

Ontological Analysis of communication-bus behavior

Bieleschweig VI

Jörn Stuphorn
stuphorn@causalis.com

- The application of Ontological Analysis (OA) to a communication bus was made
- Main parts of the work were:
 - Description of workflow for OA
 - Introduction of HAZOP into the workflow
 - Description of the system to be analysed
 - Application of iterative decomposition on system

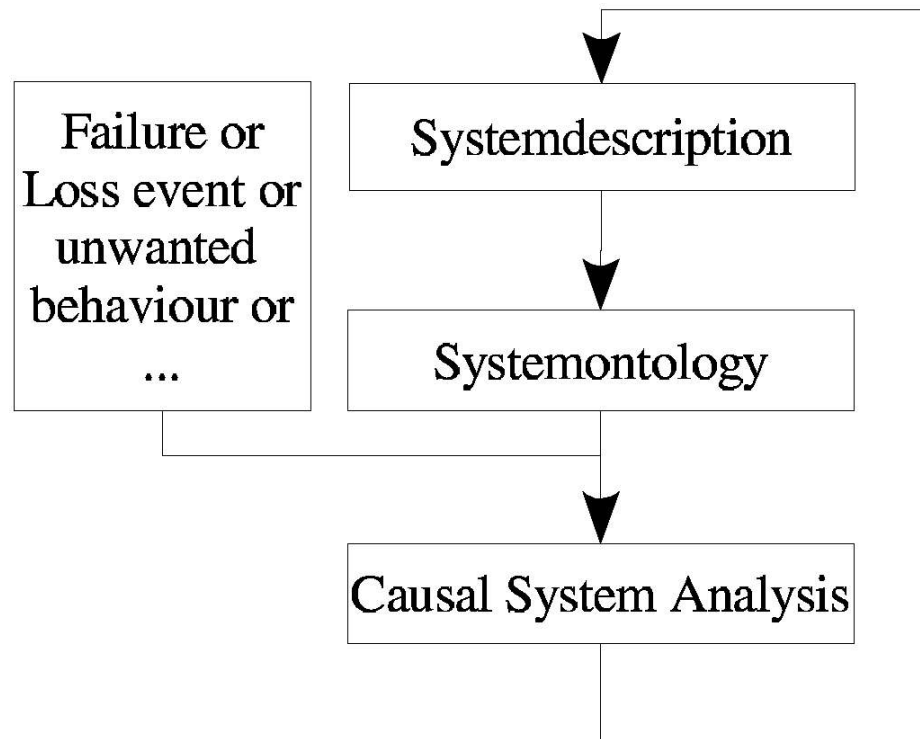
The System Investigated

- Communication network for possible use in automobiles
- Network has to facilitate safety-critical applications like
 - X-by-Wire
 - Powertrain
- Transmission modes
 - time-triggered
 - event-triggered
- Currently deployed communication buses use event-triggered transmission
 - CAN
 - J1850
 - LIN

- currently developed system
 - similar to Fly-by-Wire in aircraft construction
 - Interconnect automotive systems without mechanical-fallback
- Motivation
 - weight reduction
 - simpler integration of drive assistance programs
- Problems
 - System has to be ultra-reliable
 - existing systems for aircraft impractically expensive for auto use
 - Legacy systems must be integrated

Ontological Analysis

- Method for requirement development
- Based on ontological description of system
- Simplified development proces:
 - Ontology is formed according to a system description
 - The causal interactions leading to a failure are identified
 - The ontology is expanded in regard of findings



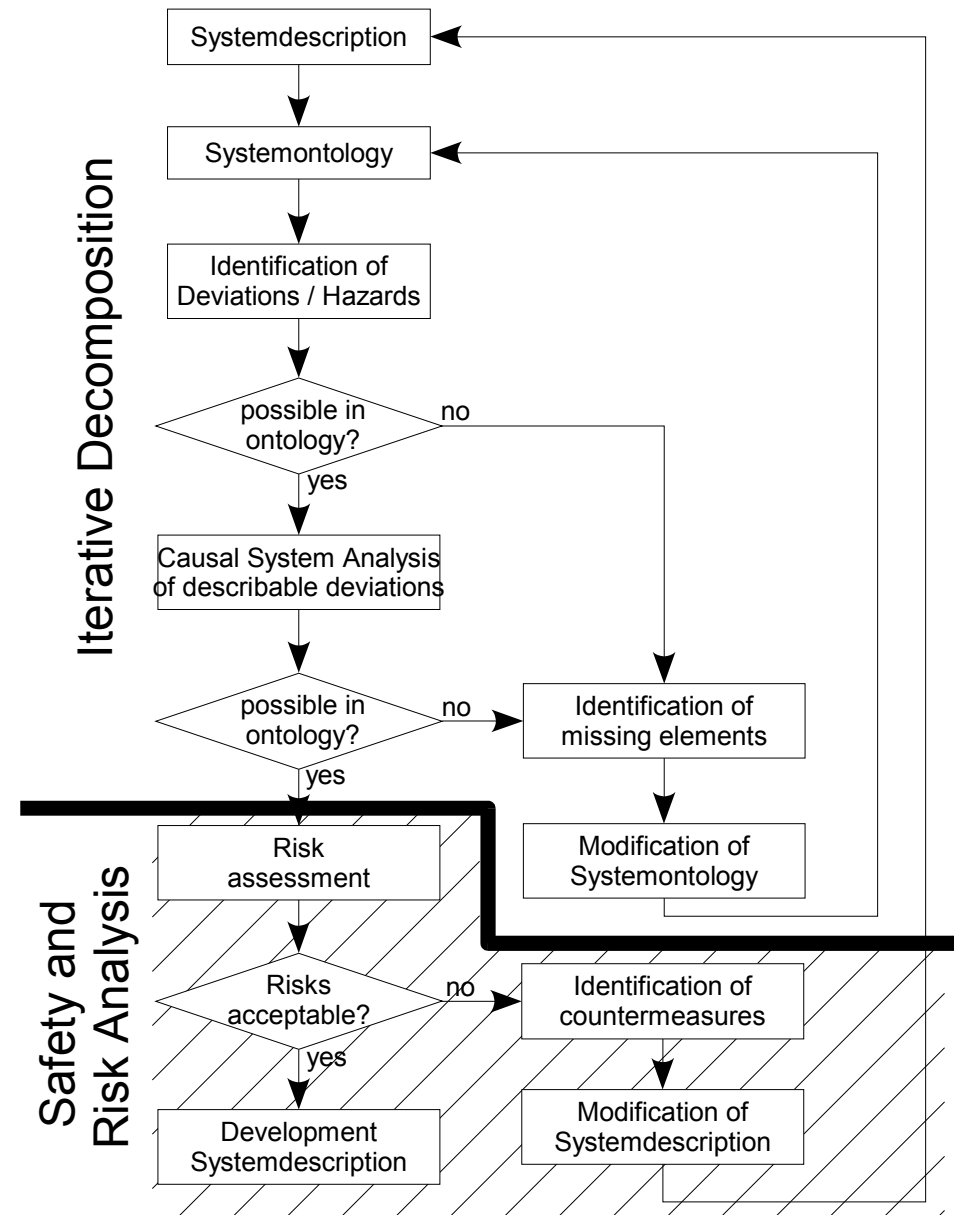
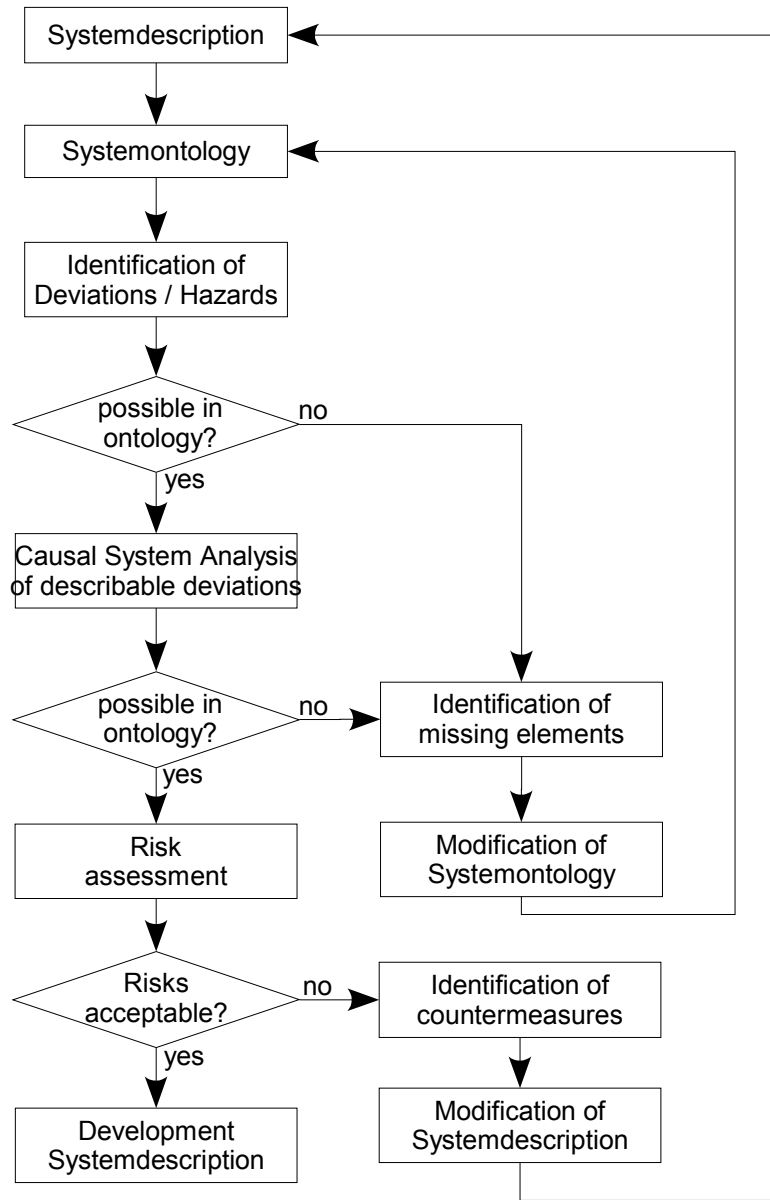
- The ontology used in OA consists of
 - Objects
 - Relations
 - un-ary (properties)
 - n-ary (relations)

- Initialisation:
 - Simple system description
 - Extreme case:
 - only one object
 - only unary relations
 - Typical case:
 - Low number of objects and relations
 - based on experience and knowledge

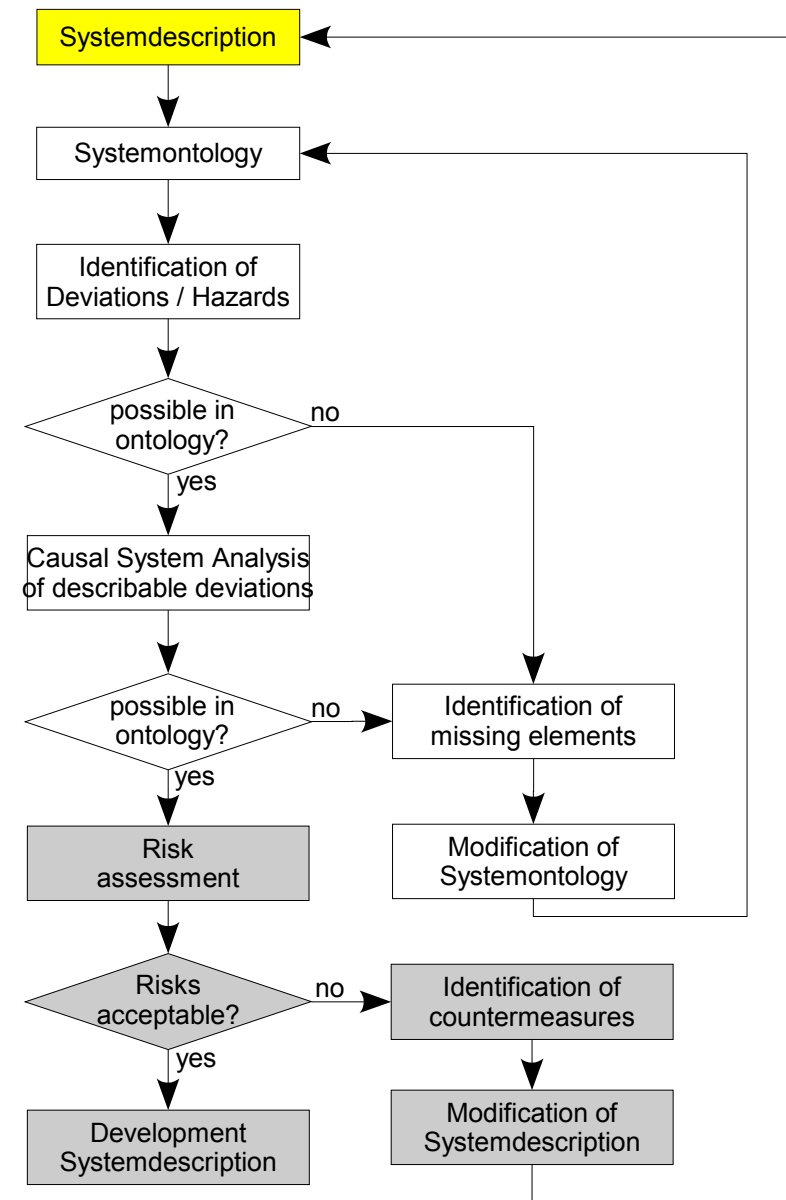
- Starting point:
an identified failure, or, loss event, or hazard, or ...
- States of the ontology causally leading to starting point are identified

- Results:
 - Identification of safety-requirements
 - Extension of ontology and system description

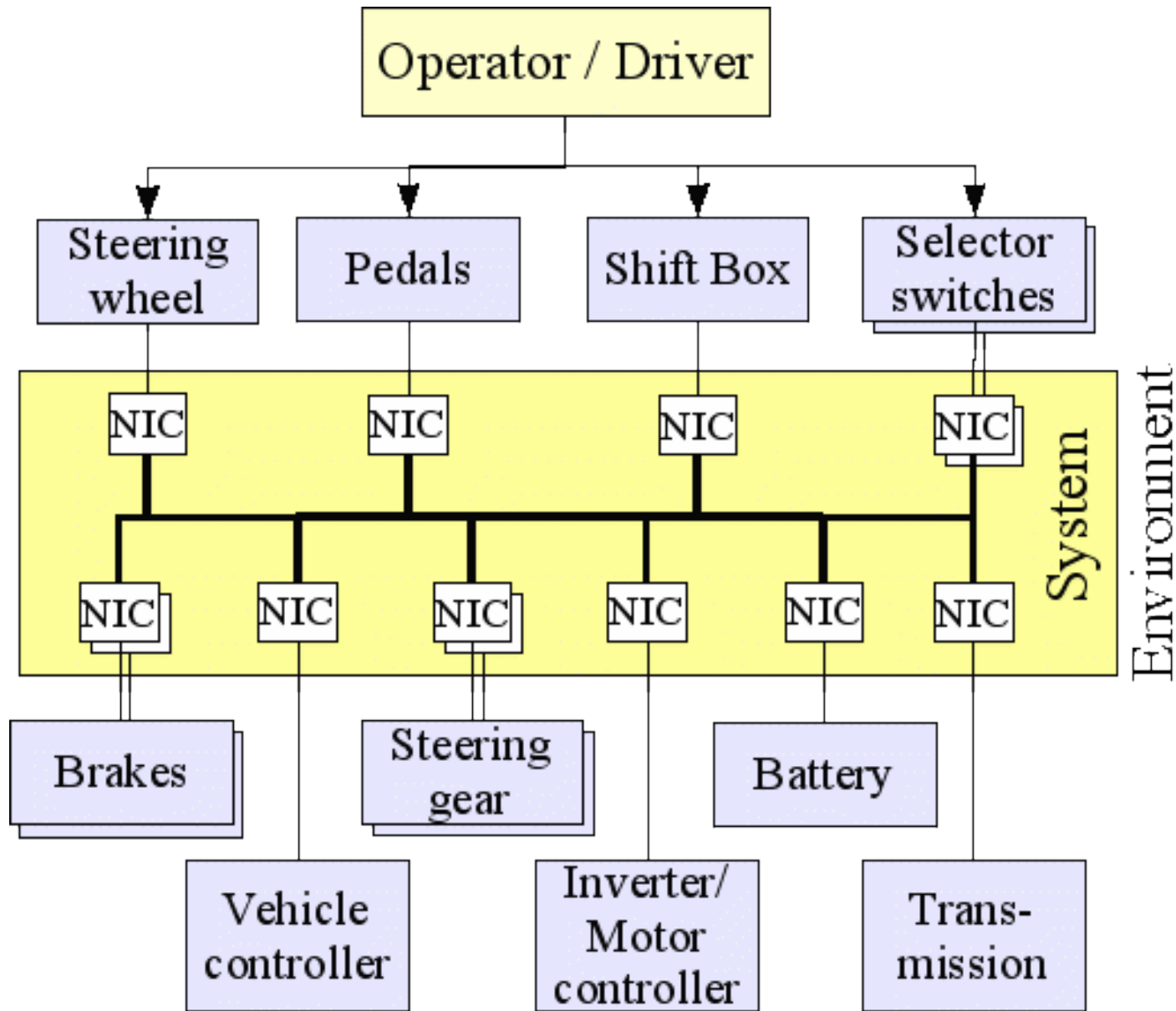
Workflow of OA



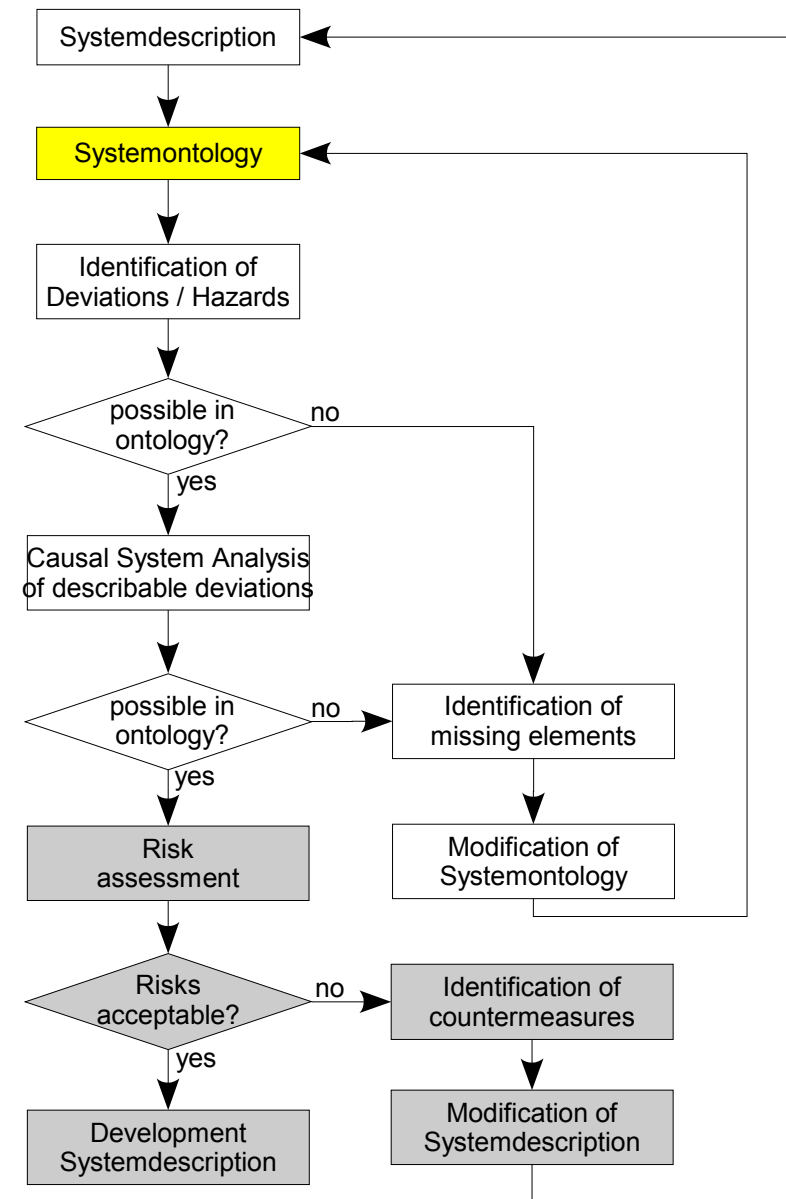
The System



System Schematics

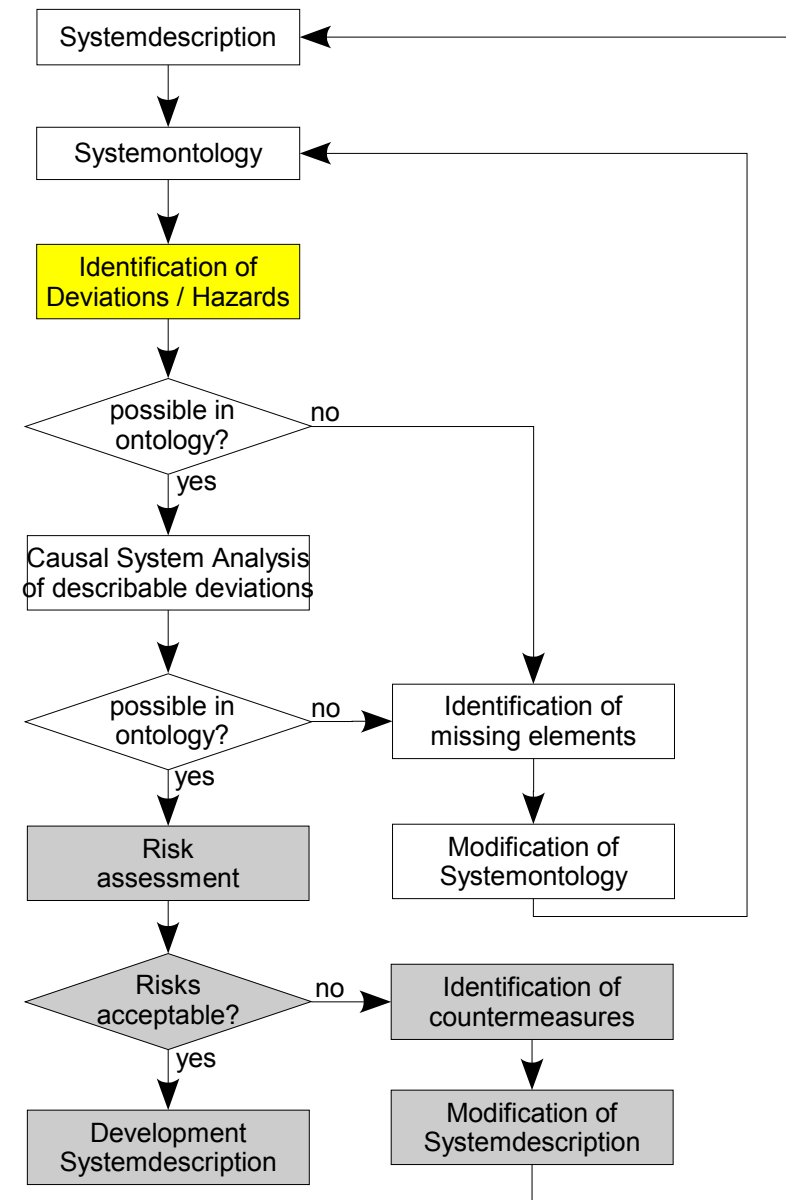


The system's ontology



- Objects
 - NIC
 - Wiring
 - Transmission
- Relations
 - Connection (Wiring, NIC)
- Properties (unary relations)
 - Input(NIC)
 - Output(NIC)
 - Intact(NIC)
 - Intact(Wiring)
 - Size(Transmission)
 - Deadline(Transmission)
 - Period(Transmission)
 - Mode(Transmission)
 - Latency(Transmission)
 - Jitter(Transmission)
- Every element of the ontology has to be accurately defined!

Identification of Deviations



- **HAZard and OPerability Study**
 - Group of experts
 - Identification of possible deviation from design intend
 - Deviations lead to causes and consequences

- **Guide-words**
 - Group agrees on a set of guide-words
 - Typical sets developed by
 - Royal Society of Chemistry (CISHEC)
A Guide to Hazard and Operability Studies, 1977
 - Redmill, Chudleigh, Catmur
System Safety: HAZOP and Software HAZOP, 1999
 - IEC 61882
Hazard and operability studies – Application guide

HAZOP – Guide-Words

| GUIDE-WORD | BY | INTERPRETATION |
|------------|-----|--|
| No | RSC | None of the design intent is achieved |
| | RCC | This is the complete negation of the design intention - No part of the intention is achieved but nothing else happens |
| More | RSC | Quantitative increase in a parameter |
| | RCC | This is a quantitative increase |
| Less | RSC | Quantitative decrease in a parameter |
| | RCC | This is a quantitative decrease |
| As well as | RSC | An additional activity occurs |
| | RCC | This is a qualitative increase, where all the design intention is achieved together with additional activity |
| Part of | RSC | Only some of the design intention is achieved |
| | RCC | This is a qualitative decrease, where only part of the design intention is achieved |
| Reverse | RSC | Logical opposite of the design intention occurs |
| | RCC | This is the logical opposite of the intention |
| Other than | RSC | Complete substitution. Another activity takes place |
| | RCC | This is a complete substitution, where no part of the original intention is achieved but something quite different happens |
| Early | RSC | The timing different from the intention |
| | RCC | Something happens earlier in time than intended |
| Late | RSC | The timing different from the intention |
| | RCC | Something happens later in time than intended |
| Before | RSC | The step (or some part of it) is effected out of sequence |
| | RCC | Something happens earlier in a sequence than intended |
| After | RSC | The step (or some part of it) is effected out of sequence |
| | RCC | Something happens later in a sequence than intended |
| Faster | RSC | The step is done with the right timing |
| Slower | RSC | The step is not done with the right timing |
| Where else | RSC | Applicable for flows, transfers, sources and destinations |

- Application of guide-words to attributes leads to combinations
- Interpretation of combinations is done in sentences

| ATTRIBUTE: | Size(Transmission) |
|------------|---|
| GUIDE WORD | INTERPRETATION |
| No | Transmission has no size |
| More | Received information is bigger than sent information |
| Less | Received information is smaller than sent information |
| As well as | a. Simultaneous transmission of several information blocks b. Additional transmission of content |
| Part of | Only part of the information is transmitted |
| Reverse | Information is sent with inverted size |
| Other than | Complete substitution of size |
| Early | a. Transmission size is transmitted early b. Transmission size is calculated early |
| Late | a. Transmission size is transmitted late b. Transmission size is calculated late |
| Before | Transmission size occurs ahead of sequence |
| After | Transmission size occurs behind sequence |
| Faster | Transmission size is transmitted too fast |
| Slower | Transmission size is transmitted too slow |

- Sentences have to be interpreted with regard to possible failures
 - example: Interpretations for Size(Transm.) sentences

Comments on the formed HAZOP sentences:

Reverse The logical opposite of size cannot be defined.

Other than The size of a transmission cannot be completely substituted. A minimal size of NULL remains.

Before, early The early or late transmission of size information will lead to corrupted transmissions if the protocol transmits this information. This deviation is identified under the sentences of transmission. Under the assumption that the size can be measured directly the timing has no influence on the measured value.

After, late The transmission of size information out-of-sequence can lead to corrupted transmissions. This deviation is identified under the sentences of transmission.

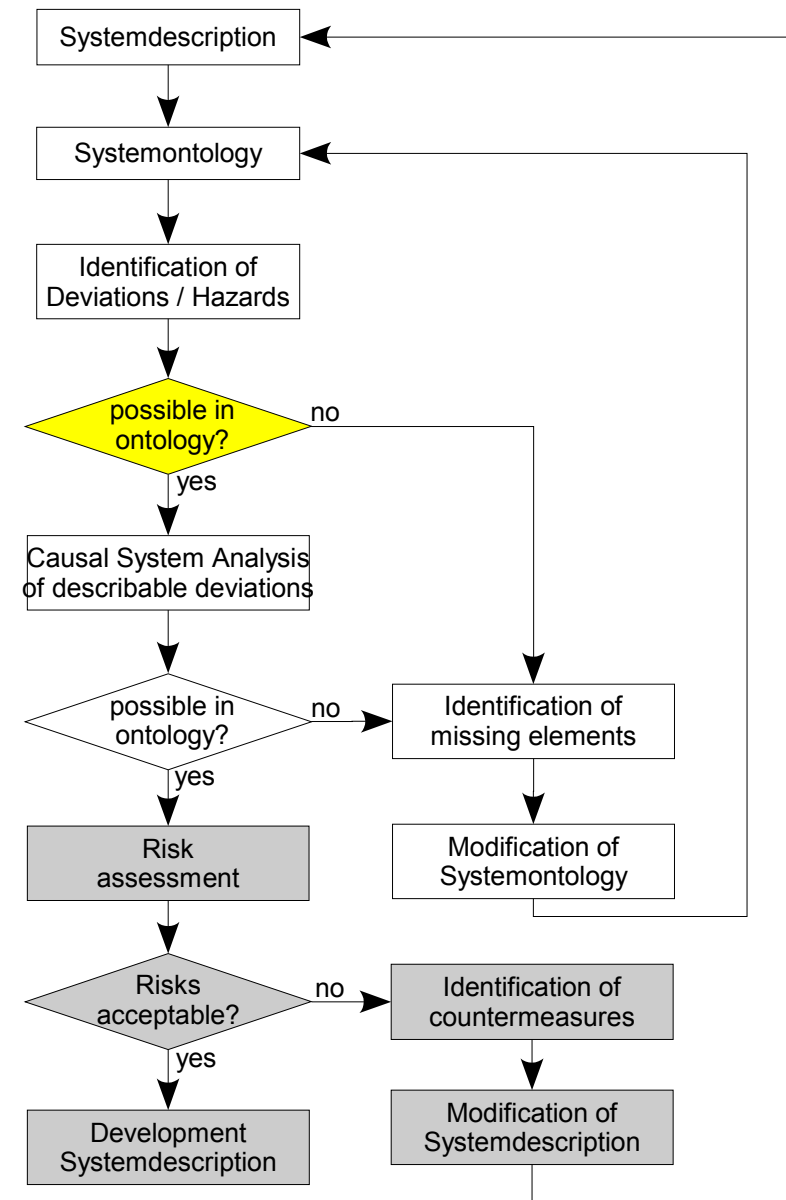
Faster, slower The message size cannot be effected by speed or transmission rate because it can be assumed, that the size can be measured directly.

- Assumptions can influence the analysis depth!

- Results:
 - List of deviations
 - List of assumptions made in the interpretations

- Next tasks:
 - Deviations:
 - Causal analysis of deviations using CIDs
 - Assumptions:
 - validate assumptions
 - If this cannot be done
integrate countermeasures

Expressing Deviations in the system-ontology

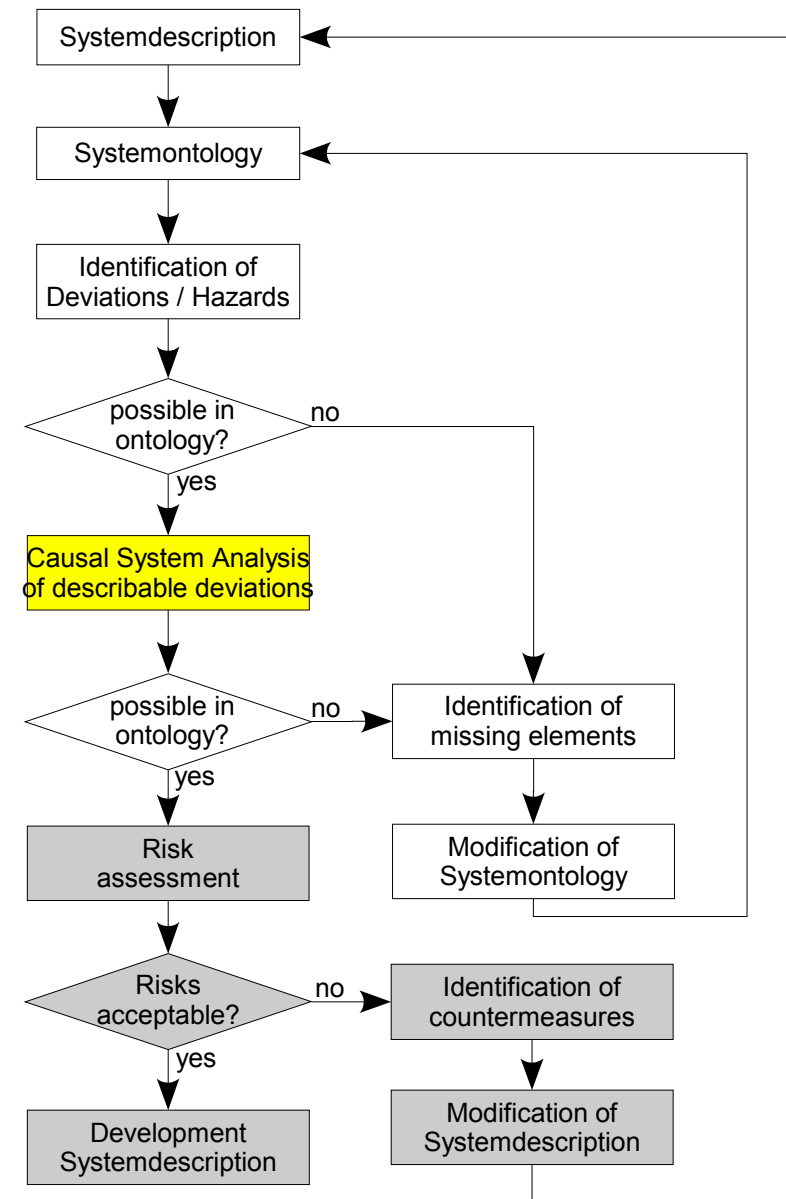


- Deviations are expressed using the ontology as a kind of language
- Deviations not translatable lead to extension of ontology
- These deviations are analysed in the next iteration

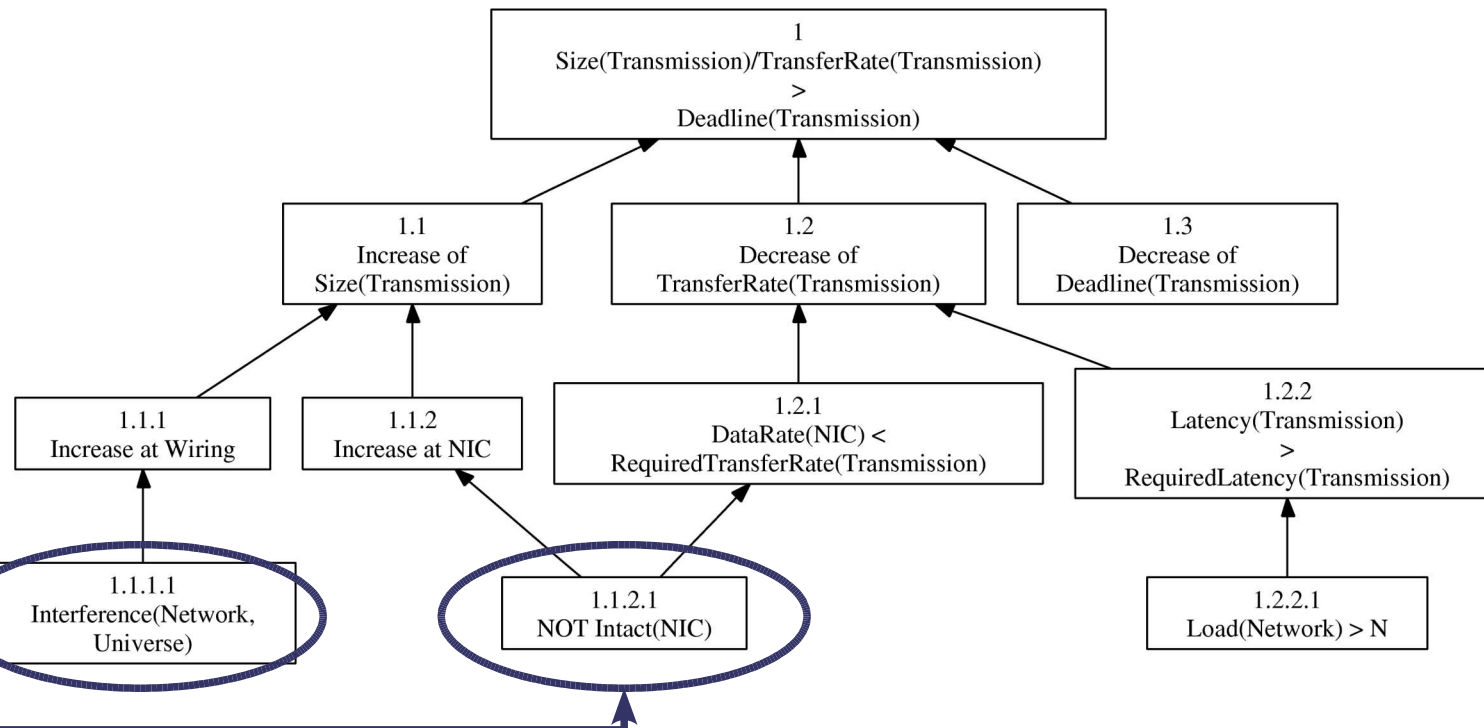
5.a NIC has no output
5.b NIC has more output to the device than expected
5.c NIC has more data to transmit than expected
5.d NIC transmits only part of the output
5.e NIC transmits inverted output
5.f Output is replaced
5.g Output is sent early
5.h Output is sent late

5.a $\text{Output}(\text{NIC}) = 0$
5.b $\text{Size}(\text{Transmission}) > \text{RequiredSize}(\text{Transmission})$
5.c $\text{Input}(\text{NIC})/\text{time} > \text{DataRate}(\text{Device}) * \text{time}$
5.d $\text{Input}(\text{NIC}) > \text{Output}(\text{NIC})$
5.e $\text{Output}(\text{NIC}) = \text{INVERSE}(\text{Input}(\text{NIC}))$
5.f $\text{Output}(\text{NIC}) \neq \text{Transmission}$
5.g $\text{TimeSent}(\text{Transmission}) < \text{RequiredTimeSent}(\text{Transmission})$
5.h $\text{TimeSent}(\text{Transmission}) > \text{RequiredTimeSent}(\text{Transmission})$

Causal System Analysis

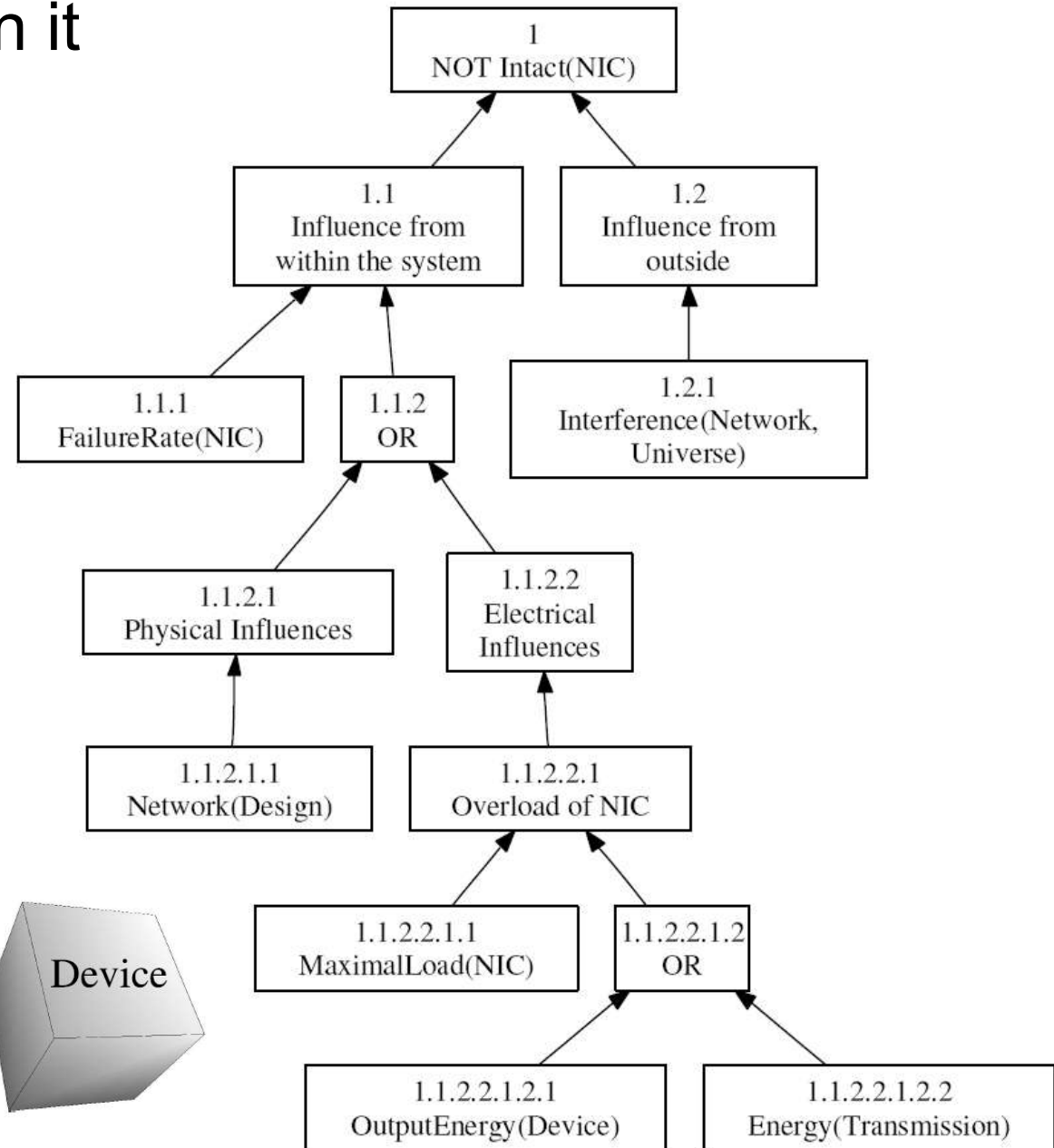
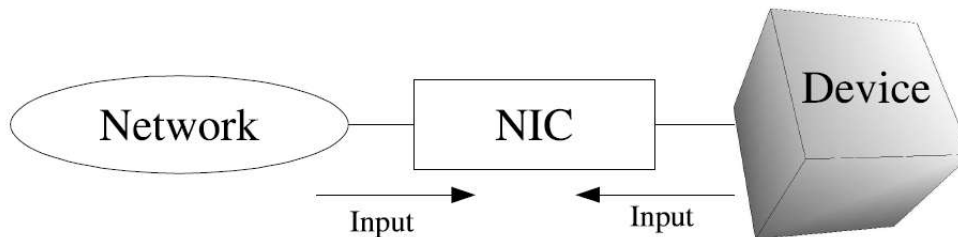


- Causal factors of ontological analogues are identified
- Stopping Rule: Analysis is stopped when
 - Previously-identified deviation occurs
 - Elements not in ontology are needed

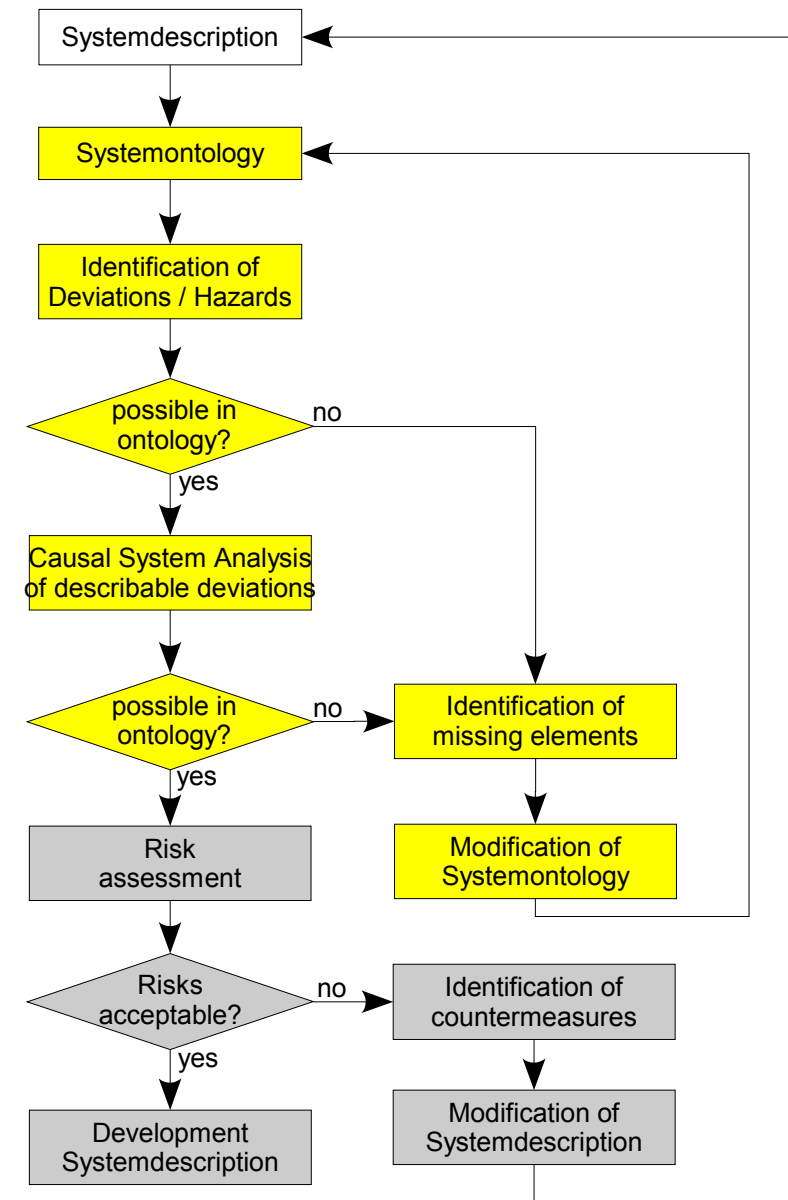


Example for CIDs

- For ease of formulation it can be useful to use narrative descriptions
- Important: all possibilities have to be accounted for
- Schematics may help in this identification

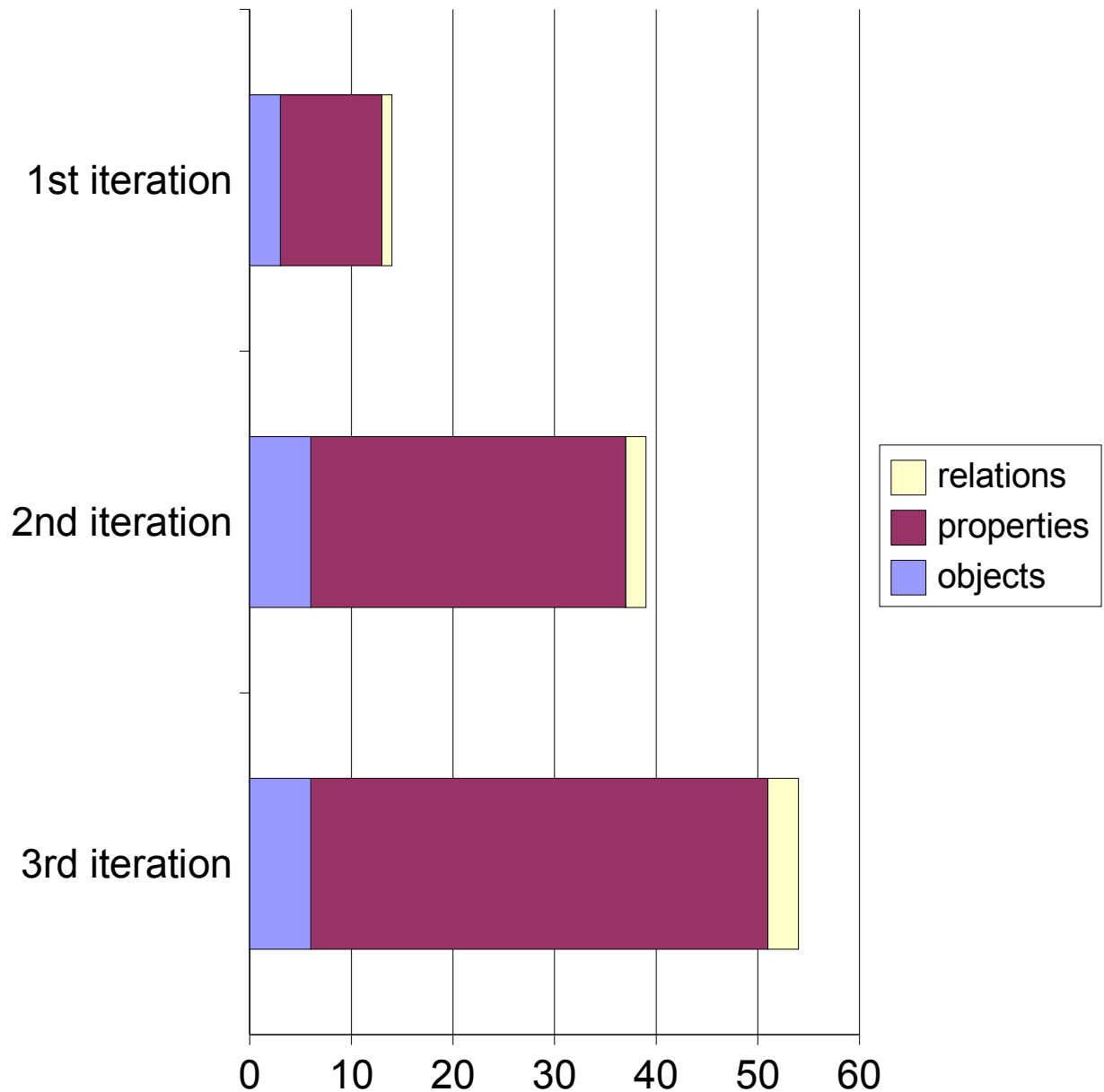


Results of the Application of the Iterative Decomposition



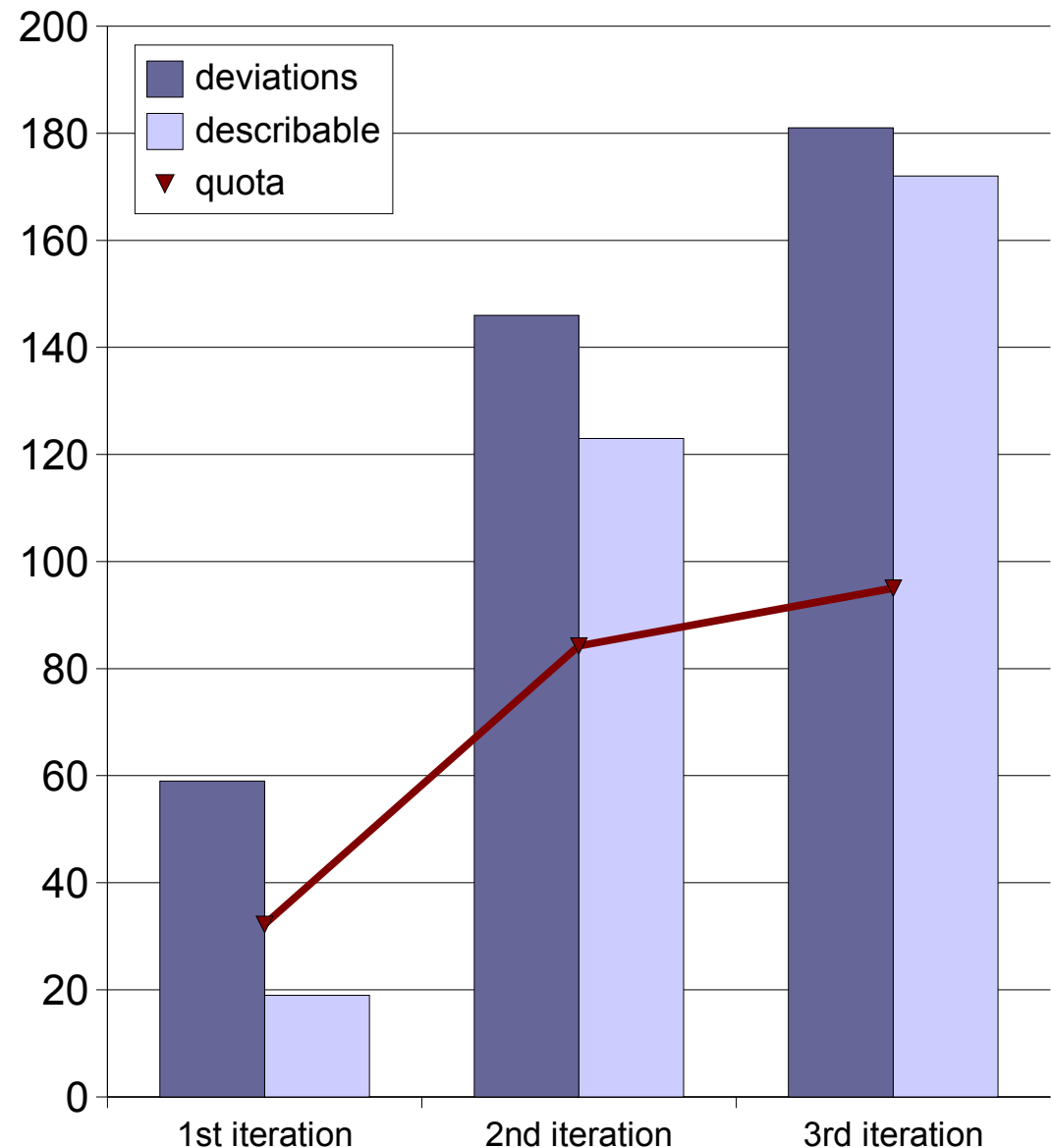
Ontology Results

- 1st iteration
 - 3 objects
 - 10 properties
 - 1 relation
- 2nd iteration
 - 6 objects
 - 31 properties
 - 2 relations
- 3rd iteration
 - 6 objects
 - 45 properties
 - 3 relations



HAZOP Results

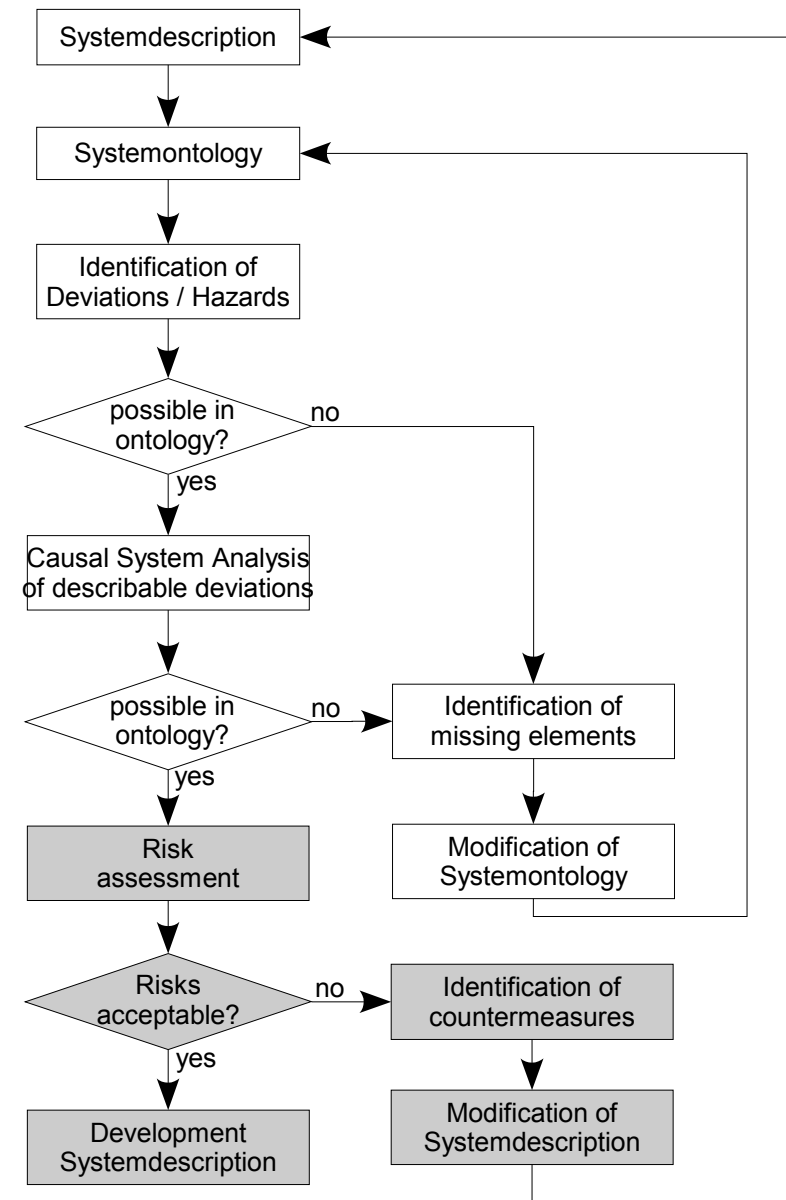
- 1st iteration
 - 59 deviations
 - 19 describable
 - quota: 32.2%
- 2nd iteration
 - 146 deviations
 - 123 describable
 - quota: 82.2%
- 3rd iteration
 - 181 deviations
 - 172 describable
 - quota: 95.0%



- The ontological analysis produces extensive documentation
- Greater size of analysis group leads to greater reliability in the number of deviations identified
 - Even a small group (e.g. one „expert“) develops detailed system safety requirements
 - Examples for identified elements after 3 iterations:
 - Shielding(Network)
 - EmissionRegulation(Transmission)

Not handled here:

**Risks and
 Completeness
 Questions**



Thank you.