
  - Countermeasures definition



Questions and … Questions

- Your questions!

- My questions:
  - Do **you** analyze item interactions?
    - Example interaction hazards found which can be shared?
  - Systematic approach at identification?
  - Approach to determine controlability?
  - Interactions of items in different cars?

Thank you

for your attention!

Backup Slides

The specification leg of the V-model

Know what you do

Item definition

Functions & States
Environment

Know what could go wrong

Hazard & Risk analysis

Safety Goals (ASIL)
Safe States

Define countermeasures

Safety Concept

Safety Requirements
Safety Measures

Not good enough?

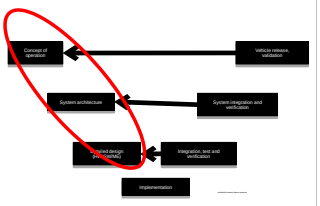
Evaluate Sufficiency

Safety Analysis

FTA
FMEA, FMEDA

Good enough?

Next Refinement Level



Identification of Failure Modes – Systematic Brainstorming

- Hazard and Operability Study (HAZOP)
  - First applied in chemical industry to identify potential hazards caused by deviations from design intent
- Approach
  - Find ways an item/component can fail based on two sets of keywords
  - Primary: Intentions or Functions of component
    - Particular aspect of design or parameter
    - Differ from component to component
  - Secondary: Deviation hints
    - Possible deviations
    - Standard Set of keywords
- Alternative result: Consequences

HAZOP secondary keywords

Keyword	General Meaning	Example Primary Keyword: Steering
No	Function not performed / unachieable	No steering moment; Steering locked
More	Quantitative increase	Too much/too long steering moment
Less	Quantitative decrease	Too few/Too short steering moment
Also	Qualitative increase (something in addition)	Vibration while steering; Steering wheel height modified
Part	Qualitative decrease (something missing)	--
Reverse	Opposite than intended	Steering moment in opposite direction
Other	Not where or how expeced (something different)	No steering moment but braking; Unexpected steering moment
Fluctuation	Not achieved all of the time	Steering moment ‚stutters‘
Early	Function performed too early	Too quick moment buildup
Late	Function performed too late	Steering moment buildup too slow


Safe and Dynamic Driving
towards Vision Zero
SensePlanAct
Chassis & Safety
Continental
38