Universität Bielefeld
Technische Fakultät
Arbeitsgruppe Rechnernetze und Verteilte Systeme

Diploma Thesis

Iterative Decomposition of a Communication-Bus System using Ontological Analysis

by

Jörn Stuphorn

Examiner: Prof. Peter B. Ladkin PhD FBCS, Universität Bielefeld
Dr.-Ing. Yorck von Collani, Robert Bosch GmbH

Bielefeld, July 2005

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig bearbeitet und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, sowie Zitate kenntlich gemacht habe.

Bielefeld, den 19. Juli 2005 Jörn Stuphorn

Contents

List of Figures

List of Tables

1 Introduction

The Ontological Analysis [Lad01] consists of two phases: the phase of iterative decomposition and the phase of hazard and risk analysis. The aim of the iterative decomposition is to describe the elements and their interactions increasingly detailed, whereas the aim of the hazard and risk analysis is the evaluation of the risk imposed by the hazards identified for the described system.

This work concentrates on the description of the methods used for the ontological analysis and demonstrating the process of iterative decomposition on the example of a communication bus system.

The subject analysed is a communication system able to transmit time- as well as event-triggered messages. If safety-critical devices like the steering or braking systems are to be connected without mechanical backup, a high level of confidence in the system used for connection of the devices has to be achieved. In newer aircraft the steering is done by using Fly-by-Wire systems that digitise the pilot's control input and transmit this information via controlling systems to the control surfaces. The automotive industry tries to adapt this approach with new control systems for vehicles, that are to be used in X-by-Wire or Powertrain communication solutions for the breaking- and steering- respectively the motor-management-system. As the communication solution applied in aircraft is very expensive, this solution will most certainly not be adopted in automobiles, where the count of units produced is very high and cheaper solutions are sought.

Existing communication systems in the automotive industry use event-triggered communication protocols like CAN [CAN91] or LIN [vW03] for the transmission of information between devices. As possible failures in the communication of the breaking system can have grave outcomes, the acceptance of the costumers and the popularity of a brand is threatened. Communication systems for safety-critical tasks must guarantee, that the information is transmitted within defined timing requirements. The differences between time- and event-triggered protocols

is obvious, if the time needed for a message being transmitted from a sender to a receiver, the latency, is observed. For event-triggered communication protocols it is only possible to achieve a required latency with a certain likelihood. In contrast time-triggered communication systems can ascertain the compliance with required communication attributes but tend to show inefficient use of the available network resources.

A communication system combining the ascertained compliance with required communication attributes and the possibility to integrate existing communication solutions is very interesting. Such a communication system enables the implementation of new control technology while supporting an easy way of migration for existing devices.

This work is divided into five parts. In the first part, the needs of communication protocols in the automotive domain are investigated. The fundamental design options for networks and proposed classifications are described. The second part describes the methods used in the ontological analysis' phase of iterative decomposition while the third part focuses on the methods used in the phase of risk assessment. The fourth part demonstrates the iterative decomposition's application on the communication system whose needs were identified in the first part. Finally the fifth part consists of the conclusions this investigation lead to and the outlook.

2 Communication in the Automotive Domain

Communication systems in the automotive domain became useful with the integration of increasing numbers of electronic devices into the vehicles. The connection of these at first separately connected systems via a communications system allowed for savings in weight, lower costs of production, and higher flexibility in comparison to the separate connection using wiring harnesses.

Electronic devices in vehicles are - amongst others - used for the monitoring of safety critical systems and are thereby increasing the reliability of the system in case of failure. If a deviation from the required behaviour is detected, the electronic system can adapt the behaviour of the mechanical system so that the required functionality is provided while the over-all system performance is reduced. This allows fail-safe operation, meaning that a failure causes the "machinery to revert to a safe condition in the event of a breakdown." [Soa03].

One of the first networks developed for the connection of electronic devices in automobiles was the Controller Area Network (CAN) developed for automotive applications starting 1983 [iA04]. In 1993 it was published as ISO 11898 [Int93]. Other networks, like GMLAN, LIN or J1850 serve the same purpose though having different areas of applications and requirements on the communication.

Following the connection of electronic devices using communication networks it becomes possible to use the information available from the sensors and introduce assistance programs to increase the comfort and safety of the passengers.

The the X-by-Wire project [Bri98], sponsored by the European Union, investigated the possibility of using network systems for the connection of electronic devices for allowing the removal of the mechanical backup in the automobile. Systems replacing mechanical backup of control devices are widely used in aerospace industry, where Fly-by-Wire systems were first introduced in the military sector and later adopted by civil aviation.

The substitution of mechanical control units with electronic control units makes it possible influence vehicle control directly and bypassing the driver's input. This leads to the driver's direct control over the vehicle being taken away and enables the possibility of increasing driving safety by counteracting problematic control input as well as enabling future drive control for the "automated highway" where vehicles controlled by computers make optimal use of the resource highway [WF00].

Additionally it makes the easy integration of drive assistance programs like steering or braking assistants possible which allows the manufacturer direct influence in the character of the vehicle that was beforehand defined by the mechanical system which could only be modified using requirements to the supplier [KH02].

The gain of weight reduction results from the replacement of mechanical backup devices like hydraulic pipes, the steering axle, and other mechanical transmission devices that usually are heavy and require intense maintenance compared to electric wiring and sensors [Whi01].

By replacing devices for mechanical backup it becomes necessary for the electronic system to cope with failure situations. In case of a failure, a fail-safe condition has to be achieved by the electronic system on its own. This implies that it has to achieve a higher level of confidence than the system previously used for this task.

Besides the gains in the replacement of the mechanical connection there are also disadvantages in this technique. Without a direct connection between a control device and the corresponding actuator the feedback to the driver has to be generated artificially. This feedback is important for the driver to maintain control over the vehicle in critical situations. Modern Fly-by-Wire systems use force-feedback control sticks to provide the pilot with this kind of information. This feedback is also important for the vehicle's manufacturer to create a brand differentiation that is influenced the handling of the vehicle.

2.1 Areas of Application

In general there are four areas in which communication systems currently are or will be used in vehicles:

- Multimedia
- Controlling
- Powertrain
- X-by-Wire

Multimedia applications require high bandwidth for the transmission of video, Internet access or cellphone integration into the sound system. These applications are not safety critical but can be an annoyance to the customer if they do not function as proposed.

Controlling information from measuring vehicle attributes like speed and wheel rotation are transmitted to the appropriate devices like the speedometer or the ABS anti-lock braking system. This information is important but in case of function loss the driver's control over the vehicle is not necessarily lost as the vehicle can be driven in case of basic braking functionality available or the vehicle's speed not displayed.

The powertrain system comprises of the engine, transmission, and exhaust components. Reduction in pollution is required by the Kyoto protocol. The European Automobile Manufacturers Association made a commitment to the European Union [Ass02] promising to meet the benchmarks set for automobiles. To achieve this reduction flexible control of injection and combustion is needed, leading to an increased efficiency of the engine and reduction of pollution.

CPUs can help to process the current attributes of the powertrain system and compute solutions for the engine control under consideration of the driver's input. A failure in the powertrain system could be serious, e.g., if the car is supposed to run in first gear and instead uses reverse. Also information leading to a lock in the transmission could render the vehicle uncontrollable.

Under the topic X-by-Wire control systems are understood, that provide control over safety critical functions without mechanical backup. This includes the possibility that a failure in the communication system can render the vehicle uncontrollable.

Systems for the tasks of Brake-by-Wire, Steer-by-Wire and sometimes Shift-by-Wire are typically counted into the group of X-by-Wire systems. Because of

Shift-by-Wire's involvement with the powertrain system this classification is arguable but may be necessary for combined control models like Bosch's KASS (Coordinated Powertrain Control) [BOS05] which combines breaking, acceleration and transmission to achieve "safety and convenience, as well as considerable fuel consumption savings."

The needs of multimedia applications are mainly dependant on the availability of very high bandwidth. Other requirements like latency or transmission deadlines are not as important as in safety critical applications. Because the investigated communication system should enable X-by-Wire systems the needs of multimedia applications are regarded as being out-of-scope for this work. If the need of multimedia applications being controlled by components connected via the safety critical network arises, a gateway connecting safety critical and multimedia network can be used, as the multimedia control messages can be sent using the lowest priority.

2.2 Types of Media Access Control

Essentially there are three commonly used approaches for reaching an agreement which node connected to the network is entitled to transmit its data. Todays LANs, which are based largely on Ethernet (IEEE802.3) [Law05] or WLAN (IEEE802.11) [Ker05] use the event-triggered approach to reach an agreement over who is entitled to send information. Another possibility for the media access is the approach taken by Token-Ring (IEEE802.5) [Mes04] for deciding on the network access. Token-Ring uses a token that grants its holder the right to transmit information. A third variant is the announcement of detailed time-tables informing each node in which frame of time it is entitled to send its data.

For communication protocols in the automotive domain the first and the third type of media access are popular. The first, e.g., is used by CAN networks, the third is used for TTP/C [TTP03] or FlexRay [Fle04] though their philosophy in using time-slots differs.

2.2.1 Event-Triggered Transmission

In networks using protocols following the event-triggered approach for media access the nodes have to verify that the media is currently not used. After a node has established that the medium is currently not occupied it is allowed to transmit its information. If the medium is occupied, the node has to delay the transmission until after the current transmission has finished. If multiple nodes are waiting for a transmission to finish, it is possible that they will simultaneously begin to transmit their information after the current transmission has finished. This behaviour leads to garbled information, a collision. The protocols have to provide a method for identifying and resolving this event.

CAN, a protocol using the event-triggered approach, transmits after the "Start of Frame"-bit as first element an 11bit identifier. This identifier is used for the negotiation which node is allowed to transmit. If a node transmits a message and detects while transmitting its identifier a state of the network that differs from the one that should have resulted out of its own transmission, the node recognises that it has lost the arbitration to another node. The node detecting this must withdraw from its attempt to send information as another node trying to send apparently has an identifier representing a higher priority.

2.2.2 Time-Triggered Transmission

Protocols using time-triggered access to the medium, control the access to the medium by defining time-slots, small time-spans, during which the exclusive right to transmit is granted to one node. This approach of time division multiple access (TDMA) has certain side-effects. First, the precision and synchronisation of all clocks in the system is essential as the size needed for the time-slots and thereby the efficiency of the protocol depends on the accuracy of timing. Second, the assurance that only one node is allowed to transmit and only this node actually transmits its information. Third, the inflexible reaction towards actual information emergence in contrast to planed or statistically awaited information emergence. If a node has no data to transmit the efficiency of resource usage is reduced.

The effects of the last point are tried to be mitigated by different protocols. QWIK [JLL99], for example, assigns a number of sending sequences with a fixed chronology of time-slots each node is aware of. The sequence that is actually used

can be decided in regard of the needs for data transmission in a given situation.

TTP/C [TTP03] tries to raise the efficiency of its bandwidth usage by allowing for time-slots to be shared by several nodes. Using statistical information these multiplexed slots are assigned to one node.

2.3 SAE Classifications

The requirements for communication networks are divided by the Society of Automotive Engineers (SAE) into three classes [Bel01]. As Lupini [Lup03] pointed out, it is reasonable to supplement these classes by new protocol classes applicable towards new types of communication.

First classification tried to specify requirements for one bus system suitable for handling all types of communication needed in a vehicle. The varying needs of applications and the higher price of communication nodes induced by higher requirements led to many different networks being installed into one vehicle.

Class A covers low-end, diagnostic (with the exempt of emission diagnostic) and general purpose communication. The transfer rate is typically below 10 Kb/s and the procurement price for each node is low. Examples for Class A protocols are UART, I^2C [I2C00] and LIN [vW03]. The SAE classification requires protocols of this class to provide event-triggered communication.

Class B networks are mid-speed networks (10Kb/s to 125Kb/s) for general information transfer like non-diagnostic, non-critical communication. The protocols of this class must provide event-driven and some periodic transmission including sleep and wakeup functionality. Nodes for Class B protocols usually cost twice as much as Class A nodes. Examples for Class B protocols are CAN (ISO 11898), GMLAN and J1850 with CAN being the protocol mostly used.

Class C networks are high speed networks (>125Kb/s) for real-time control [Bel01]. They are used for engine timing or fuel delivery and provide transfer rates from 125Kb/s to 1Mb/s. Class C protocols support transmission of periodic information. The price per node is 3 to 4 times the price of a Class A node. This price can be even higher if high quality wiring like STP (Shielded Twisted Pair) or fibre optics are required [Lup03]. CAN 2.0 [CAN91], Boeing's Intellibus or J1939 are protocols that achieve Class C functionality.

Other classes of networks and protocols listed by the SAE Technical Paper "Multiplex Bus Progression 2003" [Lup03] are Emissions Diagnostics, Mobile Media (differentiated into Low Speed, High Speed and Wireless), Safetybus and Drive-by-Wire.

These additional classes are necessary as differing tasks pose requirements on the communication making it difficult to combine these needs into one set of requirements. The requirements made on "On Board Diagnostic Systems" (OBD) that are used to control the exhaust and combustion process for the reduction of the vehicle's emissions is one of these tasks. Other applications pose special requirements as well. Video transmission requires high bandwidth to be available and safety critical tasks like airbag-control or X-by-Wire systems make high demands towards the reliability of the communication system.

2.3.1 X-by-Wire

For X-by-Wire applications like Brake-, Throttle- or Steer-by-Wire, bandwidths between 1 and 10Mb/s are required. The protocols used for these tasks have to be reliable, provide high performance and real-time information transmission. Because of these requirements the price for one node is much higher than the price of one Class A node (around 15 times as high) [Lup03].

Some of the protocols developed for these tasks are TTAgroup's TTP/C [TTP03], FlexRay [Fle04] or TTCAN [FMD+00].

The Brite-EuRam III project "Safety Related Fault Tolerant Systems in Vehicles (X-By-Wire)" [Bri98] elaborated from 1996 to 1998 a framework for automotive by-wire applications. Findings from this project were used in the ESPRIT 4 OMI project "TTA" that developed a generic time-triggered computer architecture (TTA) for the use in "fault-tolerant distributed real-time systems" [Eur96].

2.3.2 SAE Class C Requirements

In addition to the required speed of transmission, the SAE developed a taxonomy of requirements and a benchmark consisting of 53 message types and their requirements on size, transmission frequency and latency as depicted in Figure 2.1.

The taxonomy for safety critical applications given in [Soc93a] (cited after [DFMP97]):

Regularity of Information Transfer Control-oriented messages perform their task periodically, producing large amounts of data exchange. In addition real-time systems have to cope with chance events outside their sphere of control like failure events. These produce irregular communication. If a minimum inter-arrival period between chance events of the same type can be identified the type of event can be regarded as quasi-periodic.

Minimal Message Latency The application's needs determine the values acceptable for the latency of the information exchange. It depends on aspects like the bandwidth, the protocol's logical structure or the medium access method.

Fault-tolerance For safety-critical applications the detection of an error alone is not sufficient, the system has to provide a fail-operational behaviour. This behaviour must be guaranteed up to a predefined number of failures.

Robustness The communication system is vital and exposed to electromagnetic interference. It has to be tolerant to electromagnetic interference and be able to recover from a "blackout" with minimal latency.

Error detection For failures of nodes to be identified methods for reaching a consensus on which nodes and functions are operational have to be provided. Changes in this context have to be detected unanimously and timely.

Acknowledgement and Atomic Transmission Some applications require the notification that information was transmitted properly to the receiver. Other applications require a message to be received either by all recipients or by none. If such applications are needed, acknowledgement schemes and atomic transmission must be possible.

Testing The architecture should support a constructive testing method providing the possibility of every component being tested independently. This has to include that the integration of components that have passed the test does not produce side-effects.

Configurability/Composability Composability describes the behaviour that properties established with a subsystem are maintained in a super-system constructed by integration of the subsystem with others.

Because of the safety critical nature of X-by-Wire systems, the requirements on the SAE benchmark's messages for Class C networks have to be met. The SAE

Signal number	Signal description	Size/ bits	Periodic/ Sporadic	Period time/ latency(ms)
1	Traction Battery Voltage	8	P	100.0
2	Traction Battery Current	8	P	100.0
3	Traction Battery Temp; Average	8	P	1000.0
4	Auxiliary Battery Voltage	8	P	100.0
5	Traction Battery Temp; Max	8	P	1000.0
6	Auxiliary Battery Current	8	P	100.0
7	Accelerator Position	8	P	5.0
8	Brake Pressure; Master Cylinder	8	P	5.0
9	Brake Pressure; Line	8	P	5.0
10	Transaxle Lubrication Pressure	8	P	100.0
11	Transaction Clutch Line Pressure	8	P	5.0
12	Vehicle Speed	8	P	100.0
13	Traction Battery Ground Fault	1	P	1000.0
14	Hi & Lo Contactor Open/Close	4	S	5.0
15	Key Switch Run	1	S	20.0
16	Key Switch Start	1	S	20.0
17	Accelerator Switch	2	S	20.0
18	Brake Switch	1	S	20.0
19	Emergency Brake	1	S	20.0
20	Shift Lever (PRNDL)	3	S	20.0
21	Motor/trans Over Temperature	2	P	1000.0
22	Speed Control	3	S	20.0
23	12V Power Ack Vehicle Control	1	S	20.0
24	12V Power Ack Inverter	1	S	20.0
25	12V Power Ack I/M Contr.	1	S	20.0
26	Brake Mode (Parallel/Split)	1	S	20.0
27	SOC Reset	1	S	20.0
28	Interlock	1	S	20.0
29	High Contactor Control	8	S	10.0
30	Low Contactor Control	8	P	10.0
31	Reverse and 2nd Gear Clutches	2	S	20.0
32	Clutch Pressure Control	8	P	5.0
33	DC/DC Converter	1	P	1000.0
34	DC/DC Converter Current Control	8	S	20.0
35	12V Power Relay	1	S	20.0
36	Traction Battery Ground Fault Test	2	P	1000.0
37	Brake Solenoid	1	S	20.0
38	Backup Alarm	1	S	20.0
39	Warning Lights	7	S	20.0
40	Key Switch	1	S	20.0
41	Main Contactor Close	1	S	20.0
42	Torque Command	8	P	5.0
43	Torque Measured	8	P	5.0
44	FWD/REV	1	S	20.0
45	FWD/REV Ack.	1	S	20.0
46	Idle	1	S	20.0
47	Inhibit	1	S	20.0
48	Shift in Progress	1	S	20.0
49	Processed Motor Speed	8	P	5.0
50	Inverter Temperature Status	2	S	20.0
51	Shutdown	1	S	20.0
52	Status/Malfunction (TBD)	8	S	20.0
53	Main Contactor Acknowledge	1	S	20.0

Figure 2.1: SAE requirements for Class C systems [Soc93a] (as in [JLL99])

survey on a wide spectrum of commonly used networks [Soc93b], including J1850, CAN, VAN [VAN94] and AUTOLAN, concluded that none of these protocols satisfies the requirements of distributed safety critical applications on-board vehicles [DFMP97].

2.4 Requirements for Production

The requirements of the production have influenced the taxonomy described in chapter 2.3. In the automotive environment systems have to operate under the electromagnetic interference of other components in the vehicle or from outside. The communication system has to be designed to cope with the possibility of transmissions being modified or drowned by sources outside the system.

The construction of systems by integration of existing subsystems makes it desirable to do the assertion of attributes and functions for the respectively subsystems and transferring the assertions made onto the constructed system. The assumption, that it is possible to make this transfer, has to be ascertained by the construction process.

It is also desired, that by using the results of testing every component on its own conclusions on the complete system's performance can be drawn. This can only be achieved if the construction process ascertains the complete modularity of the system, guaranteeing that one component interacts with any other component only by using predefined interfaces or attributes.

Besides technical considerations and requirements, marketing requirements have also to be made on the system. The brand differentiation is largely influenced by the vehicle's handling. Until now, comfort and handling of the vehicle, important factors of the brand differentiation, result from the selection of hydraulic and mechanical components used in the vehicle. If the mechanical vehicle control is replaced by electronic systems contingencies for influencing the handling of the vehicle have to be provided. These have to maintain or adjust the handling of the vehicle to meet the customers desires or expectations.

3 Ontological Analysis: Iterative Decomposition

3.1 The Concept of Ontological Analysis

Ontological Analysis is a method for requirement development [Lad05]. Starting with a very simple system description, the system's ontology is iteratively expanded until it can be used for describing the system with the desired level of detail.

The approach starts from the description of a simplified system concentrating on basic properties and functions. Using this description an ontology of the system is developed. This ontology is then used to describe the causal relationships between its elements and their behaviour leading to failures or unwanted events.

By investigating causal relationships between elements of the ontology a systematic approach to the identification of basic system dynamics leading to unwanted events is introduced into the analysis. A method to achieve this is the Causal System Analysis [Lad01].

For the acceptance of the requirements developed, it is very important that the level of confidence given to the result is as high as possible. This confidence largely depends on the questions "Have I thought of everything?" and "How do I know, that I have thought of everything?" [Lad05], the completeness question.

It may be impossible to answer the first question with an unconditional "yes". Something could always have been missed, at least if a problem is not conceived as a problem. The question can therefore only be answered by using the level of confidence that has been achieved towards the developed system.

The measure for the level of confidence is the ratio of failures being identified by the analysis to the number of failures the system experienced after the develop-

ment. As the number of failures identified by experience and statistics increases with time, one can say, that the level of confidence given to the developed system increases with time.

For new developments it is not possible to gain the knowledge on possible failures of the developed system over the time. If the development is a modification of an older system of which already longtime experience was gained it can be possible to use this experience assuming that this knowledge can be applied in case of the new system. If the system is a brand new development neither gaining experience over time nor applying knowledge from former developments. In this case it is not possible to answer the completeness questions properly using only external failure knowledge.

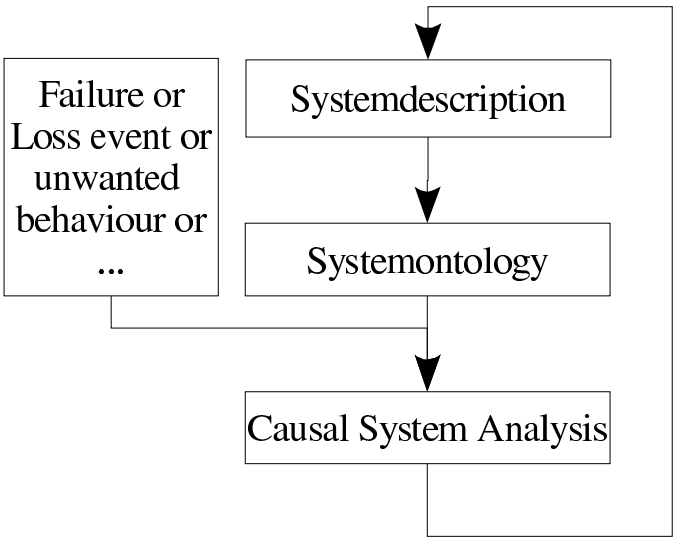


Figure 3.1: Simplified Development Process

Looking at a simplified approach to the system development using an iterative process [Fig. 3.1], it becomes obvious that for answering the first of the completeness questions any possible accident to the system has to be identified.

This is a results from the Causal System Analysis's approach of analysing relationships between elements in a "top-down" style. It identifies the causes leading to the occurrence of a higher event. This means that possible results of the highest node, the top-node, are not identified by this method. Because of this it is not possible to argument on the relations between events leading to a failure if this failure was previously not identified.

A method for systematic identification of failures or unwanted events could be

integrated into the analysis work-flow by using the ontology's elements for identifying these events. HAZOP (see chapter 3.4) provides such an approach by systematically combining guide-words with properties and identifying possible hazards to the system [CIS77][RCC99].

A second question important for the developed system is concerning the level of risk posed by the system. The system described by the developed ontology contains a certain level of risk. For the acceptance of a technical system it is important that this risk be smaller than the risk considered acceptable. The need of risk reduction as pointed out by regulations, may be required by acts or the need of standards to be fulfilled. As an example for requirements made for a system's risk as stated in German regulations an excerpt of the Eisenbahn Betriebs Ordnung is given: "Bahnanlagen und Fahrzeuge müssen so beschaffen sein, daß sie den Anforderungen der Sicherheit und Ordnung genügen. Diese Anforderungen gelten als erfüllt, wenn die Bahnanlagen und Fahrzeuge den Vorschriften dieser Verordnung und [...] anerkannten Regeln der Technik entsprechen." [Bun67, §2] (cited after [Fin68]). The United Kingdom's legislation requires specific measurements of risk to be met. The 1974 Health and Safety at Work Act demanded, that "it shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees." [HSA74, General duties(1)]. The IEC61508 standard demands that "the necessary risk reduction shall be determined for each determined hazardous event." [Int97, Part 1, 7.5.3(4.69)].

Because of this need, the system described by the ontology and by the Causal System Analysis has to be investigated with regard to risk. If the need for risk reduction is identified, appropriate countermeasures have to be developed.

For the system modified by countermeasures, the interaction of the extensions with the rest of the system must be examined. This is achieved by including the extensions into the system and analysing the extensions' impact in the next iteration step.

After integration of hazard-identification and risk-assessment the complete work-flow of the ontological analysis can be depicted as in Figure 3.2.

The concept of Ontological Analysis can be divided into two segments: first the process of the iterative decomposition of a system, second the safety and risk analysis. The first segment contains the steps needed for the refinement of the system description, the second the steps needed for the identification of possible

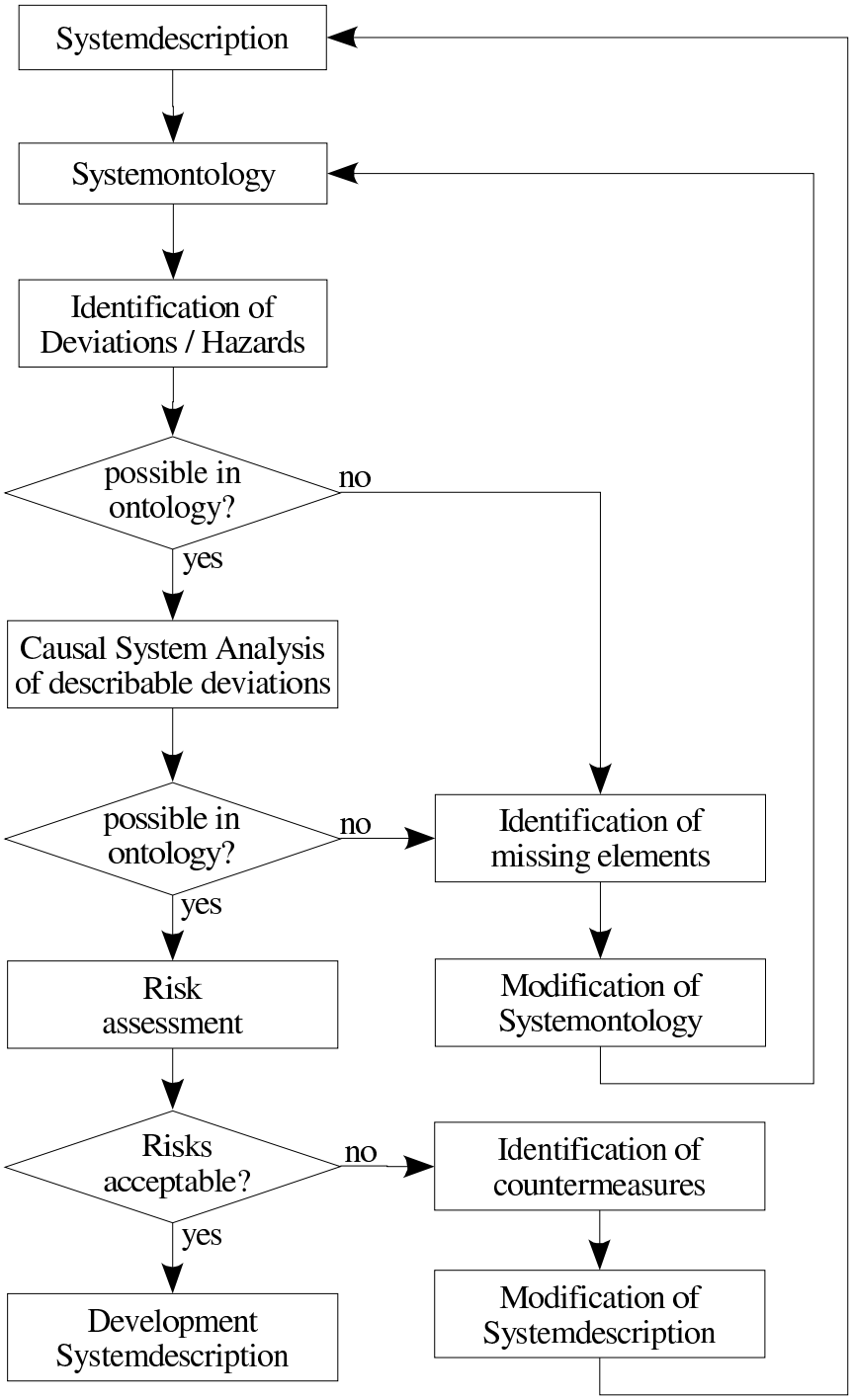


Figure 3.2: Extended OA Approach

failures of the system, the impact of these failures and the hazardous system states leading to any of these failures as well as the specification of safety requirements the implemented system has to meet. This segmentation is shown in Figure 3.3.

3.2 System Description

3.2.1 Information Needed for the Development

Before the system description can be developed, information on the system's objectives have to exist. This information should be made on the most abstract level on which the objectives can be described. It is possible to form the first description by making a diagram of the system that contains all the necessary elements to enable the system to reach its main objective. Based on this diagram a narrative text can be formed that describes the work-flow and activities that have to occur to reach the main objective. These information can be difficult to integrate into a diagram drawn to be as simple as possible.

It can happen, that the system's objectives already contain an incident scenario that has to be avoided. In this case the incident to be avoided is an objective of the system and the system description is formed at the most abstract level on which all objectives can be described. This may lead to a more elaborated system description but ensures that the relations leading to the incident scenario are thoroughly analysed from the beginning of the system development.

3.2.2 Description of the Communication System

The system investigated in this thesis is a communication system for use in the automotive domain which can be used for safety-critical control systems without mechanical backup. For this system the following usage description is made which could be represented in a simple way as in Figure 3.4. This figure partitions the displayed components into system and environment. Following [Lad01, chapter 3.3] the system consists of elements interacting to achieve a defined objective. The system's elements receive input from the environment and influence the environment by their output.

- The driver controls and manipulates the vehicle using the steering wheel,

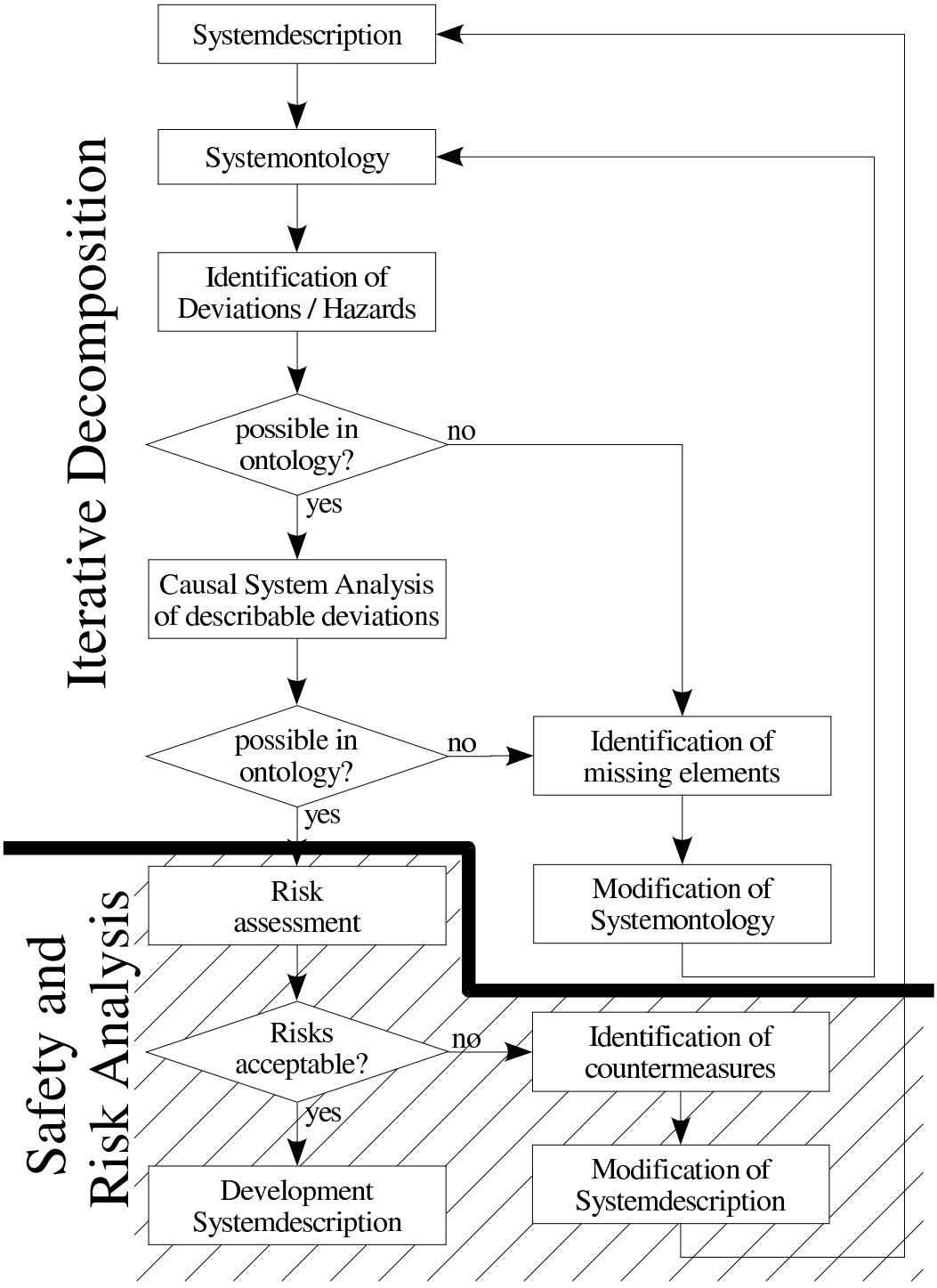


Figure 3.3: Iterative Decomposition and Safety & Risk Analysis

pedals, shift box and selector switches.

- The input is converted by sensors into signals which are presented to the network interface.
- The sensor's network interface transmits the signals using the network bus.
- The network bus distributes the signal to each network interface connected to the bus.
- Other network interfaces receive the signal and relay it to its connected device if the information is addressed to them.
- The device acts on the received information and either directs actuators under its control or computes a reaction.
- If the device has computed a reaction that is needed to be transmitted to another device, the information is presented to the network interface that transmits it using the network bus.

The purpose of the system is to enable communication needed by safety critical applications, e.g., X-by-Wire applications. For these systems at least the requirements demanded of SAE Class C networks must be met (see chapter 2.3). Additionally it has to support messages sent both time- and event-triggered mode as this was set as a requirement for the investigated system.

These needs provide the simplified system description that is to be used in the further analysis.

3.2.3 Extension of the System Description

The analysis starts from a rather abstract level of description. During the analysis sections of the system description are found to be described not detailed enough and necessary system details need to be introduced into the system. This perception is achieved through the expression of deviations in the ontology, through the analysis of relationships in the Causal System Analysis and through the safety and risk analysis. All these analysis tasks identify missing elements in the system description. The Causal System Analysis and the expression of deviations in the ontology both identify missing elements in the ontology, the safety and risk

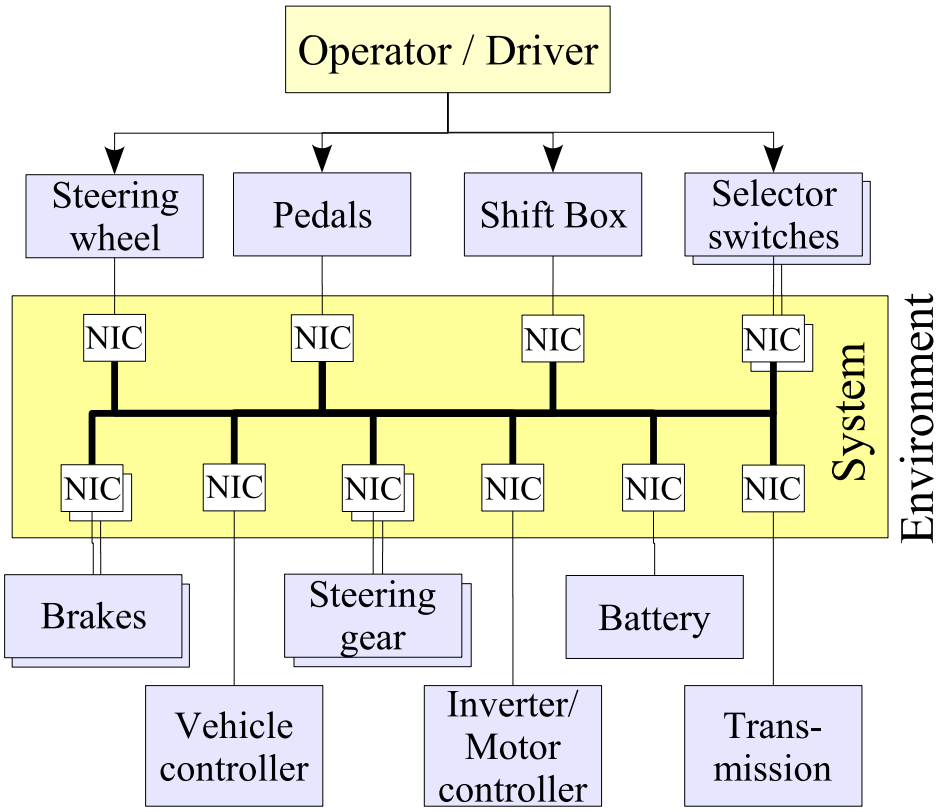


Figure 3.4: Schematic representation of automotive communication

analysis identifies modifications needed to be made to the system to reduce the level of risk posed by the system.

The extensions identified by the expression of deviations in the ontology and the Causal System Analysis can be introduced directly into the system ontology as the identification is done in the ontological notation.

The integration of extensions identified for risk reduction is made similar to the formulation of the initial system description. To avoid needed additions to the ontology being overlooked the modifications needed for the system are described like the initial system description. This description is then used for the identification of necessary additions to the ontology.

3.3 System Ontology

The system ontology is the body of formally represented knowledge of the system like Gruber and Olsend pointed out [GO94]. This knowledge is based on the developer's experience about the domain of the described system and its objectives. Ontology originates in the philosophical domain. The philosophical discipline of Ontology is described as "that department of the science of metaphysics which investigates and explains the nature and essential properties and relations of all beings, as such, or the principles and causes of being." [Por13]. By using ontologies it is possible to describe a system and the interactions of the system's objects. The formed ontology can be regarded as the vocabulary of a language used for the description of the system's behaviours.

By formulating an ontology of a system developed, it is possible to formalise the knowledge gained on the system. Following Genesereth and Nilsson "the fomalization of knowledge in declarative form begins with a conceptualization." [GN87]. Gruber pointed out, that "an ontology is an explicit specification of a conceptualization." [Gru93]

Ontologies with different structures exist. All have in common their objective to describe the elements of a system by studying the essential characteristics of elements that are needed to regard these element as entities. Older ontologies describe the system by building a conceptualisation consisting of the triple universe of discourse, a functional basis set for the universe and a relational basis set. Younger ontologies like the ontologies developed by the Web Ontology Language OWL [BvHH+04] consists of the universe of discourse, the relations and entities.

Every member of the functional basis set can be described as a relation between an element of the universe of discourse and an element representing a value. It can therefore be said, that every ontology of the former structure is an ontology of the later structure with an empty set of entities.

If the ontology is regarded as the vocabulary of a language, the way of using the vocabulary can make it possible to identify different entities of one object. One way of distinguishing objects is "Object A or Object B", where only the element "Object" is part of the ontology.

With these two statements, both types of structure can be regarded as being equivalent. Although the entities of an OWL ontology would have to be registered in an additional document if a transfer without loss of information is wanted.

The ontologies used for the ontological analysis in this work form the triple of objects, properties, and relations. The meaning or definition of every element in the ontology is noted as precisely as possible to ease the reasoning on the attribute-guide-word combinations formed by the HAZOP approach of identifying deviations.

3.3.1 Objects

Webster defined objects as everything, "about which any power or faculty is employed, or something apprehended or presented to the mind by sensation or imagination." [Web28].

Following this definition, everything that can be controlled, has a function or is presented to the mind is an object. Although this is a wide definition it enables the formulation of ontologies on logical constructs like messages in a communication system.

In the development process virtual objects like messages or information as well as imaginary elements are needed, structures which would be objects if they were realised. If it were not possible to argue on imaginary objects the system could not be analysed in detail.

3.3.2 Properties

Property is defined as "a peculiar quality of any thing; that which is inherent in a subject, or naturally essential to it" [Web28]. This means, that properties are attribute-value pairs, where the attribute is an element of the universe of discourse and the value is an element of a given range of values. They are un-ary relations of objects with objects representing values or identifiers, such as the latency of a message is a property that relates to a timing value like 5ms or the property colour of a cable relating to an object representing the colour RAL2009.

3.3.3 Relations

A relation is a "connection between things; mutual respect, or what one thing is with regard to another" [Web28]. Relations are n-ary interrelations that exist

between multiple objects.

It has to be noted, that the distinction between two kinds of un-ary relations is artificially made in this work. An un-ary relation between an objects of the ontology and an element of the universe of discourse is identified as a relation in this work whereas an un-ary relation between an object of the ontology and and element of a given range of values is identified as a property of the object.

3.3.4 Initial System Ontology

The initial system ontology is developed by identifying the most general objects needed for the system to fulfil its purpose. For these objects the necessary properties and relations that are essential for the operation are identified.

Based on the initial system-description three objects with 10 properties and one relation were identified. They are listed in the following tables with the definition of their meaning.

Object	Description
NIC	The Network Interface Controller. This is the interface between the input device and the physical network.
Wiring	The physical connection between the systems' NICs.
Transmission	The transport of information between NICs over the physical network.

Object:	**NIC**
Property	Description
Input	The information received by the NIC
Output	The information transmitted by the NIC
Intact	The integrity of the NIC, whose absence prevents the NIC from working properly.

Object:	**Wiring**
Property	Description
Intact	The integrity of the wiring, whose absence prevents the physical network from working properly.

Object:	**Transmission**
Property	Description
Size	The size of the transmission
Deadline	The latest possible point in time at which the transmission can be received without loosing its value.

Property	Description
Period	Frequency of the generation of a type of transmission
Mode	The mode used for a transmission. This can be either time-triggered or event-triggered.
Latency	The time it takes for the complete transmission of information over the network.
Jitter	The variance in the transmission time of a multitude of same-typed transmissions.

Relation	Description
Connection (Wiring, NIC)	The feature of the NIC to be connected properly with the Wiring.

3.4 Hazard-Identification

For the integration of the failure identification into the development a systematic approach is needed like the identification of deviations provided by the HAZOP technique. Hazards in HAZOP are defined as the "potential source of harm", where harm is "physical injury of damage to the health of people or damage to property or the environment" [Int01].

A central element of the HAZOP method is the identification of deviations, which can cause a hazard to occur. These deviations are discrepancies between the system behaviour and the intention the designer had in mind while constructing the system [RCC99, p.4]. The identification of all possible deviations is sufficient for the analysis resulting in all possible causes of a hazard being identified. This counterfactual relation leads to the avoidance of the hazard if any of its causal factors is absent (see chapter 3.5). By identifying possible deviations from the design intent not only the causes for hazards are identified, but also the indices towards operational problems that could possibly lead to problems are identified as well.

The deviations are generated first by the process of combining elements with a set of guide-words and then by arguing on the interpretation of the generated argument-guide-word combinations and identifying possible deviations form this interpretation process.

3.4.1 HAZOP Technique

The technique of hazard and operability study (HAZOP) was developed by Mond Division of ICI in 1963 and was adopted into standards and guidelines. It was described in [CIS77] and [RCC99] and has found widely use not only in the chemical domain but also in electro-technical and software applications in form of Process HAZOP or Software HAZOP.

A HAZOP analysis can be used for the identification of systematic weaknesses during the system design or at any time afterwards, e.g., in redesign after an incident. The analysis is performed in meetings by a team of 8 to 10 members.

Central method in the analysis is the generation of deviations by combining guide-words with attributes. The attributes are sections of the system analysed. For the deviations to be useful it has to be agreed on the guide-words used and their interpretation on a deviation. For some domains such interpretations are available, e.g., by the Royal Society of Chemistry [HMW01] which can be adapted for use in other domains. It is important that the complete HAZOP team agrees on the guide-words and their meaning. If a missing guide-word is identified at a later point in the analysis all previously analysed attributes must be analysed in respect of this new guide-word, too. Therefore a list of guide-words as complete as possible is wanted for the investigation.

The deviations are assessed by considering the effects they can have on the system. During this assessment modes of operation and the physical layout of the system has to be taken into account as well as the logical system design. Deviations describing a hazard to the system are recorded, its causes identified and countermeasures developed. The proceedings and results of the analysis are composed into a report for documenting purposes.

3.4.2 HAZOP Guide-Words

In Table 3.6 a list of guide-words and their interpretation proposed by the Royal Society of Chemistry (RSC) [HMW01] and Redmill, Chudleigh, Catmur (RCC) [RCC99] is shown.

The interpretation of the guide-word's meaning varies or was made with greater detail in the different versions.

Table 3.6: HAZOP Guide-Word Interpretations

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

Guide-words useful for the study of programmable electronic systems were identified in [Min94] by the UK Ministry of Defence. These are *no, more, less, as well as, part of, reverse, other than, early, late, before* and *after*. These are identical to the guide-words suggested by RCC who have formulated easily usable interpretations for them.

The guide-word *where else* suggested by the [HMW01] is omitted because of the following reasons. Its interpretation *Applicable for flows, transfers, sources and destinations* is problematic when used for the interpretation of sentences. It does not describe what the guide-word affects but where it can be used. Because of this the interpretation of *where else* is not clear and it looks like it is at least in network systems identical to *as well as*. As it is not part of the guide-words used by [RCC99], [CIS77], and [Min94], as well as [HMW01] itself listing it under "additional", it is omitted in the analysis of the network system in this work.

3.4.3 Attribute-Guide-Word Combinations

The agreed-on guide-words are combined systematically with every attribute of the ontology. This generates a set of tables similar to the one represented in Table 3.7.

Table 3.7: Attribute-Guide-Word Combinations for Latency(Transmission)

Attribute:	**Latency(Transmission)**
Guide word	Interpretation
No	a. Transmission has no latency
	b. Latency requirements not met
More	Transmission latency is bigger than intended
Less	Transmission latency is lower than intended
As well as	Additional latency occurred
Part of	Design intention of latency is partially achieved
Reverse	Logical opposite of transmission latency occurred
Other than	Complete substitution of transmission latency
Early	The actual latency timing effects earlier than intended
Late	The actual latency timing effects later than intended
Before	Latency occurs ahead of sequence
After	Latency occurs after sequence
Faster	Latency is defined too small
Slower	Latency is defined too big

3.4.4 Interpretation of Combinations

Some of the combinations formed cannot be interpreted while others can be interpreted in more than one way. For the later all interpretations are listed in the table like "No Latency(Transmission)", that can be interpreted as the lack of latency for a transmission or as the failure of the transmission to meet the latency requirements.

In most cases it will be possible to form a valid sentence out of a attribute-guide-word combination. Some combinations may not be expressible in a sentence and some combinations may not be interpretable. These are listed with the justification why they need not be considered as a deviation in the following analytical steps.

As an example the justification of left out combinations for "Latency(Transmission)" is shown below.

Less/Faster latency A latency smaller than intended is significant for an improved communication. Therefore this deviation represents no hazard.

As well as latency The latency is a value for the time needed for transmission of a message. Each message has only one latency. "Additional latency occurred" could mean that more than one message is transfered.

Part of latency Latency is a property implied by every kind of communication and cannot be partially achieved.

Reverse latency For latency as the gap between the sending and receiving of a message a logical opposite cannot be defined.

Other than latency This deviation is without meaning as a message transfer without latency is the same as a message transfer with latency zero. Therefore a transmission has to have a latency.

Before/After latency This deviation is without meaning as the latency has no sequence.

3.4.5 Using Assumptions

Assumptions often are used in the development to narrow the area of the system analysed. It can be argued to omit an identified deviation in the further investigation if the probability of the deviation leading to a failure is regarded as being very low. As an example the possibility of an outside event damaging a pipe is very low if the pipe is located in a high security area of a bunker two miles below the earth. In the example the occurrence of the deviation is mitigated by already existent elements that are present outside of the system.

If assumptions are made during for the interpretation of deviations the depth to which the analysis is made will be influenced. To provide that any failure possible in the system is accounted for, these assumptions have to be written down and their assertion made obligatory.

The example above demonstrates the importance of this demand. If the system containing the pipe would be build on ground level, the assumption could not be maintained. In this case the system description would have to be extended to maintain the assumption. This could be achieved by the construction of a bunker for the operation of the system.

In the interpretation of the first iteration's attribute-guide-word combinations the following assumptions were made:

Table 3.8: List of assumptions made in deviation identification (1^{st} iteration)

	Assumption
Ass01	The NIC is intact until stated otherwise.
Ass02	The Wiring is intact until stated otherwise.
Ass03	The Size(Transmission) can be measured instantaneously.
Ass04	Only time- and event-triggered transmissions will be made.
Ass05	Relations between NIC and the Wiring do not threaten the connection.

These assumptions have to be guaranteed, e.g., the third assumption results from the necessity to compute the size of a transmission before deciding if it is larger or smaller than expected or required. As this computation is made after receiving the transmission, the information on the size of the received transmission will be present at the point in time when the decision is to be made. Therefore it can be regarded as being instantaneously measured in regard to this operation.

Other assumptions, like the fourth of the above list could be guaranteed by introducing design regulations and verifying the development process and result against these regulations.

The identification of missing elements in the iterative decomposition phase is based on the results of expressing the identified deviations in the ontology and the results of the Causal System Analysis. With every assumption introduced into the interpretation of the attribute-guide-word combinations the results of the deviation are not analysed in further detail. The analysis's level of depth can therefore be controlled by the use of assumptions. Again this demonstrates the need for assumptions being guaranteed to maintain the system's functionality.

3.4.6 Ontologically Expressing Deviations

The remaining combinations following the attribute-guide-word combinations' interpretation form a list of deviations the system is susceptible to. This list can be written down and a number given to each deviation for identification purposes like presented in table 3.9.

Table 3.9: List of 1^{st} iteration's deviations

	Deviation
1.a	More NICs in system than expected
1.b	Less NICs in system than expected
1.c	A NIC is fragmented
2.a	Wiring too long
2.b	Wiring too small

	Deviation
2.c	Other medium in addition to wiring present
2.d	Wiring meets design intention only in part
3.a	No information is transmitted
3.b	More information than intended is transmitted
3.c	Less information than intended is transmitted
3.d	Additional information is transmitted
3.e	Information is only partially transmitted
3.f	Information is well formed but carries wrong content
3.g	Information is reversely transmitted
3.h	Information is sent too early
3.i	Information is received too early
3.j	Information is sent too late
3.k	Information is received too late
3.l	Information is sent ahead of sequence
3.m	Information is sent behind sequence
3.n	Transfer rate greater than intended
3.o	Transfer rate lower than intended
4.a	NIC does not get input
4.b	NIC receives more input from the device than expected
4.c	NIC receives more input from the network than expected
4.d	NIC receives input from more sources than intended
4.e	NIC reverses received input
4.f	NIC receives input early
4.g	NIC receives input late
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
6.a	The NIC is not intact
7.a	The wiring is not intact
8.a	Transmission has no size
8.b	Transmitted information is bigger than sent message
8.c	Transmitted information is smaller than sent message
8.d	Simultaneous transmission of several information blocks
8.e	Additional transmission of content
8.f	Only part of the information size is transmitted
9.a	The information is not transmitted in time
9.b	Deadline value is too small
10.a	A class of transmission occurs more often than defined
10.b	A class of transmission occurs less often than defined
11.a	Information is not transmitted
11.b	Event-triggered transmission is sent in time-triggered mode
11.c	Time-triggered transmission is sent in event-triggered mode
12.a	Transmission latency is bigger than intended
12.b	Latency is defined too big
13.a	Jitter is bigger than intended

	Deviation
14.a	No connection between wiring and NIC exists
14.b	More connections between wiring and NIC exist than designed for

The next task in the Ontological Analysis is the Causal System Analysis that identifies causal factors leading to a failure or hazard. This method is based on the description of the failure using the system's ontology. Therefore a conversion from the deviation described narratively into an ontological description has to be made.

The system ontology can be understood as definition of a vocabulary for the description of system behaviour. The deviations identified have to be describable using this vocabulary as the deviations represent problematic behaviour of the system's elements. For the later step of analysing the causal relations between the system's elements it is necessary to describe the deviating behaviour in terms of the system ontology.

As the ontology available in early analysis iterations is centred on the basic system operation it is very limited in its expressiveness. The attempt of expressing the first iteration's deviations with its ontology resulted in the analogues shown in table 3.10. Only 19 out of 59 deviations are expressible.

Table 3.10: Ontological Expressions possible in 1^{st} iteration

	Ontological Expression
1.a	*needed: Network, NodeCount(Network)*
1.b	*needed: Network, NodeCount(Network)*
1.c	Intact(NIC) = False
2.a	*needed: Length(Wiring)*
2.b	*needed: Length(Wiring)*
2.c	*needed: Interference(Network, Universe), Universe*
2.d	*needed: Requirements(Wiring)*
3.a	Size(Transmission) = 0
3.b	*needed: RequiredSize(Transmission)*
3.c	*needed: RequiredSize(Transmission)*
3.d	(Transmission A) AND (Transmission B)
3.e	Input(NIC Receiver) < Size(Transmission)
3.f	*needed: Format(Transmission)*
3.g	Output(NIC) = INVERSE(Input(NIC))
3.h	*needed: TimeSent(Transmission), RequiredTimeSent(Transmission)*
3.i	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
3.j	*needed: TimeSent(Transmission), RequiredTimeSent(Transmission)*
3.k	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
3.l	*needed: Sequence(Transmission), RequiredSequence(Transmission)*
3.m	*needed: Sequence(Transmission), RequiredSequence(Transmission)*
3.n	*needed: TransferRate(Transm.), RequiredTransferRate(Transm.)*
3.o	*needed: TransferRate(Transm.), RequiredTransferRate(Transm.)*

	Ontological Expression
4.a	Input(NIC) = 0
4.b	*needed: DataRate(Device), Device, DataRate(NIC)*
4.c	*needed: SizeRequirement(Transmission)*
4.d	*needed: Network, NodeCount(Network), DesignNodeCount(Network)*
4.e	Output(NIC) = INVERSE(Input(NIC))
4.f	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
4.g	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
5.a	Output(NIC) = 0
5.b	*needed: DataRate(NIC)*
5.c	*needed: DataRate(Device), Device*
5.d	Input(NIC) > Output(NIC)
5.e	Output(NIC) = INVERSE(Input(NIC))
5.f	*needed: Interference(Network, Universe), Universe*
5.g	*needed: TimeSent(Transmission), RequiredTimeSent(Transmission)*
5.h	*needed: TimeSent(Transmission), RequiredTimeSent(Transmission)*
6.a	Intact(NIC) = False
7.a	Intact(Wiring) = False
8.a	Size(Transmission) = 0
8.b	Input(NIC) > Size(Transmission)
8.c	Input(NIC) < Size(Transmission)
8.d	(Transmission A) AND (Transmission B)
8.e	*needed: Content(Transmission)*
8.f	Input(NIC) > Output(NIC)
9.a	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
9.b	*needed: TimeReceived(Transm.), RequiredTimeReceived(Transm.)*
10.a	*needed: RequiredPeriod(Transmission)*
10.b	*needed: RequiredPeriod(Transmission)*
11.a	Size(Transmission) = 0
11.b	*needed: RequiredMode(Transmission)*
11.c	*needed: RequiredMode(Transmission)*
12.a	*needed: RequiredLatency(Transmission)*
12.b	*needed: RequiredLatency(Transmission)*
13.a	*needed: RequiredJitter(Transmission)*
14.a	Connection(Wiring, NIC) = False
14.b	*needed: DesignNodeCount(Network)*

To allow for the next iteration's ontology to be extended into a form that allows all deviations not expressible with the current ontology to be expressible with the next iteration's ontology it proved useful to formulate possible expressions using elements not present in the current ontology.

For example deviation 3.b "More information than intended is transmitted" is not expressible using the first iteration's ontology. For stating that an actual value is higher than intended a benchmark for the intended value has to be available. To identify the elements missing in the ontology the expression "Size(Message) > SizeRequirement(Message)" was formed.

In this example this is the element ”SizeRequirement(Message)”. This element is not present in the ontology used for the first iteration. By introducing it in the second iteration's ontology it will be possible to express deviation 3.b in that analysis round.

3.4.7 Multiply Identified Deviations

The systematic approach of formulating deviations leads to the possibility of identifying deviations in differing statements. The ontology defines a common vocabulary for expressing a system and its behaviours. This offers to express the results in an precise ontological expression. An inspection of these expressions shows those deviations that are differing in words but identical in their substance. This requires that the ontology used is unambiguous and does not allow for one intend to be expressed in multiple ways.

As the formulation of the ontology is a design process it is possible to react in different ways if the ontology has to be extended to increase the expressiveness. The developer has to take care that the system ontology is formulated without ambiguities.

Those deviations translated into identical expressions only need to be investigated once in the following analysis's steps because the causal analysis of identical expressions have to lead to identical results.

In the analysis's first iteration 7 of 19 identified deviations were identified multiply. They were analysed causally only once reducing the amount of work needed for the analysis.

3.5 Causal System Analysis

The goal of the Causal System Analysis is the identification of relations between elements of the ontology or the element's behaviours leading to an unwanted event.

The Causal System Analysis is used for identifying causal factors leading to an effect. These relations than have to answer the question, if the identified causal factors are sufficient for justifying the occurrence of the effect.

3.5.1 Causal Factors

The theoretical foundations defining counterfactual relations between objects go back on Hume, who defined a cause "to be *an object, followed by another, and where all the objects similar to the first are followed by objects similar to the second.* Or in other words, *where, if the first object had not been, the second never had existed.*" [Hum99, p.146].

A formalised definition of causation was given by Lewis [Lew73, p.563]: "If c and e are two actual events such that e would not have occurred without c, then c is a cause of e."

State predicates and state changes can be expressed with events. An event is a necessary causal factor (NCF) of an effected event, if it suffices the criterion defined by Lewis [Lad01, p.110].

3.5.2 Causal Sufficiency Criterion

Identifying a number of causes of an effect does not necessarily provide a sufficient set for the justification of an effect's causation. This is achieved by defining the Causal Sufficiency Criterion that can be ascertained by using the Causal Completeness Test [Lad01, pp.219].

The Causal Completeness Test states that a set of events $A_1, ..., A_n$ are sufficient for the justification of an effect's causation if every A_i is a necessary causal factor for the effect B and the unexistence of the set $(A_1 \wedge A_2 \wedge ... \wedge A_n)$ being counterfactual to the unexistence of effect B.

3.5.3 Causal Analysis of Deviations

Using the Causal Analysis the causes of the deviations are identified by applying both methods mentioned in chapter 3.5.1 and 3.5.2. This means that for every identified factor it must be evaluated if it is a necessary causal factor for the effect and if all identified necessary causal factors are sufficient for the causation of the effect. This relations are represented in a graph called Causal Influence Diagram (CID).

Deviation 4.b *"NIC receives more input from the device than expected"* was transformed into its ontological analogue *"DataRate(NIC) > DataRate(Device)"*.

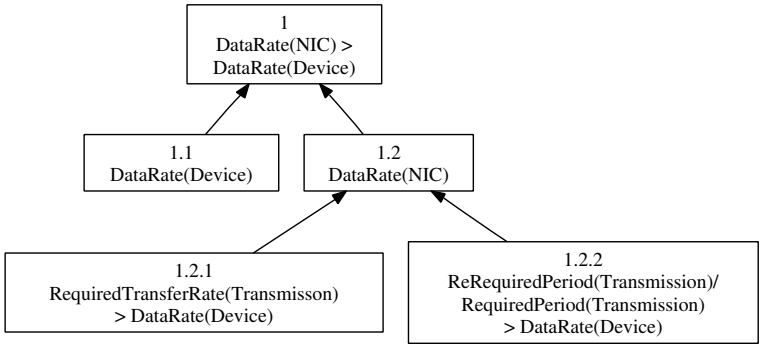


Figure 3.5: CID of deviation 04.b-1

Both DataRate(Device) and DataRate(NIC) are causal factors of this deviation. The DataRate(Device) is not further analysed as it cannot be influenced from within the communication system. The DataRate(NIC) can however be influenced. It is caused either by the definition of a RequiredTransferRate(Transmission) greater than the DataRate(Device), the RequiredSize(Transmission), or the RequiredPeriod(Transmission) being greater than the DataRate(Device).

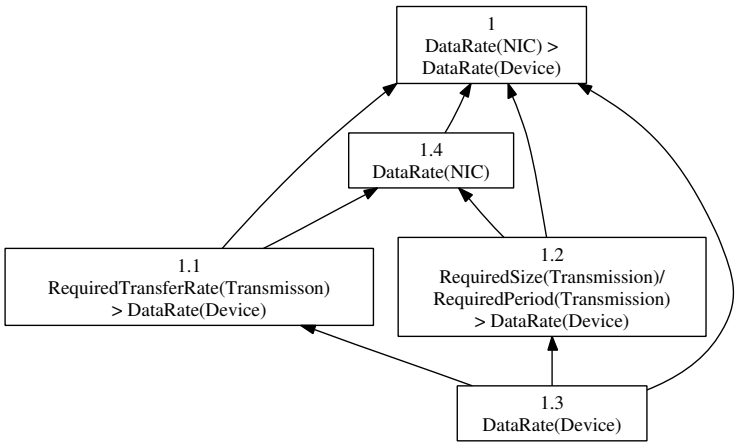


Figure 3.6: CID of deviation 04.b-2

It comes to mind, that the DataRate(Device) is a factor of both causes of the DataRate(NIC) and that both factors of DataRate(NIC) directly influence the deviation. By drawing the necessary edges it becomes obvious that the DataRate(Device) would influence the DataRate(NIC). It has to be assumed, that the ability of the NIC to transfer information is not influenced by the device's speed of information production.

After removal of edges as well as the DataRate(NIC) and the addition of the

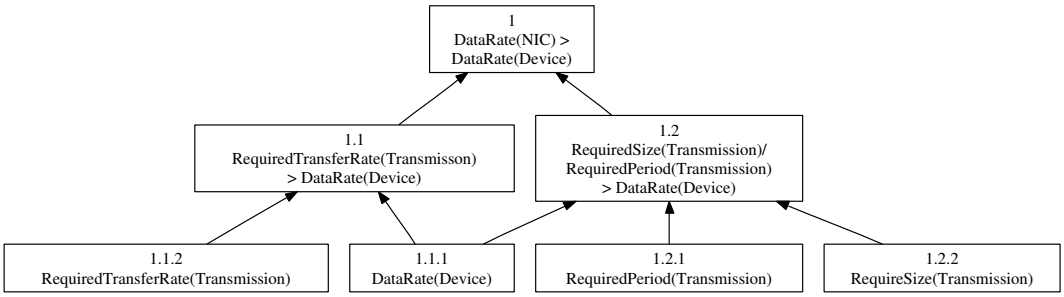


Figure 3.7: CID of deviation 04.b-4

elements used in the direct causes of the deviation, the graph depicted in Figure 3.7 results. This graph shows, that asides from the DataRate(Device) only Requirements of the Transmission can lead to this deviation.

3.5.4 Using Narrative Factor Descriptions

The use of narrative factor descriptions is very tempting as one is more used to expressing a behaviour using normal language than to expressing it in a formal way using the ontology's elements. If one keeps in mind, that in the Ontological Analysis the description of the relations between the system's elements has to be made using the ontology, a translation from narrative description to ontological description would be needed. If the complete argumentation in the CID is made by using narrative factor descriptions, the time and effort needed for the translation is increased.

As early trials by the author have shown, this approach makes it difficult to translate the nodes of the resulting CIDs into ontological expressions. The utilisation of the system ontology focuses the expression on the distinguishing elements of the system. Narrative descriptions easily deviate from these elements. This leads to a large number of elements needed to be introduced into the system if one tries to express the formed graphs using the ontology. As every new element to the ontology has to be investigated by using the attribute-guide-word combinations the complexity of the system description increases rapidly.

If narrative factor descriptions are used in the Causal System Analysis care has to be taken that only a small number of nodes are described in this way. These factors have to be effected by causes expressible in the ontology.

An application in which narrative factor descriptions proved to be useful are those cases, where it is possible to partition the events leading to a failure. As

an example the event of a NIC not receiving information can be taken. Using the knowledge that a NIC can either receive information from the network or from the device it can be said that either "No Input over Wiring" or "No Input from Device" occurred (see Figure 3.8) if "Input(NIC)=0" occurred.

After this partitioning step the problem is reduced to identifying the causes for the event that no information was received over the wiring or from the device.

This approach does not diminish the conclusions that can be drawn from the graph as the introduced narratively described factors can be eliminated from the graph. To maintain the expressiveness of the graph the edges between the nodes have to be adjusted. In the case of a factor being eliminated every factor of the eliminated node will be a direct factor for every effect the eliminated node caused.

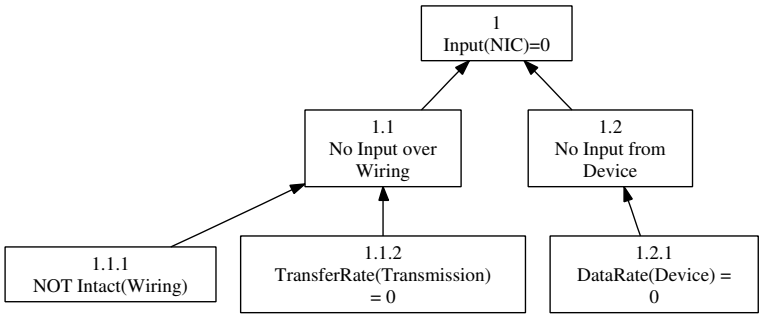


Figure 3.8: CID of deviation 04.a

For this method to be acceptable it has to be ascertained, that the systematic partitioning is done rigorously as the omission of influences would offend against the causal sufficiency criterion. Care has to be taken as it is possible that imprecise formulations complicate the identification of a set of events not meeting the criterion.

If systematic partitioning is possible, a draft can be made of the interaction between system parts. In case of the deviation "NIC does not get input" the draft shown in Figure 3.9 was made. Basing on this scheme the only inputs to the NIC are those coming from the Network or from the Device.

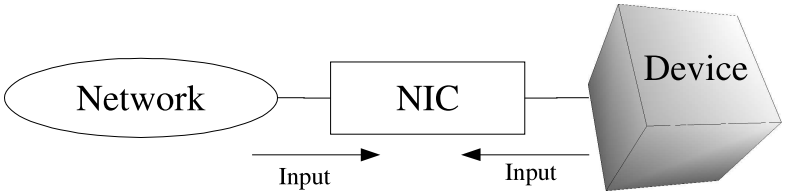


Figure 3.9: Schematic representation of input to NIC

3.5.5 Mathematical Expressions in Deviations

If expressions of deviations contain mathematical expressions every element of the equation is a necessary causal factor for the occurrence of the deviation.

An example for this is deviation 12.a "Transmission latency is bigger than intended". This deviation was expressed with "Latency(Transmission) > RequiredLatency(Transmission)".

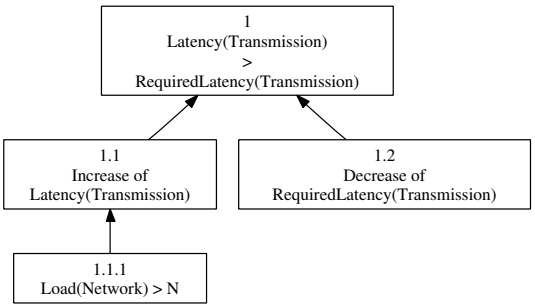


Figure 3.10: CID of deviation 12.a

As Figure 3.10 shows, the deviation can be caused by either an "Increase of Latency(Transmission)" or a "Decrease of RequiredLatency(Transmission)". This results directly out of the expression's mathematical interpretation.

3.5.6 CID's Level of Detail

Every leaf in the CID has to be either a statement in the ontology or an identified necessary addition to the ontology. The level of detail is great enough if the current leaf represents a requirement towards an elements property that can be trivially ascertained, a statement identified in another deviation and therefore analysed at another place, or a factor that is not expressible in the current ontology. If the last case occurs, an necessary addition to the ontology has been identified.

3.6 Extending the Ontology

Elements identified as required for expressing behaviour of the system need to be included in the ontology. After the initial system description is formulated and an ontology is formed out of this description, extensions of the system's ontology

result mainly out of two analysis steps: the translation of deviations to ontological expressions and the causal analysis identifying causal factors that are needed for the explanation of events but that cannot be expressed in the ontology.

The identified elements proposed for extending the ontology have to be verified against the ontology and the system's design intention. This prevents the inclusion of ambiguous elements into the ontology and deviation of the ontology's focus from the design intent.

4 Ontological Analysis: Risk Assessment

4.1 Analysis of Safety and Risk

In Ontological Analysis the iterative decomposition's result must be investigated with respect to the question if the level of risk imposed by the system is acceptable. The positive answer on this question is important for the developed system being accepted. Not only may the system be avoided or opposed by user, customer or the society but some countries like the UK or the Netherlands have introduced legislative requirements requesting the analysis of the implications posed by the safety-related systems.

Modern standards for developing and operating safety-related systems like IEC 61508 [Int97] demand that the risk of the developed system must be considered in the development process. IEC 61508 for example requires, that the risk imposed by the equipment under control (EUC) be assessed, a target level of risk, the tolerable risk be identified, and measures for risk reduction be taken such that the final level of risk imposed by the system is at least as low as the tolerable risk.

In general the analysis of safety and risk is divided into the establishment of answers to the questions:

- What is the threat I am facing?,
- How large is the risk posed by the threat?,
- What risk am I or the society willing to take?,
- What measures are used to reduce the risk? and
- What are the risks introduced by these countermeasures?.

In ontological analysis the answer to the first question is answered by the iterative decomposition that identifies the possible deviations the system is exposed to

and the interplay of factors leading to them. To answer the second question the hazard and risk posed by the system must be assessed (see chapter 4.2). The third question directly leads to the analysis of the acceptability of risk (see chapter 4.3). To answer the fourth question countermeasures guarding against an identified threat have to be developed (see chapter 4.6) and their implications identified. This identification results out of their introduction into the following iteration of the analysis, by which the last question is answered.

4.2 Assessment of Hazard and Risk

The risk imposed by the currently described system can be evaluated, if unwanted events threatening the system and the events leading to this unwanted event are identified. The method for identifying deviations discovers the events that can result in a hazardous event. As the deviations are identified by using a systematic approach only the identified deviations can move the currently described system into a hazardous state.

The hazards have to be identified by determining the effects caused from the identified deviations. For these hazards the possible impact has to be designated.

The identification of the events leading to a hazard results directly from the deviations and the causal analysis of the causal factors effecting them. The result is a graph describing the relations between events and causes, the Causal Influence Diagrams (CID).

For determining the possibility of reaching a node in a graph, the graph can be regarded as a Bayesian Belief Net (BBN) given that the graph contains no cyclic dependencies. As an algorithm for the graph's transformation into a Fault Tree exists [Lad01, chapter 10] the evaluation of the hazard's frequency by using a Fault Tree Analysis (FTA) is another possibility.

Both of these approaches demand that the formed graph does not contain loops in its structure. If loops are present either different procedures for the evaluation of the failure's frequency have to be used or the loop must be broken up and a mathematical analysis of the frequency value's expansion be used to confirm that an upper bound for the value exists. If neither of these choices is possible, the system description has to be modified to avoid the occurrence of the identified loop and enabling the assessment of the failures frequency.

The causal analysis made for the elements in the iterative decomposition did not contain any loops so that the evaluation of frequencies using either FTA or BBN

would be possible.

4.3 Analysis of Acceptability

The risk regarded as being acceptable is connected to the impact posed by a threat and the frequency of this threat to occur. Risk in engineering is usually defined as the product of the probability or frequency of an unwanted event times the impact this event would have.

$$Risk(Event) = Frequency(Event) * Consequence(Event)$$

This calculation requires that the frequency as well as the consequence of a given event is accurately determined if the level of risk imposed by an event is to be used as the indicator for making a decision.

An individual's view on these two factors is not independent from outside influences. Threats with high frequency are estimated to have lower frequencies and vice versa (see chapter 4.3.1) and threats with high impact but low frequency are over proportionally avoided (see chapter 4.3.2). Prospect Theory, developed by Kahneman and Tversky (see chapter 4.3.3) can be used to explain for deviations between the risk objectively present and the risk perceived by an individual.

As the risk regarded as being tolerable is difficult to calculate objectively, societies have developed different approaches to conclude if risk can be regarded as being acceptable or not. Some of these approaches are required by legislation like ALARP or EVR, others like GAMAB, MGS or MEM provide requirements for allowing a concession to operate the system to be issued.

4.3.1 Risk Perception

The perceived frequency of events differs from the frequency that can be estimated statistically as numerous psychological studies have shown. Two examples of these are the study by Lichtenstein et al. [LSF+78] and Combs and Slovic [CS79].

Lichtenstein et al. asked a group of subjects to estimate the annual death toll from 41 causes after giving the actual death toll of motor vehicle accidents. The results are shown in Figure 4.1.

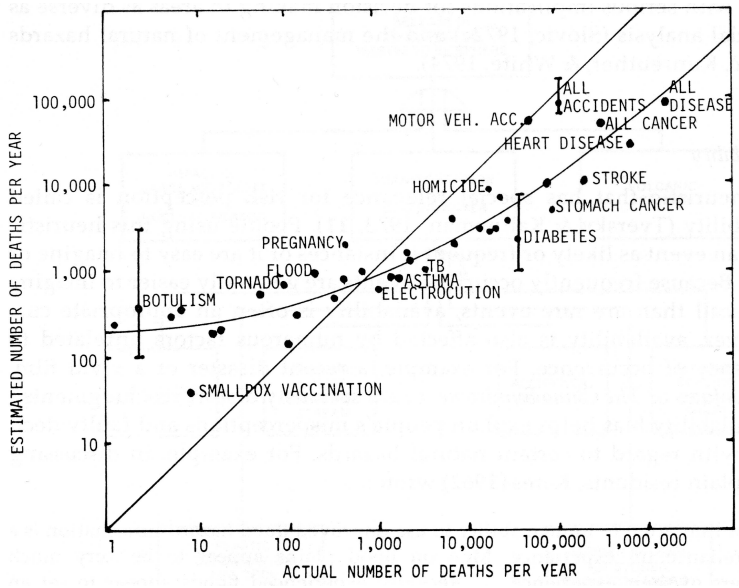


Figure 4.1: Relationship between judged frequency and the actual number of deaths of 41 causes (as in [SFL82]).

It can be observed, that the subjects overestimated the frequency of causes with low probability and underestimated the frequency of causes with high probability. An explanation to this misjudgements can be given by the availability of a cause of death. If an individual can easily think of an instance where the cause had occurred, the perceived frequency of the cause is increased. All the same the perceived frequency is reduced for causes hard to remember.

The role newspapers play in regard of the availability was studied by Combs and Slovic who investigated the subjects in newspapers. This study showed that events with catastrophic or large scale impact were reported more frequently than less dramatic events with similar frequency.

It can be assumed, that the influence of modern public-media in regard of the availability is comparable to the influence of newspapers.

4.3.2 Risk Aversion

Another aspect of the availability lies in the risk aversion people have. Risk aversion is the behaviour of a person in which the certain prospect of a choice is preferred over an uncertain prospect with the same expected value [KT79].

As the perceived frequency of an event can be exaggerated it is possible that the

PROBLEM 1: Choose between

A:	2,500 with probability	.33,	B:	2,400 with certainty.
	2,400 with probability	.66,		
	0 with probability	.01;		
$N = 72$	[18]			[82]*

PROBLEM 2: Choose between

C:	2,500 with probability	.33,	D:	2,400 with probability	.34,
	0 with probability	.67;		0 with probability	.66.
$N = 72$	[83]*			[17]	

Figure 4.2: Two choices demonstrating risk aversion and risk seeking (as in [KT79]).

risk aversion present in a person becomes irrationally high.

This behaviour is part of the certainty effect described by Kahneman and Tversky [KT79]. This effect is based on the observation that the same batch of subjects tended to prefer certain prospects over uncertain ones while preferring uncertain high prospects over prospects slightly more certain but with slightly lower possible gain as described by Allais [All53].

4.3.3 Prospect Theory

Kahneman and Tversky [KT79] formulated this theory as an alternative to the Expected Utility Theory (EUT) made by von Neumann and Morgenstern [vNM53], which predicts that a person will make his choice between uncertain prospects on the grounds of the expectation, rules on the integration of assets, and the risk aversion of the decision maker.

They noted that some observable effects contradict the EUT's predictions. These effects are the "certainty effect", the "reflection effect", and the "isolation effect".

The *certainty effect* describes the tendency of people to "overweight outcomes that are considered certain, relative to outcomes which are merely probable". This effect was shown in studies with questions like the two shown in Figure 4.2. In problem 1 the interviewees had to choose between a certain win of 2400 or a probable win with the possibility of 0.01 to win nothing. 82 percent of the interviewees chose the certain win over the less certain win. Problem 2 confronted

PREFERENCES BETWEEN POSITIVE AND NEGATIVE PROSPECTS

Positive prospects				Negative prospects			
Problem 3:	(4,000, .80)	<	(3,000).	Problem 3′:	(−4,000, .80)	>	(−3,000).
$N = 95$	[20]		[80]*	$N = 95$	[92]*		[8]
Problem 4:	(4,000, .20)	>	(3,000, .25).	Problem 4′:	(−4,000, .20)	<	(−3,000, .25).
$N = 95$	[65]*		[35]	$N = 95$	[42]		[58]
Problem 7:	(3,000, .90)	>	(6,000, .45).	Problem 7′:	(−3,000, .90)	<	(−6,000, .45).
$N = 66$	[86]*		[14]	$N = 66$	[8]		[92]*
Problem 8:	(3,000, .002)	<	(6,000, .001).	Problem 8′:	(−3,000, .002)	>	(−6,000, .001).
$N = 66$	[27]		[73]*	$N = 66$	[70]*		[30]

Figure 4.3: Preferences demonstrating the reflection effect (as in [KT79]).

the interviewees with two probable win situations. 83 percent chose the slightly less probable win of a higher amount over the offered alternative.

The *reflection effect* describes the tendency of subjects to choose the opposite prospect if the prospects are possible losses than they would choose if the prospects were possible gain (Figure 4.3). The interviewees had to choose between alternate prospects. These prospects were formulated as a possible win and as a possible loss. In every case the preferred prospect offered as a possible win was unfavoured when offered as a possible loss.

The *isolation effect* is based on the attempt of people to simplify the choice they have to make by disregarding components that all offered alternatives have in common and making the choice by focusing on the alternatives' distinguishing components. As it is possible that no uniform method for differentiation between common and distinguishing components exist this can result in inconsistent preferences of the decision maker. This can be demonstrated by comparing two gambling examples both resulting in the same prospects (Figure 4.4).

Prospect Theory, originally developed to describe decision preferences in a lottery, is designed to amount for the effects of certainty, reflection and isolation. It is divided into two stages: the phase of editing and the phase of evaluation. In the editing phase the prospects are analysed, a reference point for the evaluation is set, and a number of defined operations applied leading to a simplified description of the prospects. In the second phase the prospects are evaluated and the prospect with the highest value is chosen. This choice is made by using two scales, the decision weight $\pi(p)$ reflecting the impact of the probability p on the prospect's over-all value and $v(x)$ reflecting the outcomes subjective value.

Figure 4.5 shows a possible value function for the prospect theory. This function is formed on deviations from the reference point. Its ascent is steeper in the loss domain than in the gain domain and it is concave in the gain domain contrasted

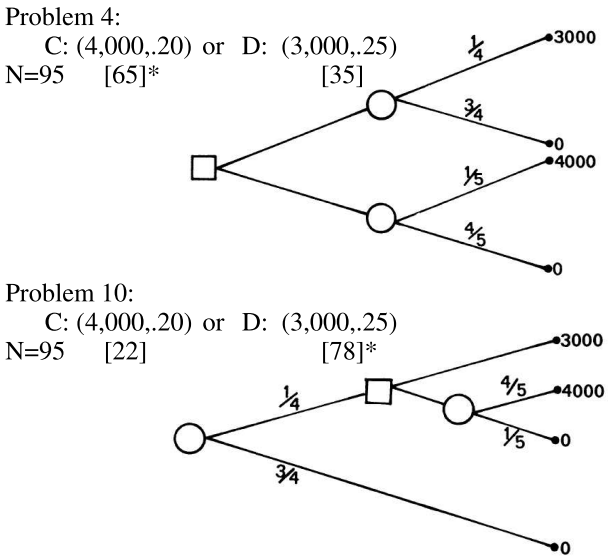


Figure 4.4: Two decision trees demonstrating the isolation effect (as in [KT79]).

by its convex form in the loss domain.

4.3.4 Coping with Risk

Stoll [Sto78] [Sto80] states, that the way people cope with risks differs from the frequency these risks have. He says, that very small risks in the region of 1 fatality per year out of 100 million people like the risk of being hit by a meteor are not consciously perceived. Risks in the region of 1 fatality per year out of 1 million people like being stroked by lightning are more suppressed than reduced by sayings. Risks in the region of 1 fatality per year out of 10.000 people will be well known by a very large percentage of the population. The people require organised protection by the government in the form of police, fire brigade etc. Risks in the region of 1 fatality per year out of 100 people e.g. initiated by a disease or plague are tried to cope with by using precaution or repression. Other irrational behaviour is possible.

Although the results of [LSF+78] in Figure 4.1 show that the perceived frequency for risks with very low frequency is exaggerated and considering the people's estimation of risks influenceable by availability, it can be noted, that regulations mainly concern risks with either high frequency or a high impact.

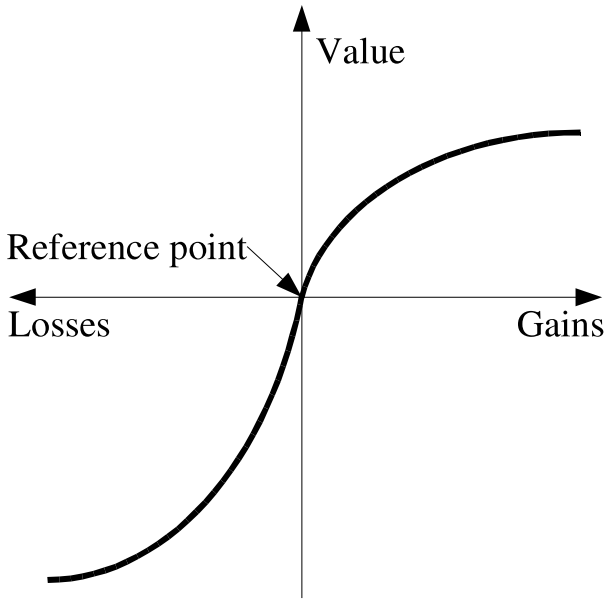


Figure 4.5: A hypothetical value function (after [KT79]).

4.4 Tolerability Norms

4.4.1 ALARP Principle

ALARP stands for "As Low As Reasonably Possible". This principle demands, that the risk induced by a technical system should be weighted against the cost implied by a reduction of this risk. The demand of comparing technical systems with current possibilities is established in the British judiciary system.

Bouder describes that the term "Best Practice" was introduced within the 1842 factory laws [Bou04]. A key case was Edwards v. The National Coal Board [Cou49] in 1949. Lord Justice Asquith decided, that:
"'Reasonably practicable' is a narrower term than 'physically possible' and seems to me to imply that a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them - the risk being insignificant in relation to the sacrifice - the defendants discharge the onus upon them. Moreover this computation falls to be made at a point in time anterior to the accident. The questions he has to answer are, firstly, what are the measures necessary and sufficient to prevent any breach of the Statute Law, and secondly, are these measures reasonably practicable."

In 1970 the Committee on Health and Safety at Work was constituted under the helm of Lord Robens to "review and make recommendations on the safety and health both of persons in the course of their employment and of the public in connection with activities on industrial, commercial or construction sites" [Nat]. The 1972 report of the Robens Committee led to the 1974 Health and Safety at Work, etc Act [HSA74], that required tasks to be safe "So Far As Is Reasonably Practicable" (SFAIR). This phrase is used in many place of the Act. One of them, Section 1, states that *"(1) It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees."*

The SFAIR concept led to ALARP, which is amongst others a fundamental requirement for nuclear facilities in the United Kingdom. Following the Sizewell B inquiry, Inspector Sir Layfield recommended that HSE should publish its thinking on risk assessment for discussion [Hea01]. This recommendation resulted in the paper "The Tolerability of Risk from Nuclear Power Stations" [Hea92] the origin of the TOR framework.

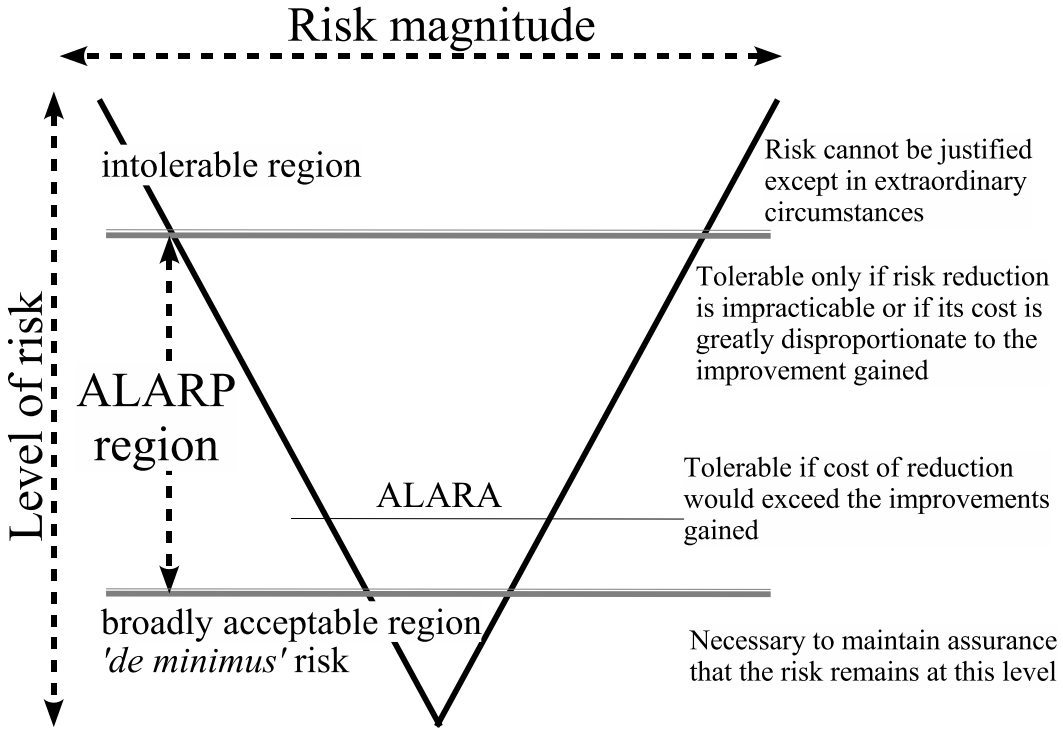


Figure 4.6: Tolerability-of-Risk Triangle

The Tolerability-of-Risk triangle represented in figure 4.6 was drawn after [Dep02]. The increasing level of risk is related to an increasing risk magnitude which is represented by a triangle. This triangle is divided by two broad limits. A level of risk lying beneath the lower limit is so small that it can be broadly

accepted. A level of risk lying above the upper limit is so high that it will only be accepted in extraordinary circumstances. Between these two limits is the ALARP region, where it has to be decided, if the cost of a reduction in risk can be justified by the resulting benefit. This cost-benefit calculation leads to a level of risk that is ALARA - As Low As Reasonably Achievable.

4.4.2 EVR

In the Netherlands production facilities working with hazardous substances are required to prepare an external safety report, the 'Externe Veiligheid Rapport' (EVR) (cited after [BC04]) every five years. This report comprises a quantitative risk analysis during which the possible failures, their impact and probability as well as the risk of the facility have to be determined. In contrast to the British ALARP principle the Dutch EVR does not refer to the risk an employee is exposed to, but the risk residents and community are exposed to. Two critical values are set, one applying to the individual risk, the other applying to the group risk.

The individual risk is the probability of any person outside the facility to die. This risk must not exceed the probability of 10^{-6} in a year.

The group risk requires the risk for a group of people always to be below 10^{-3-2n} for a failure with 10^n fatalities.

4.4.3 MGS

"*Mindestens Gleiche Sicherheit*" is used in German regulations to allow for the deviation of typically required procedures. The EBO for example demands in §2 Allgemeine Anforderungen: [Bun67]

"(1) Bahnanlagen und Fahrzeuge müssen so beschaffen sein, daß sie den Anforderungen der Sicherheit und Ordnung genügen. Diese Anforderungen gelten als erfüllt, wenn die Bahnanlagen und Fahrzeuge den Vorschriften dieser Verordnung und, soweit diese keine ausdrücklichen Vorschriften enthält, anerkannten Regeln der Technik entsprechen.

(2) Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist."

This allows for techniques that deviate from the generally recognised codes of practice if the technique ascertains a safety level that is at least equal with the

safety level provided by the generally recognised codes of practice.

4.4.4 GAMAB

"*Globalement Au Moins Aussi Bon*" is the french demand towards the level of risk a new transportation system has to fall below. It can be formulated as "All new guided transport system must offer a level of risk globally at least as good as the one offered by any equivalent existing system." [CZKL01].

This principle considers the global level of risk induced by a system and exceeds the demand made by MGS by demanding that the risk must be lower than any equivalent existing system rather than the level of risk achieved by the generally recognised codes of practice.

By considering the globally induced risk, the GAMAB principle allows the manufacturer to distribute the risk induced between subsystems as long as the globally required level of risk is achieved.

4.4.5 MEM

If looked at the mortality table (Fig. 4.7) for Germany based on 2001/2003's statistic, one recognises a minimal probability of females and males between the age of 7 and 10 which lies at about $2 * 10^{-4} \frac{Deaths}{Person*Year}$.

The concept of MEM, the Minimum Endogenous Mortality, was introduced by Albert Kuhlmann [Kuh81]. While the mortality table displays the total probability of dying for people of a given age, Kuhlmann suggests that the "natural" probability of dying can be taken as a limiting value. Under "natural" probability the probability under the exclusion external influences such as accidents or inherent deformities is understood.

It is noted [Kuh81, Risiko-Akzeptanz], that for children between 5 and 15 years the value of the MEM is with $2 * 10^{-4} \frac{Deaths}{Person*Year}$ at the lowest point. This minimum can be observed amongst all western countries. In combination with the assumption that an additional risk in the size of the MEM will be acceptable by people, this value can be used as an absolute lower limit the risk of death induced by technical devices may present.

MEM argues that a person can be exposed to 20 technical systems at once. The tolerable individual risk therefore is $1 * 10^{-5} \frac{Deaths}{Person*Year}$.

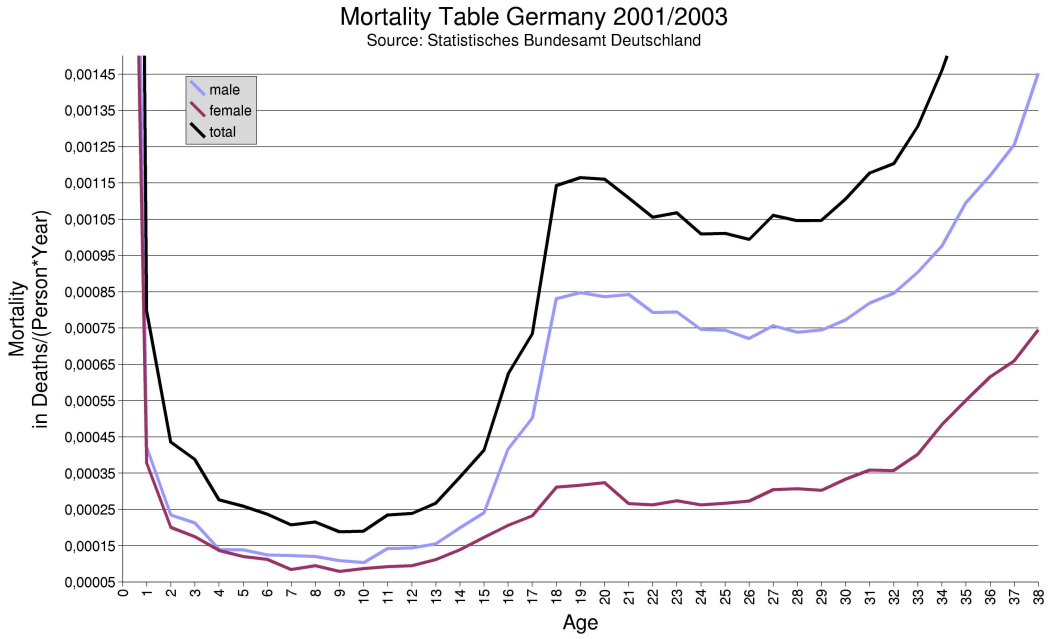


Figure 4.7: Mortality Table for Germany 2001/2003

Taking into account the aversion towards risks with disastrous results, beginning with a risk of 100 fatalities the tolerable individual risk becomes smaller as depicted in Figure 4.8. This reduction is introduced because of the observation that risk-aversion is increased by large scale events with catastrophic impact. Under the assumption that risk-aversion increases with the number of fatalities the acceptable level of risk becomes lower with the possible impact of a failure.

In situations, where the user is exposed to less than 20 technical systems, it may be permissible to modify the value identified for the maximal tolerable individual risk by arguing on the number of technical systems the user is exposed to [Bra05]. For example if a person travels by train one can argue that for the time travelling he is only exposed to one technical system. The standard value for the maximal tolerable individual risk for such an accident identified by MEM would be $1 * 10^{-6} \frac{Deaths}{Person * Year}$ if one estimates that an accident could lead to casualties in the range of $1 * 10^{2} to 1 * 10^{3}$. Using the assumption that the passenger is only exposed to one technical system while driving with the train, the maximal tolerable individual risk for such an accident would be about $2 * 10^{-5} \frac{Deaths}{Person * Year}$.

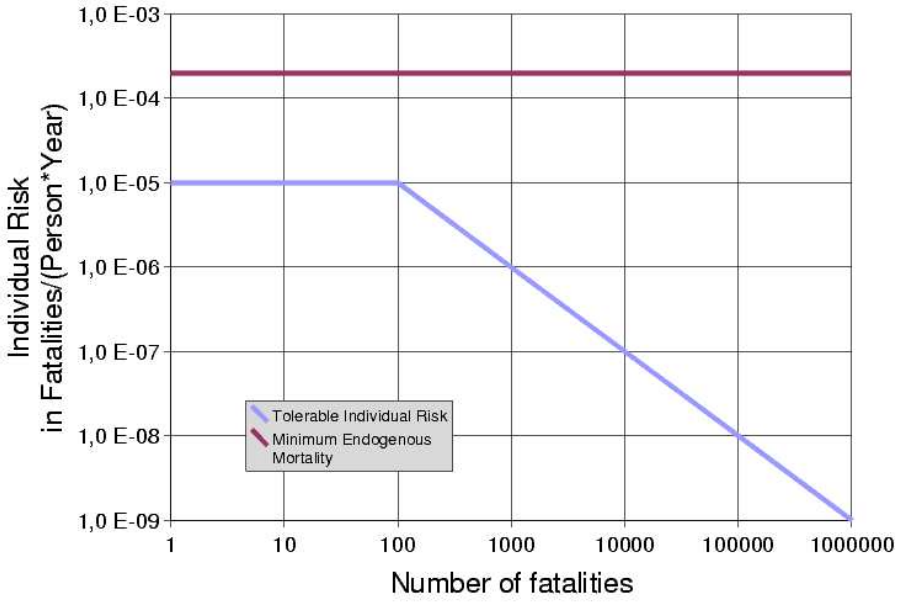


Figure 4.8: Tolerable individual risk in MEM

4.5 Safety Requirements and Specification

The safety requirements must specify the claims towards failure rate and failure impact any part of the system must meet. These requirements consist of facilities for risk reduction and the reduction in risk they have to effect. IEC 61508 requires overall safety requirements to be specified. This demands that safety requirements for every safety function guarding against a hazardous event have to be specified "in terms of the safety functions requirements and safety integrity requirements" [Int97, part 1, chapter 7.5].

The specification of these requirements is done by identification of possible failures and assessment of the EUC's risk of failing in the identified way. For the assessment of necessary risk reduction the failure's tolerable risk must be identified. The necessary risk reduction then results from the comparison between EUC risk and tolerable risk. If the necessity for risk reduction is established, facilities have to be developed to provide this increase in safety.

4.6 Countermeasures

Countermeasures are facilities for the reduction of risk. In Ontological Analysis they have to be introduced in the system if an assumption cannot be assured or if the risk of a deviation is not acceptable.

These countermeasures are additions to the system and prevent or at least mitigate the possibility of the system to reach a hazardous state. This can be realised either by directly influencing the behaviour and properties of the system's elements or by passively preventing elements of the system to enter a hazardous state.

At least the countermeasures actively interacting with the system to prevent a deviation to occur pose the threat of introducing new deviations into the system through their interaction. Countermeasures have to be introduced into the system description and their possible implications be analysed. It may be the case that a countermeasure is not advisable due to its implications to the system. In this case the system design has to balance possible countermeasures against each other and identify the solution with least implicated additional risk.

5 Iterative Decomposition: Running Example

5.1 1^{st} Iteration

The findings of the analysis's first iteration were already used as examples in chapter 3. The resulting tables are therefore not again displayed in this part but are referred to.

By using the initial system description (see chapter 3.2.2) an ontology for the system is developed (see chapter 3.3.4). All elements of the ontology are investigated by using the HAZOP method for deviation identification. The formed attribute-guide-word combinations are listed in appendix A.1.

Combinations that are identified as possible deviations lead to a list shown in Table 3.9.

The assumptions made during the identification of deviations in the first iteration are shown in Table 3.8. These assumptions have to be guaranteed. If this is not possible, the corresponding attribute-guide-word combinations have to be investigated and the ontology extended, until the deviation can be expressed properly.

For the Causal System Analysis the identified deviation has to be described by using the ontology's elements. It is likely that in early iterations a deviation cannot be described by the ontology used. If a deviation is not expressible the ontology has to be extended. The newly introduced elements will be gathered and analysed in the next analysis iteration. Using the ontology available in the first iteration the deviations shown in Table 3.10 are expressible using the ontology.

5.1.1 Extensions to the Ontology

For deviations not expressible with the ontology currently used the questions "What elements of the ontology would be needed for the expression of this deviation?" and "What would the expression be?" are asked. This leads to missing elements and expressions of the deviation that could be used in later iterations.

Deviation 4.b (*NIC receives more input from the device than expected*) cannot be expressed with the first iteration's ontology as the combination 'more input' would require the element 'Device' to be part of the ontology. For the comparison of input the elements 'DataRate(NIC)' and 'DataRate(Device)' are needed. The entry in the ontological expression table is therefore:

	Ontological expression
4.b	*needed: DataRate(Device), Device, DataRate(NIC)*

The possible expression 'DataRate(Device)*time > DataRate(NIC)*time' for deviation 4.b is noted for later use.

As only 19 of 59 deviations are expressible in the first iteration it is decided to include the identified extensions into the ontology before beginning with the causal analysis of the expressions.

The elements identified to be missing are:

	Type	Element
01	Object	Network
02	Property	DesignNodeCount(Network)
03	Property	NodeCount(Network)
04	Object	Universe
05	Relation	Interference(Network, Universe)
06	Object	Device
07	Property	DataRate(Device)
08	Property	DataRate(NIC)
09	Property	Length(Wiring)
10	Property	Requirements(Wiring)
11	Property	Content(Transmission)
12	Property	Format(Transmission)
13	Property	RequiredJitter(Transmission)
14	Property	RequiredLatency(Transmission)
15	Property	RequiredMode(Transmission)
16	Property	RequiredPeriod(Transmission)
17	Property	RequiredSequence(Transmission)

	Type	Element
18	Property	RequiredSize(Transmission)
19	Property	RequiredTimeReceived(Transmission)
20	Property	RequiredTimeSent(Transmission)
21	Property	RequiredTransferRate(Transmission)
22	Property	Sequence(Transmission)
23	Property	SizeRequirement(Transmission)
24	Property	TimeReceived(Transmission)
25	Property	TimeSent(Transmission)
26	Property	TransferRate(Transmission)

5.2 2^{nd} Iteration

5.2.1 System Ontology

The second iteration's ontology is expanded by the elements identified to be necessary for the description of some deviations identified in the first iteration. The second iteration's ontology therefore has the form:

5.2.1.1 Objects

Object	Description
NIC	The Network Interface Controller. It is the interface between the input device and the physical network.
Wiring	The physical connection between the systems' NICs.
Transmission	The transport of information between NICs over the physical network.
Network	The system consisting of Wiring and NICs that exists to provide means for devices to communicate.
Universe	The unity of all objects that are part of the system, the environment and the world.
Device	The facility that uses the network to communicate with other facilities.

5.2.1.2 Properties

Object:	**NIC**
Property	Description
Input	The information received by the NIC
Output	The information transmitted by the NIC

Property	Description
Intact	The integrity of the NIC, whose absence prevents the NIC from working properly.
DataRate	The speed that is formed by the volume of information the NIC can transmit in a given time unit.

Object:	**Wiring**
Property	Description
Intact	The integrity of the Wiring, whose absence prevents the physical network from working properly.
Length	The distance a transmission has to cover for reaching every NIC connected to the Wiring once.
Requirements	The unity of all requirements the Wiring has to fulfil.

Object:	**Transmission**
Property	Description
Size	The size of the Transmission
Deadline	The latest possible point in time at which the Transmission can be received without loosing its value.
Period	Frequency of the generation of a type of Transmission
Mode	The mode used for the Transmission. This can be either time-triggered or event-triggered.
Latency	The time it takes for the complete transmission of information over the network.
Jitter	The variance in the transmission time of a multitude of same-typed transmissions.
Content	The payload transfered with the Transmission.
Format	The layout of information the Transmission is structured by.
Sequence	The sequence in which the transmission succeed each other.
TimeSent	The point in time the Transmission is completely relayed from the NIC to the Wiring.
TimeReceived	The point in time the Transmission is completely relayed from the Wiring to the NIC.
TransferRate	The speed that is formed by the volume of information the Wiring can transmit in a given time unit between any two NICs.
RequiredJitter	The value given in the requirements of the communication for the maximal value that is acceptable for the Jitter of the Transmission.
RequiredLatency	The value given in the requirements of the communication for the maximal value that is acceptable for the Latency of the Transmission.
RequiredMode	The Mode given in the requirements of the communication the Transmission has to be transfered by.
RequiredPeriod	The value for the Period given in the requirements of the communication the Transmission is suspected to have.
RequiredSequence	The point in succession given in the requirements of the communication the Transmission has to follow.

Property	Description
RequiredSize	The value given in the requirements of the communication for the maximal value that is acceptable for the Size of the Transmission.
RequiredTimeSent	The value derived from the requirements of the communication for the maximal value that is acceptable for the TimeSent of the Transmission.
RequiredTimeReceived	The value derived from the requirements of the communication for the maximal value that is acceptable for the TimeReceived of the Transmission.
RequiredTransferRate	The value given in the requirements of the communication for the TransferRate of the Transmission.

Object:	**Network**
Property	Description
NodeCount	The number of nodes connected to the Wiring.
DesignNodeCount	The number of nodes used for the design and the formulation of requirements.

Object:	**Device**
Property	Description
DataRate	The speed that is formed by the volume of information the Device can process in a given time unit.

5.2.1.3 Relations

Relation	Description
Connection(Wiring, NIC)	The feature of the NIC to be connected properly with the Wiring.
Interference(Network, Universe)	The feature of the Universe to influence the function of the Wiring.

5.2.2 Deviations Identified by HAZOP

The new elements added to the ontology in the second iteration are analysed with regard to deviations by using the HAZOP technique. The resulting attribute-guide-word combinations are listed in appendix A.2.

The following deviations for the new elements are identified by the interpretation:

Table 5.10: List of deviations identified in 2^{nd} iteration

	Deviation
15.a	The network is vaster than intended
15.b	The network is smaller than intended
15.c	Only part of the network exists
15.d	The network works faster than intended
15.e	The network works slower than intended
16.a	The Device does not exist
16.b	There are more devices than intended
16.c	There are less devices than intended
16.d	The device only exists in part
16.e	The device works faster than expected
17.a	The length of the Wiring is greater than expected
17.b	The length of the Wiring is smaller than expected
17.c	Only part of the length of the Wiring is achieved
18.a	Less requirements of the Wiring than needed were defined
19.a	The Transmission carries no content
19.b	The Transmission carries more content than expected
19.c	The Transmission carries less content than expected
19.d	The content is only transmitted in part
19.e	The content of the Transmission is inverted
19.f	The content is transmitted early
19.g	The content is transmitted late
19.h	The content is transmitted early in sequence
19.i	The content is transmitted late in sequence
19.j	The content is transmitted faster than expected
19.k	The content is transmitted slower than expected
20.a	The format is too restricted for fulfilling the needs of the communication
20.b	The format is only achieved in part
20.c	The format is reversed
21.a	The sequence is to restricted for fulfilling the needs of the communication
21.b	The sequence of transmission is only partially achieved
21.c	The sequence of transmission is reversed
21.d	The sequence does not provide enough room for transmission
22.a	The transmission is not sent
22.b	The time of sending is greater than expected
22.c	The time of sending is smaller than expected
22.d	The transmission is sent early
22.e	The transmission is sent late
22.f	The transmission is sent early in sequence
22.g	The transmission is sent late in sequence
23.a	The transmission is not received
23.b	The time of receiving is greater than expected
23.c	The time of receiving is smaller than expected
23.d	The transmission is received early
23.e	The transmission is received late
23.f	The transmission is received early in sequence
23.g	The transmission is received late in sequence
24.a	The transfer rate is greater than expected
24.b	The transfer rate is smaller than expected

	Deviation
24.c	The transfer rate is only partially achieved
24.d	The transfer rate is faster than expected
24.e	The transfer rate is slower than expected
25.a	Value required for jitter greater than needed
25.b	Value required for jitter only partially achieved
26.a	Value required for latency is greater than needed
26.b	Value required for latency is only partially achieved
27.a	Required mode of transmission is greater than needed
27.b	Required mode of transmission is smaller than needed
27.c	The mode requirement of transmission is reversed
28.a	Required frequency of transmission is smaller than needed
28.b	The period requirement of transmission is only partially achieved
28.c	Period requirement of transmission is slower than in reality
29.a	Required sequence of transmission is less elaborated than needed
29.b	Sequence requirement is reversed
30.a	The required size of the Transmission too small
31.a	No maximal acceptable value of TimeSent(Transm.) can be derived
31.b	The maximal acceptable value of TimeSent(Transmission) is too large
31.c	The maximal acceptable value of TimeSent(Transmission) is too small
32.a	No maximal acceptable value of TimeReceived(Transm.) can be derived
32.b	The maximal acceptable value of TimeReceived(Transm.) is too large
32.c	The maximal acceptable value of TimeReceived(Transm.) is too small
33.a	The value acceptable for the TransferRate(Transmission) is too large
33.b	The value acceptable for the TransferRate(Transmission) is too small
33.c	The value acceptable for the TransferRate(Transmission) is too fast
33.d	The value acceptable for the TransferRate(Transmission) is too slow
34.a	No nodes connected to the Wiring
34.b	The count of nodes is too large
34.c	The count of nodes is too small
35.a	Network design does not specify count of nodes in network
35.b	The count of nodes used in network design is too large
35.c	The count of nodes used in network design is too small
35.d	The count of nodes used in network design is only partially achieved
36.a	The device does not produce data
36.b	The data rate of the device is too great
36.c	The data rate of the device is too small
36.d	The data rate of the device is only partially achieved
36.e	The data rate of the device is too fast
36.f	The data rate of the device is too slow
37.a	The interference between Universe and Network is bigger than expected
37.b	The interference between Universe and Network is reversed

5.2.3 Assumptions Used in the Identification

In addition to the assumptions already made for the first iteration the following assumptions are made in the interpretation of the HAZOP sentences of the second iteration.

Table 5.11: List of assumptions made in deviation identification (2^{nd} iteration)

	Assumption
Ass06	More than one property of the NIC will be present.
Ass07	The DataRate(NIC) can be measured instantaneously.
Ass08	The Wiring will exist.
Ass09	The computation of the Length(Wiring) will be correct.
Ass10	The Length(Wiring) can be measured instantaneously.
Ass11	Requirements for the Wiring will be defined.
Ass12	Any two Requirements(Wiring) do not contradict or interfere with each other.
Ass13	Errors in Requirements(Wiring) will be identified and corrected.
Ass14	Attributes of the Transmission will not interfere with the Format(Transmission).
Ass15	A Format(Transmission) will be defined.
Ass16	Attributes of the Transmission will not interfere with the Sequence(Transmission).
Ass17	A Sequence(Transmission) will be defined.
Ass18	The measurement of TimeSent(Transmission) is done without systematic error.
Ass19	The TimeSent(Transmission) is measured instantaneously.
Ass20	The measurement of TimeReceived(Transmission) is done without systematic error.
Ass21	The TimeReceived(Transmission) is measured instantaneously.
Ass22	The measurement of TransferRate(Transmission) is done without systematic error.
Ass23	The TransferRate(Transmission) is measured instantaneously.
Ass24	A value for RequiredJitter(Transmission) will be defined.
Ass25	Any two requirements of the Transmission do not contradict each other.
Ass26	A value for RequiredMode(Transmission) will be defined.
Ass27	A value for RequiredPeriod(Transmission) will be defined.
Ass28	Errors in requirements of the Transmission will be identified and corrected.
Ass29	A RequiredSequence(Transmission) will be defined for time-triggered messages.
Ass30	A value for RequiredSize(Transmission) will be defined.
Ass31	A value for RequiredTransferRate(Transmission) will be defined.
Ass32	The computation of NodeCount(Network) is done without systematic error.
Ass33	The computation of NodeCount(Network) is done instantaneously.
Ass34	A DataRate(Device) can be computed if data is produced by the device.
Ass35	The DataRate(Device) is computed instantaneously.

5.2.4 Ontological Expressions of Deviations

All deviations from the first iteration that could not be expressed are expressed using the extended ontology of the second iteration. Likewise all in the second iteration newly identified deviations are attempted to be expressed in the currently available ontology.

The resulting expressions are shown in Table 5.12.

The ontology was extended after the first iteration so that all deviations identified in the first iteration are expressible with the ontology available in the second iteration. This result is due to the formulation of possible expressions for deviations made in the first iteration but for which necessary elements of the ontology are missing (see chapter 3.4.6).

After the second iteration's identification of deviations altogether 146 deviations were identified by the first two analysis iterations. 123 of these 146 deviation were expressible using the ontology of the second iteration.

Table 5.12: List of expressions possible in 2^{nd} iteration

	Ontological Expression
1.a	NodeCount(Network) > DesignNodeCount(Network)
1.b	NodeCount(Network) < DesignNodeCount(Network)
1.c	Intact(NIC) = False
2.a	Length(Wiring) > RequiredDeadline(Transmission) $*2.0 * 10^8 \frac{m}{s}$
2.b	$\{\exists(NIC\ i)\|(Connection(Wiring, i) = FALSE)\}$
2.c	Wiring a $\wedge$ Wiring b
2.d	*needed: Design(Wiring)*
3.a	Size(Transmission) = 0
3.b	Size(Transmission) > RequiredSize(Transmission)
3.c	Size(Transmission) < RequiredSize(Transmission)
3.d	(Transmission A) $\wedge$ (Transmission B)
3.e	Output(NIC Sender) > Input(NIC Receiver)
3.f	Format(Transmission A) = correct $\wedge$ Content(Transmission A) = incorrect
3.g	Output(NIC) = INVERSE(Input(NIC))
3.h	TimeSent(Transmission) < RequiredTimeSent(Transmission)
3.i	TimeReceived(Transmission) < RequiredTimeReceived(Transmission)
3.j	TimeSent(Transmission) > RequiredTimeSent(Transmission)
3.k	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
3.l	Sequence(Transmission) < RequiredSequence(Transmission)
3.m	Sequence(Transmission) > RequiredSequence(Transmission)
3.n	TransferRate(Transmission) > RequiredTransferRate(Transmission)
3.o	TransferRate(Transmission) < RequiredTransferRate(Transmission)
4.a	Input(NIC) = 0
4.b	DataRate(Device)*time > DataRate(NIC)*time
4.c	DataRate(NIC)*time > DataRate(Device)*time
4.d	NodeCount(Network) > DesignNodeCount(Network)
4.e	Output(NIC) = INVERSE(Input(NIC))
4.f	TimeReceived(Transmission) < RequiredTimeReceived(Transmission)
4.g	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
5.a	Output(NIC) = 0
5.b	Size(Transmission) > RequiredSize(Transmission)
5.c	Input(NIC)/time > DataRate(Device)*time
5.d	Input(NIC) > Output(NIC)
5.e	Output(NIC) = INVERSE(Input(NIC))
5.f	Output(NIC) != Transmission
5.g	TimeSent(Transmission) < RequiredTimeSent(Transmission)
5.h	TimeSent(Transmission) > RequiredTimeSent(Transmission)

	Ontological Expression
6.a	Intact(NIC) = False
7.a	Intact(Wiring) = False
8.a	Size(Transmission) = 0
8.b	Input(NIC) > Output(NIC)
8.c	Input(NIC) < Output(NIC)
8.d	Transmission A $\wedge$ Transmission B
8.e	Transmission A $\wedge$ Transmission B
8.f	Input(NIC) > Output(NIC)
9.a	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
9.b	$\frac{Size(Transmission)}{TransferRate(Transmission)} > Deadline(Transmission)$
10.a	Period(Transmission) > RequiredPeriod(Transmission)
10.b	Period(Transmission) < RequiredPeriod(Transmission)
11.a	Size(Transmission) = 0
11.b	Mode(Transmission) = INVERSE(RequiredMode(Transmission))
11.c	Mode(Transmission) = INVERSE(RequiredMode(Transmission))
12.a	Latency(Transmission) > RequiredLatency(Transmission)
12.b	RequiredLatency(Transmission) > N
13.a	Jitter(Transmission) > RequiredJitter(Transmission)
14.a	Connection(Wiring, NIC) = False
14.b	Connection(Wiring, NIC) $\wedge$ Connection(Wiring, NIC)
15.a	NodeCount(Network) > DesignNodeCount(Network)
15.b	NodeCount(Network) < DesignNodeCount(Network)
15.c	NodeCount(Network) < DesignNodeCount(Network)
15.d	TransferRate(Transmission) > RequiredTransferRate(Transmission)
15.e	TransferRate(Transmission) > RequiredTransferRate(Transmission)
16.a	$\nexists$ Device
16.b	*needed: Connection(NIC, Device)*
16.c	*needed: Connection(NIC, Device)*
16.d	*needed: Intact(Device)*
16.e	DataRate(Device) > TransferRate(Transmission)
17.a	Length(Wiring) > RequiredDeadline(Transmission) $*2.0 * 10^8 \frac{m}{s}$
17.b	$\{\exists(NIC\ i)\|(Connection(Wiring, i) = FALSE)\}$
17.c	$\{\exists(NIC\ i)\|(Connection(Wiring, i) = FALSE)\}$
18.a	*By refining the ontology every requirement for Wiring is identified needed for reaching a level of confidence.*
19.a	Content(Transmission) = 0
19.b	*needed: Overhead(Transmission)*
19.c	*needed: Overhead(Transmission)*
19.d	*needed: Overhead(Transmission)*
19.e	*needed: Header(Transmission)*
19.f	TimeSent(Transmission) < RequiredTimeSent(Transmission)
19.g	TimeSent(Transmission) > RequiredTimeSent(Transmission)
19.h	Sequence(Transmission) < RequiredSequence(Transmission)
19.i	Sequence(Transmission) < RequiredSequence(Transmission)
19.j	TransferRate(Transmission) > RequiredTransferRate(Transmission)
19.k	TransferRate(Transmission) < RequiredTransferRate(Transmission)
20.a	Content(Transmission) $\subset$ Input(NIC)
20.b	Size(Transmission) < Output(NIC)
20.c	Transmission = INVERSE(Output(NIC))
21.a	$\exists$ Transmission a $\wedge$ $\nexists$ Sequence(Transmission a)

	Ontological Expression
21.b	Sequence(Transmission) != RequiredSequence(Transmission)
21.c	Sequence(Transmission) = INVERSE(RequiredSequence(Transmission)
21.d	Size(Transmission) > RequiredSize(Transmission)
22.a	TimeSent(Transmission) = 0
22.b	TimeSent(Transmission) > RequiredTimeSent(Transmission)
22.c	TimeSent(Transmission) < RequiredTimeSent(Transmission)
22.d	TimeSent(Transmission) < RequiredTimeSent(Transmission)
22.e	TimeSent(Transmission) > RequiredTimeSent(Transmission)
22.f	Sequence(Transmission) < RequiredSequence(Transmission)
22.g	Sequence(Transmission) > RequiredSequence(Transmission)
23.a	TimeReceived(Transmission) = 0
23.b	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
23.c	TimeReceived(Transmission) < RequiredTimeReceived(Transmission)
23.d	TimeReceived(Transmission) < RequiredTimeReceived(Transmission)
23.e	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
23.f	Sequence(Transmission) < RequiredSequence(Transmission)
23.g	Sequence(Transmission) > RequiredSequence(Transmission)
24.a	TransferRate(Transmission) > RequiredTransferRate(Transmission)
24.b	TransferRate(Transmission) < RequiredTransferRate(Transmission)
24.c	TransferRate(Transmission) < RequiredTransferRate(Transmission)
24.d	TransferRate(Transmission) > RequiredTransferRate(Transmission)
24.e	TransferRate(Transmission) < RequiredTransferRate(Transmission)
25.a	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
25.b	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
26.a	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
26.b	TimeReceived(Transmission) > RequiredTimeReceived(Transmission)
27.a	Mode(Transmission) < RequiredMode(Transmission)
27.b	Mode(Transmission) > RequiredMode(Transmission)
27.c	RequiredMode(Transmission) = INVERSE(Mode(Transmission))
28.a	Period(Transmission) > RequiredPeriod(Transmission)
28.b	Period(Transmission) > RequiredPeriod(Transmission)
28.c	Period(Transmission) > RequiredPeriod(Transmission)
29.a	Sequence(Transmission) = INVERSE(RequiredSequence(Transmission))
29.c	RequiredSequence(Transm.) = INVERSE(Sequence(Transm.))
30.a	RequiredSize(Transmission) < Size(Transmission)
31.a	$\nexists$ RequiredTimeSent(Transmission)
31.b	RequiredTimeSent(Transmission) + Latency(Transmission) > Deadline(Transmission)
31.c	RequiredTimeSent(Transmission) $\notin$ RequiredSequence(Transmission)
32.a	$\nexists$ RequiredTimeReceived(Transmission)
32.b	RequiredTimeReceived(Transmission) > Deadline(Transmission)
32.c	Sequence(Transmission) < RequiredSequence(Transmission)
33.a	RequiredTransferRate(Transmission) < DataRate(Device)
33.b	RequiredTransferRate(Transmission) < DataRate(Device)
34.a	NodeCount(Network) = 0
34.b	NodeCount(Network) > DesignNodeCount(Network)
34.c	NodeCount(Network) < DesignNodeCount(Network)
35.a	DesignNodeCount(Network) = 0
35.b	DesignNodeCount(Network) > NodeCount(Network)
35.c	DesignNodeCount(Network) < NodeCount(Network)

	Ontological Expression
35.d	DesignNodeCount(Network) < NodeCount(Network)
36.a	DataRate(Device) = 0
36.b	DataRate(Device) > DataRate(NIC)
36.c	DataRate(Device)*time < RequiredSize(Transmission)
36.d	DataRate(Device)*time < RequiredSize(Transmission)
36.e	DataRate(Device) > DataRate(NIC)
36.f	DataRate(Device)*time < RequiredSize(Transmission)
37.a	*needed: Shielding(Network)*
37.b	*needed: EmissionRegulation(Network)*

5.2.5 Causal Influence Diagrams

The Causal Influence Diagrams formed in the second iteration are listed in appendix B.1.

The diagrams are formed by using a deviation's ontological expression top-node in the graph and then identifying those elements of the ontology that are needed to cause the deviation to occur. This investigation uses the principles of counterfactual and causal completeness test (see chapter 3.5).

Using the diagrams it is possible to identify essential events or interactions that can lead to problematic situations. As can be seen in the next chapter, the different approach to the description of deviations leads to the identification of system elements. It can be observed, that some elements identified to be needed in the ontology were not identified with the attribute-guide-word method but the causal analysis showed them to be needed.

The use of causal influence diagrams occasionally pointed towards a special class of deviations. Some deviations seemed to be problematic to the system if they would occur. The causal analysis using the system ontology showed that the deviation can never occur due to the fact that some of the causes needed for their occurrence were contradictory to each other.

This occurred in the CID for deviation 19.c, where two nodes, state that the "DataRate(Device)*time" has either be smaller than "RequiredSize(Transmission)" - node 1.1.1 - or larger than "RequiredSize(Transmission)" - node 1.3.1 (see Figure 5.1).

As the partitioning of the factors leading to the deviation was made mathematically, the absence of any of the deviation's factors would result in the deviation to occur. Therefore the antithesis in the CID does not lead to the graph being invalid. Either event 1.1 "Decrease in Content(Transmission)" or event 1.3

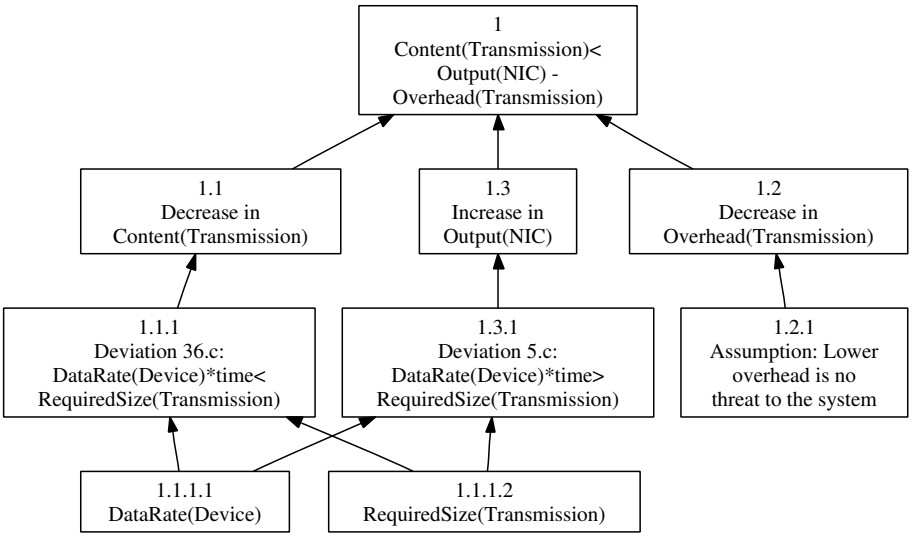


Figure 5.1: CID of deviation 19.c

"Increase in Output(NIC)" can occur not both together.

5.2.6 Identified Elements Missing in Ontology

The elements identified to be missing were:

	Type	Element	identified by
27	Property	FailureRate(NIC)	CID
28	Property	PowerRating(NIC)	CID
29	Property	Design(NIC)	CID
30	Property	Design(Wiring)	Deviation
31	Property	FailureRate(Wiring)	CID
32	Property	Overhead(Transmission)	Deviation
33	Property	Header(Transmission)	Deviation
34	Property	Energy(Transmission)	CID
35	Property	Shielding(Network)	Deviation
36	Property	EmissionRegulation(Network)	Deviation
37	Property	Load(Network)	CID
38	Property	Design(Network)	CID
39	Property	Intact(Device)	Deviation
40	Property	OutputEnergy(Device)	CID
41	Relation	Connection(NIC, Device)	Deviation

5.3 3rd Iteration

5.3.1 System Ontology

After trying to express the formed deviations of the previous iteration using the second iteration's ontology, 6 missing elements were identified in the ontology previously used. The creation of Causal Influence Diagrams leading to a deviation identified 8 additional elements missing in the ontology. The ontology for the third iteration was expended by these 14 identified elements.

5.3.1.1 Objects

Object	Description
NIC	The Network Interface Controller. It is the interface between the input device and the physical network.
Wiring	The physical connection between the systems' NICs.
Transmission	The transport of information between NICs over the physical network.
Network	The system consisting of Wiring and NICs that exists to provide means for devices to communicate.
Universe	The unity of all objects that are part of the system, the environment and the world.
Device	The facility that uses the network to communicate with other facilities.

5.3.1.2 Properties:

Object:	**NIC**
Property	Description
Input	The information received by the NIC
Output	The information transmitted by the NIC
Intact	The integrity of the NIC, whose absence prevents the NIC from working properly.
DataRate	The speed that is formed by the volume of information the NIC can transmit in a given time unit.
FailureRate	The expected rate at which the functionality of the NIC cannot be maintained.
PowerRating	The maximal voltage or current at which the NIC can maintain its function.
Design	The result of all constructional decisions made for the NIC, including its interfaces.

Object:	**Wiring**
Property	Description
Intact	The integrity of the Wiring, whose absence prevents the physical network from working properly.
Length	The distance a transmission has to cover for reaching every NIC connected to the Wiring once.
Requirements	The unity of all requirements the Wiring has to fulfil.
Design	The result of all constructional decisions made for the Wiring.
FailureRate	The expected rate at which the functionality of the Wiring cannot be maintained.

Object:	**Transmission**
Property	Description
Size	The size of the Transmission
Deadline	The latest possible point in time at which the Transmission can be received without loosing its value.
Period	Frequency of the generation of a type of Transmission
Mode	The mode used for the Transmission. This can be either time-triggered or event-triggered.
Latency	The time it takes for the complete transmission of information over the network.
Jitter	The variance in the transmission time of a multitude of same-typed transmissions.
Content	The payload transfered with the Transmission.
Format	The layout of information the Transmission is structured by.
Sequence	The sequence in which the transmission succeed each other.
TimeSent	The point in time the Transmission is completely relayed from the NIC to the Wiring.
TimeReceived	The point in time the Transmission is completely relayed from the Wiring to the NIC.
TransferRate	The speed that is formed by the volume of information the Wiring can transmit in a given time unit between any two NICs.
RequiredJitter	The value given in the requirements of the communication for the maximal value that is acceptable for the Jitter of the Transmission.
RequiredLatency	The value given in the requirements of the communication for the maximal value that is acceptable for the Latency of the Transmission.
RequiredMode	The Mode given in the requirements of the communication the Transmission has to be transfered by.
RequiredPeriod	The value for the Period given in the requirements of the communication the Transmission is suspected to have.
RequiredSequence	The point in succession given in the requirements of the communication the Transmission has to follow.
RequiredSize	The value given in the requirements of the communication for the maximal value that is acceptable for the Size of the Transmission.

Property	Description
RequiredTimeSent	The value derived from the requirements of the communication for the maximal value that is acceptable for the TimeSent of the Transmission.
RequiredTimeReceived	The value derived from the requirements of the communication for the maximal value that is acceptable for the TimeReceived of the Transmission.
RequiredTransferRate	The value given in the requirements of the communication for the TransferRate of the Transmission.
Overhead	The amount of information transmitted that is not content.
Header	The amount of information needed by the Transmission for the handling of the information.
Energy	The current and voltage the Transmission is transfered by.

Object:	**Network**
Property	Description
NodeCount	The number of nodes connected to the Wiring.
DesignNodeCount	The number of nodes used for the design and the formulation of requirements.
Shielding	The facilities used for the protection of the parts building the network against electro-magnetic interference.
EmissionRegulation	The regulatory limits set for the intensity of emissions emitted by the Network.
Load	The ration of information transmitted to the amount maximal transmittable.
Design	The result of all constructional decisions made for the Network.

Object:	**Device**
Property	Description
DataRate	The speed that is formed by the volume of information the Device can process in a given time unit.
Intact	The integrity of the Device, whose absence prevents the Device from working properly.
OutputEnergy	The current and voltage used by the Device for transmission of information to the NIC.

5.3.1.3 Relations

Relation	Description
Connection(Wiring, NIC)	The feature of the NIC to be connected properly with the Wiring.
Interference(Network, Universe)	The feature of the Universe to influence the function of the Wiring.
Connection(NIC, Device)	The feature of the Device to be connected properly to the NIC.

5.3.2 New Deviations Identified by HAZOP

In addition to the deviations already identified in the first two iterations the following deviations were identified by the interpretation of the attribute-guideword combinations formed for the ontology's new elements in the third iteration.

Table 5.21: List of deviations formed

	Deviation
38.a	The FailureRate for the NIC is bigger than acceptable
39.a	The PowerRating for the NIC is lower than intended
39.b	The PowerRating for the NIC is only partially achieved
40.a	The Design of the NIC is less elaborated than needed
40.b	The Design of the NIC was only partially realised
41.a	The Design of the Wiring is less elaborated than needed
41.b	The Design of the Wiring was only partially realised
42.a	The FailureRate for the Wiring is too high
43.a	The Overhead of the Transmission is bigger than acceptable
44.a	The Energy of the Transmission is bigger than expected
44.b	The Energy of the Transmission is smaller than expected
44.c	The Energy is only partially achieved
44.d	The Energy is reversed
45.a	The Network has no Shielding
45.b	The Shielding is less elaborated than needed
45.c	The Shielding is only partially achieved
46.a	The regulations are only partially achieved
47.a	The Load of the Network is greater than expected
47.b	The Load is only partially achieved
48.a	The Design of the Network is less elaborated than needed
48.b	The Design of the Network is only partially achieved
49.a	The Device is not intact
49.b	The Device is less intact than needed
49.c	The Device is only partially intact
50.a	The Device has no OutputEnergy
50.b	The OutputEnergy of the Device is bigger than expected
50.c	The OutputEnergy of the Device is lower than expected
50.d	The OutputEnergy of the Device is only partially achieved
50.e	The OutputEnergy of the Device is reversed
51.a	The Device is not connected to the NIC
51.b	More than one connection between NIC and Device exists
51.c	Less connections than expected exist between NIC and Device
51.d	The connection between Device and NIC is only partially achieved
51.e	The connection between Device and NIC works faster than expected
51.f	The connection between Device and NIC works slower than expected

5.3.3 Assumptions Used in the Identification

As in the first two iterations assumptions on the formed combinations were made in the third iteration.

Table 5.22: List of assumptions made in deviation identification (3^{rd} iteration)

	Assumption
Ass36	The FailureRate of the NIC is known.
Ass37	Quality conformance tests have verified the NICs' FailureRate.
Ass38	The values for the PowerRating of the NIC are known.
Ass39	The maximal values for the PowerRating of the NIC are not variable.
Ass40	No attribute of the NIC contradicts the Design of the NIC.
Ass41	No attribute of the NIC contradicts the Design of the NIC.
Ass42	The FailureRate of the Wiring is known.
Ass43	Quality conformance tests have verified the Wirings' FailureRate.
Ass44	The Energy used for the Transmission can be measured instantaneously.
Ass45	No attribute of the Wiring influences the functionality of the Shielding.
Ass46	The Load of the Network can be measured instantaneously.
Ass47	No attribute of the Network contradicts its Design.
Ass48	The OutputEnergy of the Device can be measured instantaneously.
Ass49	No relation between NIC and Device influence their Connection.

5.3.4 Ontological Expressions of Deviations

Table 5.23: List of associations possible in this iteration

	Ontological Expression
2.d	Design(Wiring) ∩ Requirements(Wiring) ≠ Requirements(Wiring)
16.b	Connection(NIC, Device a) ∧ Connection(NIC, Device b)
16.c	Connection(NIC, Device) = FALSE
16.d	Intact(Device) = FALSE
19.b	Content(Transm.) > RequiredSize(Transm.) - Overhead(Transm.)
19.c	Content(Transm.) < Output(NIC) - Overhead(Transm.)
19.d	Content(Transm.) < Output(NIC) - Overhead(Transm.)
19.e	Content(Transm.) = INVERSE(Output(NIC) - Header(Transm.))
37.a	Interference(Network, Universe) > Shielding(Network)
37.b	Interference(Universe, Network) > EmissionRegulation(Transmission)
38.a	*needed: RequiredFailureRate(NIC)*
39.a.1	Energy(Transm.) > PowerRating(NIC)
39.a.2	OutputEnergy(Device) > PowerRating(NIC)
39.b.1	Energy(Transm.) > PowerRating(NIC)
39.b.2	OutputEnergy(Device) > PowerRating(NIC)
40.a	*needed: Requirements(NIC)*
40.b	Design(NIC)\{Design(NIC) ∩ NIC}≠ ∅
41.a	Requirements(Wir.)\{Requirements(Wir.) ∩ Design(Wir.)} ≠ ∅

	Ontological Expression
41.b	Design(Wiring)\{Design(Wiring) ∩ Wiring} ≠ ∅
42.a	*needed: RequiredFailureRate(Wiring)*
43.a	Content(Transmission) < DataRate(Device) * time
44.a	Energy(Transmission) > PowerRating(NIC)
44.b	*needed: Sensitivity(NIC)*
44.c	*needed: Sensitivity(NIC)*
44.d	*needed: OutputEnergy(NIC)*
45.a	Shielding(Network) = 0
45.b	Interference(Network, Universe) > N
45.c	Interference(Network, Universe) > N
46.a	*needed: Emission(Network)*
47.a	Jitter(Transmission) > RequiredJitter(Transmission)
47.b	$\sum Output(NIC)/time < \sum RequiredTransferRate(Transmission)$
48.a	NodeCount(Network) < DesignNodeCount(Network)
48.b	NodeCount(Network) < DesignNodeCount(Network)
49.a	NOT Intact(Device)
49.b	NOT Intact(Device)
49.c	NOT Intact(Device)
50.a	OutputEnergy(Device)=0
50.b	OutputEnergy(Device) > PowerRating(NIC)
50.c	*needed: Sensitivity(NIC)*
50.d	*needed: Sensitivity(NIC)*
50.e	INVERSE OutputEnergy(Device)
51.a	Connection(NIC, Device) = FALSE
51.b	Connection(NIC i, Device a) ∧ Connection(NIC i, Device b)
51.c.1	Connection(NIC, Device) = FALSE
51.c.2	Reduction of Redundancy (no hazard to the system)
51.c.3	DataRate(Device)/time < RequiredTransferRate(Transmission)
51.d.1	Connection(NIC, Device) = FALSE
51.d.2	Reduction of Redundancy (no hazard to the system)
51.d.3	DataRate(Device)/time < RequiredTransferRate(Transmission)
51.e	DataRate(Device) > TransferRate(Transmission)
51.f	DataRate(Device) > TransferRate(Transmission)

6 Conclusions and Outlook

6.1 Conclusions

6.1.1 Ontological Analysis

This work described how the combination of several assessment methods for system and safety development can be used for a systematic approach to formulate a detailed description of a system in development.

This application showed, that the combination of deviation identification, ontological system description and Causal System Analysis led to detailed description of the elements the system's functionality depends on.

The level of detail discovered by applying the iterative decomposition was high, considering the description resulted from only three iterations. After two analysis iterations elements like Shielding or the OutputEnergy of a Device were identified to be needed as elements of the ontology.

In chapter 3 the importance for a development method to identify a set of requirements as complete as possible was pointed out. In Ontological Analysis the requirements result from of a complete investigation using the phases of iterative decomposition and safety and risk analysis. As this work concentrated on the iterative decomposition of the system, the result can not answer the completeness question satisfactorily.

As can be noted by looking at the results of this work the system ontology became more detailed with each iteration. This increase in detail is not distributed evenly over the investigated system but problematic regions were described with greater detail while unproblematic regions were kept simple.

This results from the application of HAZOP's attribute-guide-word combinations

that identify possible deviations from the design intent. If this knowledge is expressed using the ontology, identified missing elements in the ontology will be related to the deviation. Unproblematic elements of the system will not lead to a deviation and cannot introduce new elements into the system.

If the results of this work are used as input for the safety and risk analysis this characteristic is useful, as the development of risk reducing countermeasures is concentrated on the problematic regions of the system.

The ratios between deviations expressible and those not expressible indicate that the system is described increasingly detailed. It may be possible, that at a later point in the iterative decomposition an element is identified, that leads to a region of the system description previously not investigated. As the elements identified in this context will be introduced into the ontology and the description refined by the iterative decomposition it can be assumed, that the ratio would later on improve again. In the process of the iterative decomposition elements missing in the system ontology are identified and increasingly more elements are included into the description. If an upper limit for the number of problematic regions in a system exists, the ontology will evolve into a state where all problematic events can be described using the ontology.

It was observed in the iterative decomposition that the description of the system was made with a level of detail increasing with the number of iterations used. If this tendency can be kept up, the description will approximate to a complete description.

6.1.2 Communication-Bus

The identification of deviations identified only a small number of deviations that originated from the protocol's method for media access. For attributes considering timing requirements of the communication system the importance of the method used for media access was not apparent from the deviation's formulations. The influence of the media access in these deviations was identified by the Causal Influence Diagrams of these deviations. These relations lead to deviations that cannot occur, depending on the type of media access chosen.

6.1.3 Problems Encountered

The methods included in Ontological Analysis have to be used carefully. If a method is applied not properly, it has the ability to reduce the confidence that

can be placed into the resulting system description.

The formulation of the system ontology must be verified to be unambiguous. If the ontology would be ambiguous the expressions made by using the ontology can be misleading.

Gruber [Gru93] pointed out that "a commitment to a common ontology is a guarantee of consistency, but not completeness, with respect and assertions using the vocabulary defined in the ontology." This requires that the system's elements are not only expressed by using the ontology's vocabulary but share the same knowledge to achieve completeness.

A problem of the HAZOP method lies in its dependence on a complete system description being used for the analysis as pointed out by [RCC99, p.47]. This problem would lead to the study's completeness being endangered and additional representations needed to be made if elements important for the safety of the system are missing from the description. This problem can be barred in Ontological Analysis assuming that the phases of iterative decomposition and risk and hazard analysis describe the system precisely and identify all additions to be made as well as their implications to the system.

The task of expressing deviations by using the system ontology can lead to mistakes if not made accurate. Software assistance aiding the developer by presenting the identified deviation and the ontology available could concentrate the developer's view exclusively on the stated problem, reducing the tendency to use short-cuts and thereby making faulty expressions.

The results from the task of Causal System Analysis depend on the careful application of the requirements made towards necessary causal factors and the Causal Sufficiency Criterion being met.

If CIDs based on the ontological expression of a deviation are analysed systematically like described in chapter 3.5.5, the Causal Sufficiency Criterion can be over-determined. This does not influence the conclusions that can be made on the analysis. For the risk and hazard analysis it would be desirable to extend the notation of the Causal Influence Diagrams by elements indicating if a relation between cause and effect represents a boolean "AND" or an "OR". This might make the determination of a hazard's frequency easier.

The identification of missing elements can influence the analysis's results in the same way the formulation of the ontology does. It has to be warranted that the ontology does not become ambiguous through the added elements.

For the investigation presented in this work, the "team" consisted only of the

author. This "group" size would not be permissible for a typical HAZOP analysis. In the application of the iterative decomposition on the investigated example this group size had not as big an influence as would be expected. For the purpose of detecting erroneous expressions or Causal Influence Diagrams a larger size for the development group would be preferable. Whereas it can be said in respect to the achieved results that the team size need not be as large as demanded by HAZOP. A group of three developers might be sufficient. Using software support the documentation of the development could be made automatically using the input from the development process.

6.1.4 Summarisation

The iterative decomposition can be used for the description of a system with great level of detail and concentrating on problematic regions in the system.

For allowing the Ontological Analysis to answer the completeness questions satisfactorily the phase of iterative decomposition must enable the detailed description of a system and the phase of safety and risk analysis must identify hazards and risk sufficiently accurate and develop countermeasures to reduce the risk beneath a level acceptable. These two phases combined can provide a satisfying answer to the completeness question.

It was shown that the iterative decomposition can achieve this goal if applied properly.

The interaction of systematic approaches for the identification and expression of problematic parts of the system led to a description of the system especially detailed in areas that can lead to problematic behaviour of the system.

The problems encountered during the analysis indicate, that it is very important to apply the analysis's methods accurately and avoid the use of short-cuts. Short-cuts may seem to increase the speed of the analysis but pose the threat of compromise the results of the investigation.

As the amount of decisions that have to made in the analysis is very large, using short-cuts is tempting. Methods assisting the analysis process by presenting the information available and needed for the current task. Software assistance can also take the documentation of the analysis's findings.

Another important result is introduced by using the approach of logical reasoning for describing occurrences leading to a failure. This makes it possible to verify the reasoning the development was made by. Basing on this reasoning the pro-

ceedings of the development process can be documented comprehensively. If the results were found not to be appropriate from some point of view it is possible to demonstrate, how the result was achieved. An argumentation could than be made on whether different views on the system are needed. This is possible due to the design of an ontology describing the system. The ontology of this design process produces need not be the same for each group of developers as people can have different perceptions of preferred elements.

6.2 Outlook

The result of the iterative decomposition is a detailed description of the system. As every technical system induces risk into the environment the detailed description alone cannot sufficiently prove that the development has covered for every possible behaviour of the system. Risks will have to be avoided or mitigated. For this additions to the system in form of countermeasures must be made. These will interact with the system components and can introduce other failures through this interaction.

For stating, that every failure has been considered, the impacts of these additions on the system have to be analysed thoroughly. It has to be shown, that the phase of safety and risk analysis can provide for this requirement.

The phase of safety and risk analysis has to be researched with greater detail. The central points in this task is to identify risk regarded as acceptable and the assessment of risk imposed by a system.

In areas where people involved with a system have only limited influence on controlling the risk, like with chemical production facilities or mass-transit, detailed requirements are made towards acceptable risk. In areas where people involved with a system have the possibility to control risk or impact, like with road traffic, it is more difficult to identify a level of risk that is acceptable. Even demands like MGS or GAMAB may prove difficult as the statistical information on accidents differs between countries and the decision if a fatality enters the statistic is made on the time elapsed between accident and death.

The safety and risk analysis can only produce precise information on the expected frequency of an accident, if every accident results from a hazard. As Ladkin pointed out [Lad01] this is not necessarily be the case. For Ontological Analysis this implies, that the system description must identify all possible factors that can lead to an accident. It is possible that these factors are not part of the system. This mapping is reasonable if it is not possible to exert influence on them. It has

to be researched, if Ontological Analysis can provide this requirement or what influences its omission would have.

Ontological Analysis is a promising approach for systematically developing detailed system requirements. It is a rather new technique that is, asides from this work, currently applied in requirements development for a Train Dispatching System [Sie05].

The main reasons because of which this method in not broadly applied today are the method being young and software assistance only being available for partial tasks. The development of a supporting software solution would improve the spread of the method. It could be concentrated as a first step on the phase of iterative decomposition and later on include the phase of safety and risk analysis.

A HAZOP tables

A.1 HAZOP sentences of system - 1st Iteration

Attribute:		**NIC**
Guide word		Interpretation
No		No part of the NIC intention is achieved
More		More NICs in system than expected
Less		Less NICs in system than expected
As well as		An additional NIC occurred in the system
Part of		A NIC is fragmented
Reverse		Logical opposite of NIC occurs
Other than		NIC is replaced by something different
Early	a.	NIC is integrated early
	b.	NIC transmits early
Late	a.	NIC is integrated late
	b.	NIC transmits late
Before		NIC transmits ahead of sequence
After		NIC transmits late in sequence
Faster		NIC transmits too fast
Slower		NIC transmits too slow

Comments on the formed HAZOP sentences:

No This sentence does not lead to a deviation because a network cannot exist without NICs. A NIC may be included into a connected device but it has to exist.

As well as The occurrence of an additional NIC in the system would lead to the deviation of More NIC.

Reverse The logical opposite of a NIC is ”no NIC”.

Other than The replacement of NICs with something different leads to a network without NICs. This would lead to a network without function.

Early (a), Late (a) These deviations do not represent an immediate threat to the system. They will probably be part of the causal analysis of other deviations and therefore are not analysed on their own at least in phase 1.

Early (b),Late (b), Before, After, Faster, Slower These sentences can only be interpreted in respect of the function of the NIC. As the transmission is analysed separately these sentences are interpreted there.

Attribute:		**Wiring**
Guide word		Interpretation
No		No physical connection between NICs
More		Wiring too long
Less		Wiring too small
As well as		Other medium in addition to wiring present
Part of		Wiring meets design intention only in part
Reverse	a.	Function of wiring is reversed
	b.	Wiring integrated falsely
Other than		Complete substitution of Wiring

Guide word	Interpretation
Early	Wiring integrated too early
Late	Wiring integrated too late
Before	Wiring integrated before it was supposed to be
After	Wiring integrated after it was supposed to be
Faster	Wiring integrated too fast
Slower	Wiring integrated too slow

Comments on the formed HAZOP sentences:

No This deviation is identified with "Connection(Wiring, NIC)"

Reverse (a) If the function of the wiring is reversed this would mean, that no connection between the NICs is provided by the wiring. This is equal with "No wiring".

Reverse (b) As long as the functionality of the wiring is assured, the way it was integrated does not have to be regarded.

Other than If the wiring would be completely substituted the physical connection between the NICs would be lost. This is equivalent to No Wiring.

Early, late, before, after, faster, slower The wiring has to provide the functionality to connect the NICs with each other. The timing of integration does not have to be regarded, if the functionality is assured.

Attribute:		**Transmission**
Guide word		Interpretation
No		No information is transmitted
More		More information than intended is transmitted
Less		Less information than intended is transmitted
As well as		Additional information is transmitted
Part of		Information is only partially transmitted
Reverse	a.	Transmission is well formed but carries wrong content
	b.	Information is reversely transmitted
Other than		Complete substitution of transmission
Early	a.	Transmission is sent too early
	b.	Transmission is received too early
Late	a.	Transmission is sent too late
	b.	Transmission is received too late
Before		Transmission is sent ahead of sequence
After		Transmission is sent behind sequence
Faster		Transfer rate greater than intended
Slower		Transfer rate lower than intended

Comments on the formed HAZOP sentences:

Other than The communication is based on the transmission of information without which the network cannot exist.

Attribute:	**Input(NIC)**	
Guide word	Interpretation	
No		NIC does not get input
More	a.	NIC receives more input than expected from the device
	b.	NIC receives more input than expected from the network
Less	a.	NIC receives less input than expected from the device
	b.	NIC receives less input than expected from the network
As well as	a.	NIC receives input from more sources than expected
	b.	NIC receives more input than expected from the network
Part of	a.	NIC receives only part of the expected input from the device
	b.	NIC receives only part of the expected input from the network
Reverse	a.	NIC reverses received input
	b.	NIC receives input in reverse order
Other than		Input of NIC is replaced
Early		NIC receives input early
Late		NIC receives input late
Before		The input is effected ahead of sequence
After		The input is effected behind sequence
Faster		Input is received faster than expected
Slower		Input is received slower than expected

Comments on the formed HAZOP sentences:

Less Less input received by the NIC is no deviation if the expected value was too high in comparison with the reality. If this assumption is not true, the resulting deviation is identified by "Less transmission" or "Part of transmission".

As well as (b) This sentence is identical with More Input (b)

Part of (a) This sentence is identical with Less Input (a)

Part of (b) This sentence is identical with Less Input (b)

Reverse (b) This sentence results in a combination of Before Input and After Input because the sequence of the input is altered.

Other than The input of the NIC can only be replaced by the already identified No Input which is the logical opposite of Input.

Before, after The sequence in not relevant for the input. It is relevant for the message and its deviations are identified there.

Faster, slower These deviations depend on the transmission rate of the message which is identified under Faster/Slower Message.

Attribute:	**Output(NIC)**	
Guide word	Interpretation	
No		NIC has no output
More	a.	NIC has more output to the device than expected
	b.	NIC has more data to transmit than expected
Less		NIC has less output then expected
As well as		NIC has output for more devices than expected
Part of		NIC transmits only part of the output

Guide word	Interpretation	
Reverse	a.	NIC transmits inverted output
	b.	NIC transmits output in reverse order
Other than		Output is replaced
Early		Output is sent early
Late		Output is sent late
Before		Output is sent ahead of sequence
After		Output is sent behind sequence
Faster		Output is sent faster
Slower		Output is sent slower

Comments on the formed HAZOP sentences:

Less Less input transmitted by the NIC is no deviation if the expected value was too high in comparison with the reality. If this assumption is not true, the resulting deviation has to be identified with the object "Device" as this object has to generate less information than expected.

Reverse (b) This sentence results in a combination of Before Output and After Output because the sequence of the output is altered.

Before/after The sequence in not relevant for the output. It is relevant for the message and its deviations are identified there.

Faster, slower These deviations depend on the transmission rate of the message which is identified under Faster/Slower Message.

More (b) This is no deviation because it describes the normal behaviour of the system in an extended environment.

Attribute:	**Intact(NIC)**
Guide word	Interpretation
No	The NIC is not intact
More	The NIC is more than intact
Less	The NIC is less than intact
As well as	The NIC is more than intact
Part of	The NIC is only in part intact
Reverse	The concept of intact is reversed
Other than	The concept of intact is replaced
Early	The concept of intact happens early
Late	The concept of intact happens late
Before	The concept of intact happens before something
After	The concept of intact happens after something
Faster	The concept of intact is faster than intended
Slower	The concept of intact is slower than intended

Comments on the formed HAZOP sentences

More, Less, As well as, Part of An object can be either intact or not but cannot be in

between these states.

Reverse The concept of intact aims at assessing the functionality of the NIC. Reversing the concept would only result in switching the labels. The assessment of the functionality would not be limited.

Other than A NIC has to be intact to be able to operate. Because of this Intact(NIC) is irreplaceable.

Early, Faster If the NIC is intact early or faster than needed, it will be intact any time afterwards until it breaks. This is the expected state of Intact(NIC) and no threat.

Late, Slower If the NIC would achieve its functionality later than needed, it would not be intact at the required time. This deviation is identified with "No Intact(NIC)".

Before, After If the NIC is intact before an event it can be assumed that it will be intact at the time of the event until stated otherwise. Likewise it can be assumed that if the NIC is intact after an event it was intact before the event if not stated otherwise. These are the expected states of Intact(NIC) and no threats.

Attribute:	**Intact(Wiring)**
Guide word	Interpretation
No	The wiring is not intact
More	The wiring is more than intact
Less	The wiring is less than intact
As well as	The wiring is more than intact
Part of	The wiring is only in part intact
Reverse	The concept of intact is reversed
Other than	The concept of intact is replaced
Early	The concept of intact happens early
Late	The concept of intact happens late
Before	The concept of intact happens before something
After	The concept of intact happens after something
Faster	The concept of intact is faster than intended
Slower	The concept of intact is slower than intended

Comments on the formed HAZOP sentences

More, less, as well as, part of An object can be either intact or not but cannot be in between these states.

Reverse The concept of intact aims at assessing the functionality of the wiring. Reversing the concept would only result in switching the labels. The assessment of the functionality would not be limited.

Other than The wiring has to be intact to be able to operate. Because of this Intact(Wiring) is irreplaceable.

Early, faster If the wiring is intact early or faster than needed, it will be intact any time afterwards until it breaks. This is the expected state of Intact(Wiring) and no threat.

Late, Slower If the wiring would achieve its functionality later than needed, it would not be intact at the required time. This deviation is identified with "No Intact(Wiring)".

Before, after If the wiring is intact before an event it can be assumed that it will be intact at the time of the event until stated otherwise. Likewise it can be assumed that if the wiring is intact after an event it was intact before the event if not stated otherwise. These are the expected states of Intact(Wiring) and no threats.

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

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.

ATTRIBUTE:	**Deadline(Transmission)**
GUIDE WORD	INTERPRETATION
No	The information is not transmitted in time
More	Deadline for a transmission type was defined with greater value than needed
Less	Deadline for a transmission type was defined with lower value than needed
As well as	Additional deadline occurred

Guide word	Interpretation
Part of	Design intent of deadline is only partially achieved
Reverse	Logical opposite of deadline occurs
Other than	Complete substitution of deadline
Early	The deadline value is too small
Late	Decrease in system performance because of too great deadline value
Before	The deadline is effected ahead of sequence
After	The deadline is effected behind sequence
Faster	The deadline value is too low
Slower	The deadline value is too big

Comments on the formed HAZOP sentences:

Less, early, faster The deadline for a transmission type was defined with a smaller value than needed. This is no immediate threat to the communication but an unnecessary increase of the system costs.

As well as The deadline of a transmission type cannot be influenced by other messages of any type.

Part of The design intention regarding deadline is the need for a transmission type to be transmitted in a defined time span. This can either be achieved or not, but not in part.

Reverse The logical opposite of the deadline of a transmission type cannot be defined.

Other than deadline Deadline is a value given by the system design and cannot be substituted.

Before, after A deadline in defined with a fixed value and therefore cannot be effected.

Late This is the same deviation as "more deadline"

Attribute:	**Period(Transmission)**
Guide word	Interpretation
No	None of the period intent is achieved
More	A class of transmission occurs more often than defined
Less	A class of transmission occurs less often than defined
As well as	Additional period occurred
Part of	Only part of period is achieved
Reverse	A sporadic transmission type is sent periodically and vice versa
Other than	Complete substitution of period
Early	Period timing early
Late	Period timing late
Before	Period occurs ahead of sequence
After	Period occurs behind sequence
Faster	A sporadic transmission type is transmitted periodically
Slower	A periodic transmission type is transmitted sporadically

Comments on the formed HAZOP sentences:

No The period describes the recurrence rate of a transmission type and divides it into two groups, periodic and sporadic transmission types. The intent of period would be the classification of transmission types. This is always achieved regardless of the transmission meeting its assigned class.

As well as The period of a transmission is a definition. It meets the defined value or misses it.

Part of If only part of the period would be achieved, the real rate of occurrence would be smaller than the predicted. This is equal to "Less Period(Transmission)".

Reverse This sentence is the combination of FASTER PERIOD and SLOWER PERIOD.

Other than Period is a definition and therefore cannot be completely substituted.

Before, after, early, late The period is a value representing a communication type. It isn't bound to any sequence.

ATTRIBUTE:	**Mode(Transmission)**
GUIDE WORD	INTERPRETATION
No	Information is not transmitted
More	Event triggered transmission is sent in time triggered mode
Less	Time triggered transmission is sent in event triggered mode
As well as	Additional mode occurred
Part of	Only part of mode is achieved
Reverse	Logical opposite of mode occurs
Other than	The network is replaced by something completely different
Early	Mode timing early
Late	Mode timing late
Before	Mode occurs ahead of sequence
After	Mode occurs behind sequence
Faster	Mode is done with the right timing
Slower	Mode is not done with the right timing

Comments on the formed HAZOP sentences:

As well as One transmission can only have one mode. Therefore this deviation isn't credible.

Part of The mode of transmission is achieved or is not achieved. It cannot be partially achieved.

Reverse A logical opposite to the mode of transmission does not exist.

Other than A message has to be transmitted either in time- or event-triggered mode. The investigated network cannot include transmission modes developed in the future.

Before, after, early, late The mode of transmission is a value representing a communication type. It isn't bound to any sequence.

Faster, slower Timing does not affect the mode of transmission.

Attribute:	**Latency(Transmission)**
Guide word	Interpretation
No	Transmission has no latency
More	Transmission latency is bigger than intended
Less	Transmission latency is lower than intended
As well as	Additional latency occurred
Part of	Design intention of latency is partially achieved
Reverse	Logical opposite of latency occurred
Other than	Complete substitution of latency
Early	The actual latency timing effects earlier than intended
Late	The actual latency timing effects later than intended
Before	Latency occurs ahead of sequence
After	Latency occurs after sequence
Faster	Latency is defined too small
Slower	Latency is defined too big

Comments on the formed HAZOP sentences:

No The latency is a value essential for the transmission of information. It can be NULL but has to exist.

Less, faster A latency smaller than intended is significant for an improved communication. Therefore this deviation represents no hazard.

As well as The latency is a value for the time needed for transmission of information. Each transmission has only one latency. "Additional latency occurred" could mean that more than one transmission occurred simultaneously.

Part of Latency is a property implied by every kind of communication and cannot be partially achieved.

Reverse For latency as the gap between the sending and receiving of a transmission a logical opposite cannot be defined.

Other than This deviation is without meaning as a transmission without latency is the same as a transmission with latency zero. Therefore a transmission has to have a latency.

Early, late, before, after These deviations are without meaning as the latency has no sequence.

Attribute:	**Jitter(Transmission)**
Guide word	Interpretation
No	Design intent of jitter is not achieved
More	Jitter is bigger than intended
Less	Jitter is lower than intended
As well as	Additional jitter occurred
Part of	Design intent of jitter is partially achieved
Reverse	Logical opposite of jitter occurs
Other than	Complete substitution of jitter
Early	Jitter timing effects earlier than intended
Late	Jitter timing effects later than intended
Before	Jitter occurs ahead of sequence

Guide word	Interpretation
After	Jitter occurs behind sequence
Faster	Jitter timing is faster than intended
Slower	Jitter timing is slower than intended

Comments on the formed HAZOP sentences:

No Jitter is a fundamental concept of digital communications. It is therefore existent at everytime in such a communication.

Less, early, faster A jitter smaller than intended is significant for an improved communication. Therefore this deviation represents no hazard.

As well as The jitter is identified for the transfer of one transmission type. If more than one transmission type is transfered each has its jitter value. If the jitter of multiple types of transmission could influence each other, this would lead to an increased or reduced jitter value. These effects are identified by the deviations "more jitter" and "less jitter".

Part of The design intention regarding jitter is the definition of the highest jitter which is acceptable for the system. This intention cannot be partially achieved.

Reverse For jitter as the variance of the transmission time a logical opposite cannot be defined.

Other than This is equivalent to a jitter of zero and represents no problem.

Before, after This deviation is without meaning as jitter has no sequence.

Late, slower This deviation is identical with "more jitter".

Attribute:	**Connection(Wiring, NIC)**
Guide word	Interpretation
No	No connection between wiring and NIC exists
More	More connections between wiring and NIC exist than designed for
Less	Less connections between wiring and NIC exist than designed for
As well as	In addition to the connection other relation between wiring and NIC exist
Part of	Connection between wiring and NIC only partially achieved
Reverse	Connection between wiring and NIC reversed
Other than	Connection between wiring and NIC is replaced by different concept
Early	Connection happens early
Late	Connection happens late
Before	Connection happens early in sequence
After	Connection happens late in sequence
Faster	Connection happens faster than designed for
Slower	Connection happens slower than designed for

Comments on the formed HAZOP sentences:

Less, part of These sentences are related to "no connection" as all lead to a connection not properly working.

As well as Under the assumption, that other relations between wiring and NIC do not threaten the connection, like a spring trying to separate them, other relations can coexist with this relation.

Reverse If this deviation has any meaning at all, the reversal of the connection would be equal to ”no connection”.

Other than The wiring is a main part of the system connecting the NICs. Therefore a connection between the wiring and the NICs has to exist.

Early, late, before, after, faster, slower For this relation only the properly function is important. Timing, sequence or speed of the assurance of the properly function is not relevant.

A.2 HAZOP sentences of system - 2^{nd} Iteration

Attribute:	**Network**
Guide word	Interpretation
No	No network exists
More	The network is vaster than intended
Less	The network is smaller than intended
As well as	Something else exists in addition to the network
Part of	Only part of the network exists
Reverse	The network is reversed
Other than	The network is replaced by different concept
Early	The network exists early
Late	The network exists late
Before	The network exists early in sequence
After	The network exists late in sequence
Faster	The network works faster than intended
Slower	The network works slower than intended

Comments on the formed HAZOP sentences:

No, other than The system is designed to provide the means of communication. Therefore the network has to exist and cannot be replaced.

As well as Something else will always exist in addition to the network. At least the devices connected by the network will be present. The only deviation this can pose is the interference of the external elements on the network. This is identified with Interference(Network, Universe)

Reverse For the network as a system a reversal is not credible.

Early, late, before, after The network has to be in working order at that point in time, when a transmission is made. The state of the network before or after this is not important.

Attribute:	**Universe**
Guide word	Interpretation
No	There is no Universe
More	There are more elements in the Universe then expected
Less	There are less elements in the Universe then expected
As well as	Something else exists in addition to the Universe
Part of	The Universe exists only in part
Reverse	The concept of Universe is inverted
Other than	The Universe is replaced by different concept
Early	The Universe exists early
Late	The Universe exists late
Before	The Universe exists early in sequence
After	The Universe exists late in sequence
Faster	The Universe is faster than expected
Slower	The Universe is slower than expected

Comments on the formed HAZOP sentences:

No By definition there will be a universe if at least one element exists. For the network to function properly the existence of at least the Wiring, one NIC and Device can be assumed as given.

More. less, part of The element with the ability to influence the system are those inside the system and those in the environment providing input to the system. If this set of elements is increased or decreased the resulting deviations are identified with the respective element.

As well as The Universe contains every element that exists. Therefore no element outside the universe can exist.

Reverse The reversal of the Universe would be the set of all elements that are not part of the system, the environment or the world. This set has to be empty at all times because no elements outside the Universe can exist. This sentence would mean that the universe switches into a set with no elements. This is not credible because in the result the network would not exist either which is argued in "No Network".

Other than The concept of Universe consists of the definition of the sum of sets. This mathematical set cannot be replaced completely but only renamed.

Early, late, before, after, faster, slower The sum of the elements of the system, the environment and the world can be formulated at every point in time and is not susceptible to speed. Therefore these sentences cannot be interpreted in a credible way.

Attribute:	**Device**
Guide word	Interpretation
No	The Device does not exist
More	There are more devices than intended
Less	There are less devices than intended
As well as	In addition to the device something else exists
Part of	The device only exists in part
Reverse	The device is inverted
Other than	The device is replaced by different concept
Early	The device exists early
Late	The device exists late
Before	The device exists early in sequence
After	The device exists late in sequence
Faster	The device works faster than expected
Slower	The device works slower than expected

Comments on the formed HAZOP sentences:

As well as Something else will always exist in addition to the Device. If it can influence some aspect of the system it is assumed, that it is identified and possible deviations with it.

Reverse The device is a physical object. In this context a reversal is not credible.

Other than The NIC has to get information form some kind of device. The concept of Device can therefore not be replaced.

Early, late, before, after Only the ability of the device to function is important not when this ability is achieved.

Slower If the Device produces less information than expected, resources are wasted but the system not threatened.

Attribute:	**DataRate(NIC)**
Guide word	Interpretation
No	NIC has no DataRate
More	The DataRate of the NIC is greater than expected
Less	The DataRate of the NIC is smaller than expected
As well as	Other properties of the NIC are present in addition to the DataRate
Part of	The DataRate is only achieved in part
Reverse	The DataRate is inverted
Other than	The DataRate is replaced by different concept
Early	The DataRate is measured early
Late	The DataRate is measured late
Before	The DataRate is measured early in sequence
After	The DataRate is measured late in sequence
Faster	The DataRate is measured faster than expected
Slower	The DataRate is measured slower than expected

Comments on the formed HAZOP sentences:

As well as It can be assumed, that other properties of the NIC are present and that they don't interfere with the DataRate of the NIC. If they do, the value of the DataRate will vary and either the deviation "More" or the deviation "Less" will describe the resulting deviation.

Reverse The DataRate is a value describing the speed of transmission the NIC works with. The reversal is not credible in this case.

Other than The DataRate the NIC works with is used. This concept can only be renamed but not replaced by a different concept.

Early, late, before, after, faster, slower The DataRate is a value describing the speed of transmission the NIC works with. It can be assumed that this value is measured instantaneously and is therefore not susceptible to timing or speed.

Attribute:	**Length(Wiring)**
Guide word	Interpretation
No	No length can be measured for the Wiring
More	The length of the Wiring is greater than expected
Less	The length of the Wiring is smaller than expected
As well as	In addition to the length other attributes of the Wiring are present
Part of	Only part of the length of the Wiring is achieved
Reverse	The length of the Wiring is inverted
Other than	The length of the Wiring is replaced by a different concept
Early	The length of the Wiring is measured early

Guide word	Interpretation
Late	The length of the Wiring is measured late
Before	The length of the Wiring is measured early in sequence
After	The length of the Wiring is measured late in sequence
Faster	The length of the Wiring is measured faster than expected
Slower	The length of the Wiring is measured slower than expected

Comments on the formed HAZOP sentences:

No Assuming that the Wiring exists a length can be computed even if it is equal to zero.

As well as Other attributes of Wiring will always be present. They cannot influence Length(Wiring) as this is the value of the distance a transmission has to cover for reaching every NIC connected to the Wiring at least once. Influences can only lead to an increase or decrease in this value. The problems caused by this are covered in "More" and "Less".

Reverse The distance a transmission has to cover can only be reversed if the computation of the value is faulty. This is assumed to be not the case.

Other than The distance a transmission has to cover for reaching every NIC on the Wiring at least once is required in the ontology. A replacement could only have another name but no other content.

Early, late, before, after, faster, slower Assuming that the computation of the value can be done instantaneously timing and speed cannot influence the attribute.

Attribute:	**Requirements(Wiring)**
Guide word	Interpretation
No	No requirements of the Wiring were defined
More	More requirements of the Wiring than needed were defined
Less	Less requirements of the Wiring than needed were defined
As well as	Other properties of the Wiring are present in addition to the requirements of the Wiring
Part of	The requirements of the Wiring are only partially met
Reverse	The requirements of the Wiring are inverted
Other than	The requirements of the Wiring are replaced by different concept
Early	The requirements of the Wiring are defined early
Late	The requirements of the Wiring are defined late
Before	The requirements of the Wiring are defined early in sequence
After	The requirements of the Wiring are defined late in sequence
Faster	The requirements of the Wiring are defined faster than expected
Slower	The requirements of the Wiring are defined slower than expected

Comments on the formed HAZOP sentences:

No It is assumed that requirements are defined at least for the length of the Wiring.

More, as well as Maybe more requirements of the Wiring were needed than actually used for the system design. It is assumed, that the additional requirements were checked against

interference or contradictions.

Part of The event of requirements not being met is a deviation of the element that needs to fulfil the requirement.

Reverse The reversal of requirements would either lead to "No requirements" or a change of the values in the requirements. Changed values would be requirements although useless. It is assumed, that useless values for requirements are identified and corrected.

Other than Requirements have to be given and cannot be replaced by a different concept.

Early, before, faster, slower The requirements have to exist at the time they are needed for the system design. If they exist, they will have been defined earlier. The speed of this definition is of no concern if the requirements are correct.

Late, after A requirement not being defined at the time it is needed, equals to "Less Requirements".

ATTRIBUTE:	**Content(Transmission)**
GUIDE WORD	INTERPRETATION
No	The Transmission carries no content
More	The Transmission carries more content than expected
Less	The Transmission carries less content than expected
As well as	Other attributes of the Transmission are present in addition to the content
Part of	The content is only transmitted in part
Reverse	The content of the Transmission is inverted
Other than	The content is replaced by different concept
Early	The content is transmitted early
Late	The content is transmitted late
Before	The content is transmitted early in sequence
After	The content is transmitted late in sequence
Faster	The content is transmitted faster than expected
Slower	The content is transmitted slower than expected

Comments on the formed HAZOP sentences:

As well as Other attributes of the Transmission will always be present. This will even be the case if no content is present.

Other than The communication is based on the transmission of content. This concept cannot be replaced.

ATTRIBUTE:	**Format(Transmission)**
GUIDE WORD	INTERPRETATION
No	Transmission has no format
More	The format of the Transmission is more elaborated than needed
Less	The format is too restricted for fulfilling the needs of the communication
As well as	Other attributes of the Transmission are present in addition to the format
Part of	The format is only achieved in part

Guide word	Interpretation
Reverse	The format is reversed
Other than	The format is replaced by different concept
Early	The format is defined early
Late	The format is defined late
Before	The format is defined early in sequence
After	The format is defined late in sequence
Faster	The format is defined faster than expected
Slower	The format is defined slower than expected

Comments on the formed HAZOP sentences:

No, other than Without a format the transmission could not be interpreted. It is therefore assumed that a format is defined.

More If the defined format is too elaborated it would result in a waste of resources but would not threaten the function of the system.

As well as Other attributes of the Transmission will be present in addition to the format. It is assumed that they do not interfere with the format.

Early, late, before, after, faster, slower The format has to be defined at the time of its use. Assuming that it is defined, it will have been defined earlier and cannot be defined later. The sequence and speed are of no concern.

Attribute:	**Sequence(Transmission)**
Guide word	Interpretation
No	No sequence of transmission defined
More	The sequence is more extensive than needed
Less	The sequence is to restricted for fulfilling the needs of the communication
As well as	Other attributes of transmission are present in addition to the sequence
Part of	The sequence of transmission is only partially achieved
Reverse	The sequence of transmission is reversed
Other than	The sequence of transmission is replaced by a different concept
Early	The sequence of transmission is defined early
Late	The sequence of transmission is defined late
Before	The sequence of transmission is defined early in sequence
After	The sequence of transmission is defined late in sequence
Faster	The sequence does not provide enough room for transmission
Slower	The sequence does provide more than enough room for transmission

Comments on the formed HAZOP sentences:

No In the case of event-triggered transmission the missing of a defined sequence is typical and cannot be a deviation. In the case of time-triggered transmission a defined sequence is required and can be assumed to be defined.

More, slower If the defined sequence is too elaborated it would result in a waste of resources but would not threaten the function of the system.

As well as Other attributes of the Transmission will be present in addition to the sequence. It is assumed that they do not interfere with the sequence.

Early, late, before, after The sequence has to be defined at the time of its use. Assuming that it is defined, it will have been defined earlier and cannot be defined later. The sequence of definition is of no concern.

Attribute:	**TimeSent(Transmission)**
Guide word	Interpretation
No	The transmission is not sent
More	The time of sending is greater than expected
Less	The time of sending is smaller than expected
As well as	Other attributes of Transmission are present in addition to TimeSent
Part of	The time of sending is only partially achieved
Reverse	The time of sending is reversed
Other than	The time of sending is replaced by different concept
Early	The transmission is sent early
Late	The transmission is sent late
Before	The transmission is sent early in sequence
After	The transmission is sent late in sequence
Faster	The time of sending is measured faster than expected
Slower	The time of sending is measured slower than expected

Comments on the formed HAZOP sentences:

As well as Other attributes of the Transmission will be present in addition to the TimeSent. Even if they interfere with the sending of the Transmission the value of TimeSent would remain computable.

Part of The TimeSent is the value for the time at which the Transmission is completely relayed from the NIC to the Wiring. This value can either be computed or not. Intermediate values are not possible.

Reverse The reversal in the computation of the value would lead either to "No TimeSent" or an invalid value for the TimeSent. It is assumed, that the computation of the value for TimeSent is done without systematic error.

Other than The value for TimeSent is required and cannot be replaced by different concept.

Faster, slower Under the assumption, that TimeSent can be computed instantaneously, the speed of computation is not relevant.

Attribute:	**TimeReceived(Transmission)**
Guide word	Interpretation
No	The transmission is not received
More	The time of reception is greater than expected
Less	The time of reception is smaller than expected

Guide word	Interpretation
As well as	Other attributes of Transmission are present in addition to TimeReceived
Part of	The time of reception is only partially achieved
Reverse	The time of reception is reversed
Other than	The time of reception is replaced by different concept
Early	The transmission is received early
Late	The transmission is received late
Before	The transmission is received early in sequence
After	The transmission is received late in sequence
Faster	The time of reception is measured faster than expected
Slower	The time of reception is measured slower than expected

Comments on the formed HAZOP sentences:

As well as Other attributes of the Transmission will be present in addition to the TimeReceived. Even if the interfere with the sending of the Transmission the value of TimeReceived would remain computable.

Part of The TimeReceived is the value for the time at which the Transmission is completely relayed from the Wiring to the NIC. This value can either be computed or not. Intermediate values are not possible.

Reverse The reversal in the computation of the value would lead either to "No TimeReceived" or an invalid value for the TimeReceived. It is assumed, that the computation of the value for TimeReceived is done without systematic error.

Other than The value for TimeReceived is required and cannot be replaced by different concept.

Faster, slower Under the assumption, that TimeReceived can be computed instantaneously, the speed of computation is not relevant.

Attribute:	**TransferRate(Transmission)**
Guide word	Interpretation
No	The Transmission has no transfer rate
More	The transfer rate is greater than expected
Less	The transfer rate is smaller than expected
As well as	Other attributes of Transmission are present in addition to TransferRate
Part of	The transfer rate is only partially achieved
Reverse	The transfer rate is reversed
Other than	The transfer rate is replaced by different concept
Early	The transfer rate is measured early
Late	The transfer rate is measured late
Before	The transfer rate is measured early in sequence
After	The transfer rate is measured late in sequence
Faster	The transfer rate is faster than expected
Slower	The transfer rate is slower than expected

Comments on the formed HAZOP sentences:

No If the information is transmitted a TransferRate can be computed. If this is not the case, the resulting deviation is identified with "No Transmission".

As well as Other attributes of the Transmission will be present in addition to the TransferRate. Even if the interfere with the sending of the Transmission the value of TransferRate would remain computable.

Reverse The reversal in the computation of the value would lead either to "No TransferRate" or an invalid value for the TransferRate. It is assumed, that the computation of the value for TransferRate is done without systematic error.

Other than The value for TransferRate is required and cannot be replaced by different concept.

Early, late, before, after Assuming that the computation of the value can be done instantaneously, timing cannot influence the attribute.

ATTRIBUTE:	**RequiredJitter(Transmission)**
GUIDE WORD	INTERPRETATION
No	No requirement for jitter defined
More	Value required for jitter greater than needed
Less	Value required for jitter smaller than needed
As well as	Other requirements of Transmission in addition to RequiredJitter present
Part of	Value required for jitter only partially achieved
Reverse	Value required for jitter is reversed
Other than	Jitter requirement is replaced by different concept
Early	Jitter requirement is defined early
Late	Jitter requirement is defined late
Before	Jitter requirement is defined early in sequence
After	Jitter requirement is defined late in sequence
Faster	Jitter requirement is defined faster than expected
Slower	Jitter requirement is defined slower than expected

Comments on the formed HAZOP sentences:

No The maximal value allowed for the jitter of a transmission is required for the system design. It is assumed to be defined.

Less The requiring of a smaller than needed value for jitter would result in the wasting of resources. This does not threaten the systems function.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Reverse The RequiredJitter is the definition of a value for the maximal allowed value of a transmissions' jitter. This definition may be incorrect but cannot be reversed.

Other than The value for RequiredJitter is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The RequiredJitter has to be defined at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredLatency(Transmission)**
Guide word	Interpretation
No	No requirement for latency defined
More	Value required for latency is greater than needed
Less	Value required for latency is smaller than needed
As well as	Other requirements of Transmission in addition to RequiredLatency present
Part of	Value required for latency is only partially achieved
Reverse	Value required for latency is reversed
Other than	Latency requirement is replaced by different concept
Early	Latency requirement is defined early
Late	Latency requirement is defined late
Before	Latency requirement is defined early in sequence
After	Latency requirement is defined late in sequence
Faster	Latency requirement is defined faster than expected
Slower	Latency requirement is defined slower than expected

Comments on the formed HAZOP sentences:

No The maximal value allowed for the latency of a transmission is required for the system design. It is assumed to be defined.

Less The requiring of a smaller than needed value for latency would result in the wasting of resources. This does not threaten the systems function.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Reverse The RequiredLatency is the definition of a value for the maximal allowed value of a transmissions' latency. This definition may be incorrect but cannot be reversed.

Other than The value for RequiredLatency is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The RequiredLatency has to be defined at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredMode(Transmission)**
Guide word	Interpretation
No	No requirement for transmission mode defined
More	Required mode of transmission is greater than needed
Less	Required mode of transmission is smaller than needed
As well as	Other attributes of Transmission present in addition to RequiredMode
Part of	The mode requirement of transmission is only partially achieved
Reverse	The mode requirement of transmission is reversed

Guide word	Interpretation
Other than	The mode requirement of transmission is replaced by a different concept
Early	Mode requirement defined early
Late	Mode requirement defined late
Before	Mode requirement defined early in sequence
After	Mode requirement defined late in sequence
Faster	Mode requirement of transmission is faster than in reality
Slower	Mode requirement of transmission is slower than in reality

Comments on the formed HAZOP sentences:

No The mode used for the Transmission is required for the system design. It is assumed to be defined.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Part of The requirement has to be defined or not. Intermediate values are not possible.

Other than The value for RequiredMode is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The requirement for the mode of transmission has to be defined at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredPeriod(Transmission)**
Guide word	Interpretation
No	No requirement for transmission period is defined
More	Required frequency of transmission is greater than needed
Less	Required frequency of transmission is smaller than needed
As well as	Other attributes of Transmission present in addition to Required-Period
Part of	The period requirement of transmission is only partially achieved
Reverse	The period requirement of transmission is reversed
Other than	The period requirement of transmission is replaced by different concept
Early	Period requirement defined early
Late	Period requirement defined late
Before	Period requirement defined early in sequence
After	Period requirement defined late in sequence
Faster	Period requirement of transmission is faster than in reality
Slower	Period requirement of transmission is slower than in reality

Comments on the formed HAZOP sentences:

No The period suspected for the Transmission is required for the system design. It is assumed to be defined.

More, faster If the suspected frequency of the Transmission is greater than the frequency met in reality, resources are wasted. This does not threaten the function of the system.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Reverse The requirement has to be defined. A reversal could result in an incorrect value. It is assumed, that incorrect requirements are identified and corrected.

Other than The value for RequiredPeriod is needed and cannot be replaced by different concept.

Early, late, before, after The requirement for the frequency of transmission has to be defined at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredSequence(Transmission)**
Guide word	Interpretation
No	No requirement for sequence is defined
More	Required sequence of transmission is more elaborated than needed
Less	Required sequence of transmission is less elaborated than needed
As well as	Other attributes of Transmission present in addition to Required-Sequence
Part of	Sequence requirement only partially achieved
Reverse	Sequence requirement is reversed
Other than	Sequence requirement is replaced by different concept
Early	Sequence requirement is defined early
Late	Sequence requirement is defined late
Before	Sequence requirement is defined early in sequence
After	Sequence requirement is defined late in sequence
Faster	Sequence requirement is defined faster than expected
Slower	Sequence requirement is defined slower than expected

Comments on the formed HAZOP sentences:

No In the case of event-triggered transmission the missing of a defined sequence is typical and cannot be a deviation. In the case of time-triggered transmission a defined sequence is required and can be assumed to be defined.

More If the required sequence of the Transmission is more elaborated than needed, resources are wasted. This does not threaten the function of the system.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Part of The sequence requirement can either be achieved or not. Intermediates are not possible.

Other than The sequence of the Transmission is needed for time-triggered communication and cannot be replaced by different concept.

Early, late, before, after The definition of the sequence has to exist at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

ATTRIBUTE:	**RequiredSize(Transmission)**
GUIDE WORD	INTERPRETATION
No	No requirement for size of transmission is defined
More	The required size of the Transmission too large
Less	The required size of the Transmission too small
As well as	Other attributes of Transmission present in addition to RequiredSize
Part of	The required size of the Transmission is only partially achieved
Reverse	The required size of the Transmission is reversed
Other than	The required size of the Transmission is replaced by different concept
Early	Size requirement is defined early
Late	Size requirement is defined late
Before	Size requirement is defined early in sequence
After	Size requirement is defined late in sequence
Faster	Size requirement is defined too fast
Slower	Size requirement is defined too slow

Comments on the formed HAZOP sentences:

No The maximal value allowed for the size of a transmission is required for the system design. It is assumed to be defined.

More The requiring of a larger than needed value for the transmission size would result in the wasting of resources. This does not threaten the systems function.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Part of The maximal size of a transmission can either be achieved or not. Intermediate values are not possible. The partial transmission of information is identified with "Part of Transmission".

Reverse The maximal size of the Transmission is a definition. It may be incorrect but cannot be reversed.

Other than The maximal value for the size of the Transmission is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The maximal size of the Transmission has to be defined at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

ATTRIBUTE:	**RequiredTimeSent(Transmission)**
GUIDE WORD	INTERPRETATION
No	No maximal acceptable value of TimeSent(Transm.) can be derived
More	The maximal acceptable value of TimeSent(Transm.) is too large
Less	The maximal acceptable value of TimeSent(Transm.) is too small
As well as	Other attributes of Transmission present in addition to RequiredTimeSent
Part of	The maximal acceptable value of TimeSent(Transm.) is only partially achieved

Guide word	Interpretation
Reverse	The maximal acceptable value of TimeSent(Transm.) is reversed
Other than	The maximal acceptable value of TimeSent(Transm.) is replaced by different concept
Early	The maximal acceptable value of TimeSent(Transm.) is derived early
Late	The maximal acceptable value of TimeSent(Transm.) is derived late
Before	The maximal acceptable value of TimeSent(Transm.) is derived early in sequence
After	The maximal acceptable value of TimeSent(Transm.) is derived late in sequence
Faster	The maximal acceptable value of TimeSent(Transm.) is derived faster than expected
Slower	The maximal acceptable value of TimeSent(Transm.) is derived slower than expected

Comments on the formed HAZOP sentences:

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Part of The maximal acceptable value for TimeSent can either be achieved or not. Intermediate values are not possible.

Reverse The maximal acceptable value for TimeSent is a definition. It may be incorrect but cannot be reversed.

Other than The maximal acceptable value for TimeSent is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The maximal acceptable value for TimeSent has to exist at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredTimeReceived(Transmission)**
Guide word	Interpretation
No	No maximal acceptable value of TimeReceived(Transm.) can be derived
More	The maximal acceptable value of TimeReceived(Transm.) is too large
Less	The maximal acceptable value of TimeReceived(Transm.) is too small
As well as	Other attributes of Transmission are present in addition to RequiredTimeReceived
Part of	The maximal acceptable value of TimeReceived(Transm.) is only partially achieved
Reverse	The maximal acceptable value of TimeReceived(Transm.) is reversed
Other than	The maximal acceptable value of TimeReceived(Transm.) is replaced by different concept

Guide word	Interpretation
Early	The maximal acceptable value of TimeReceived(Transm.) is derived early
Late	The maximal acceptable value of TimeReceived(Transm.) is derived late
Before	The maximal acceptable value of TimeReceived(Transm.) is derived early in sequence
After	The maximal acceptable value of TimeReceived(Transm.) is derived late in sequence
Faster	The maximal acceptable value of TimeReceived(Transm.) is derived faster than expected
Slower	The maximal acceptable value of TimeReceived(Transm.) is derived slower than expected

Comments on the formed HAZOP sentences:

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Part of The maximal acceptable value for TimeReceived can either be achieved or not. Intermediate values are not possible.

Reverse The maximal acceptable value for TimeReceived is a definition. It may be incorrect but cannot be reversed.

Other than The maximal acceptable value for TimeReceived is needed and cannot be replaced by different concept.

Early, late, before, after, faster, slower The maximal acceptable value for TimeReceived has to exist at the time of its use. It will have been defined earlier and cannot be defined later. The sequence or speed of definition is of no concern.

Attribute:	**RequiredTransferRate(Transmission)**
Guide word	Interpretation
No	The value acceptable for the TransferRate(Transm.) is not defined
More	The value acceptable for the TransferRate(Transm.) is too large
Less	The value acceptable for the TransferRate(Transm.) is too small
As well as	Other attributes of Transmission are present in addition to RequiredTransferRate
Part of	The value acceptable for the TransferRate(Transm.) is only partially achieved
Reverse	The value acceptable for the TransferRate(Transm.) is reversed
Other than	The value acceptable for the TransferRate(Transm.) is replaced by different concept
Early	The value acceptable for the TransferRate(Transm.) is defined early
Late	The value acceptable for the TransferRate(Transm.) is defined late
Before	The value acceptable for the TransferRate(Transm.) is defined early in sequence
After	The value acceptable for the TransferRate(Transm.) is defined late in sequence

Guide word	Interpretation
Faster	The value acceptable for the TransferRate(Transm.) is too fast
Slower	The value acceptable for the TransferRate(Transm.) is too slow

Comments on the formed HAZOP sentences:

No The value allowed for the TransferRate of a transmission is required for the system design. It is assumed to be defined.

More, part of The value acceptable for the TransferRate being too large is a waste of resources but no threat to the system.

As well as Other requirements of the Transmission will be present. It is assumed that the given requirements do not contradict each other.

Reverse The value allowed for the TransferRate of a transmission is fixed in the definition. It may be incorrect but cannot be reversed.

Other than The value allowed for the TransferRate of the Transmission is needed and cannot be replaced by different concept.

Early, late, before, after The value allowed for the TransferRate of the Transmission has to be defined at the time of its use. It can have been defined earlier and cannot be defined later. The sequence of definition is of no concern.

Attribute:	**NodeCount(Network)**
Guide word	Interpretation
No	No nodes connected to the Wiring
More	The count of nodes is too large
Less	The count of nodes is too small
As well as	Other attributes of Network present in addition to NodeCount
Part of	The count of nodes is only partially achieved
Reverse	The count of nodes is reversed
Other than	The count of nodes is replaced by different concept
Early	The count of nodes is computed early
Late	The count of nodes is computed late
Before	The count of nodes is computed early in sequence
After	The count of nodes is computed late in sequence
Faster	The count of nodes is computed too fast
Slower	The count of nodes is computed too slow

Comments on the formed HAZOP sentences:

As well as Other attributes of the Network will be present. They can increase the count of nodes in the network but not interfere with the computation of the number.

Part of The count of nodes can be achieved or not. Intermediates are not possible.

Reverse It can be assumed, that the nodes will be counted without systematic failure in the counting process.

Other than The number of nodes in the network have to be counted. This concept cannot be replaced.

Early, late, before, after, faster, slower It is assumed, that the process of counting the nodes is done instantaneously. Timing and speed is of no concern in this case.

ATTRIBUTE:	**DesignNodeCount(Network)**
GUIDE WORD	INTERPRETATION
No	Network design does not specify count of nodes in network
More	The count of nodes used in network design is too large
Less	The count of nodes used in network design is too small
As well as	Other attributes of the Network present in addition to DesignNodeCount
Part of	The count of nodes used in network design is only partially achieved
Reverse	The count of nodes used in network design is reversed
Other than	The count of nodes used in network design is replaced by different concept
Early	The count of nodes used in network design is defined early
Late	The count of nodes used in network design is defined late
Before	The count of nodes used in network design is defined early in sequence
After	The count of nodes used in network design is defined late in sequence
Faster	The count of nodes used in network design is defined too fast
Slower	The count of nodes used in network design is defined too slow

Comments on the formed HAZOP sentences:

As well as Other attributes of the Network will be present. They can increase the count of nodes in the network but not interfere with the computation of the number.

Reverse The number of nodes required in the system definition cannot be reversed.

Other than The number of nodes required in the system definition is important for the setting of communication timing and sizes. It cannot be replaced.

Early, late, before, after, faster, slower The value allowed for the number of nodes in the Network has to be defined before it is used. It may have been defined earlier and cannot be defined later. The sequence and speed of definition is of no concern.

ATTRIBUTE:	**DataRate(Device)**
GUIDE WORD	INTERPRETATION
No	a. The device does not produce data
	b. No data rate can be computed for the device
More	The data rate of the device is too great
Less	The data rate of the device is too small
As well as	Other attributes of the Device present in addition to DataRate
Part of	The data rate of the device is only partially achieved
Reverse	The data rate of the device is reversed

Guide word	Interpretation
Other than	The data rate of the device is replaced by different concept
Early	The data rate of the device is computed early
Late	The data rate of the device is computed late
Before	The data rate of the device is computed early in sequence
After	The data rate of the device is computed late in sequence
Faster	The data rate of the device is too fast
Slower	The data rate of the device is too slow

Comments on the formed HAZOP sentences:

No (b) If the device produces data it can be assumed, that the data rate of the device can be computed.

As well as Other attributes of the Device will be present. They can only influence the value of the data rate but not interfere with its computation.

Reverse The data rate cannot be reversed, assuming that no systematic failures occur during the computation.

Other than The data rate cannot be replaced by a different concept.

Early, late, before, after It is assumed, that the computation of the data rate is done instantaneously. In this case timing is of no concern.

Attribute:	**Interference(Network, Universe)**
Guide word	Interpretation
No	No interference between Universe and Network occurs
More	The interference between Universe and Network is bigger than expected
Less	The interference between Universe and Network is smaller than expected
As well as	Other relation between Universe and Network is present in addition to Interference
Part of	The interference between Universe and Network is only partially achieved
Reverse	The interference between Universe and Network is reversed
Other than	The interference between Universe and Network is replaced by different concept
Early	The interference between Universe and Network occurs early
Late	The interference between Universe and Network occurs late
Before	The interference between Universe and Network occurs early in sequence
After	The interference between Universe and Network occurs late in sequence
Faster	The interference between Universe and Network occurs too fast
Slower	The interference between Universe and Network occurs too slow

Comments on the formed HAZOP sentences:

No No interference between Universe and Network would be the ideal function and not a deviation.

Less If the interference is smaller than expected, resources are wasted but the system is not concerned.

As well as Other relations between the Universe and the Network may be present but can only vary the value of the interference.

Early, late, before, after, faster, slower For the interference between Universe and Network the only important question is if the interference occurs at one point in time. Whether it was present before or after is of no concern, neither is a speed in which the interference might occur.

A.3 HAZOP sentences of system - 3^{rd} Iteration

Attribute:	**FailureRate(NIC)**
Guide word	Interpretation
No	No FailureRate for the NIC is known
More	The FailureRate for the NIC is bigger than acceptable
Less	The FailureRate for the NIC is lower than required
As well as	Other attributes in addition to FailureRate(NIC) are present
Part of	The FailureRate is only partially known
Reverse	The FailureRate is reversed
Other than	The FailureRate is replaced by different concept
Early	The FailureRate was determined early
Late	The FailureRate was determined late
Before	The FailureRate was determined early in sequence
After	The FailureRate was determined late in sequence
Faster	The FailureRate is bigger than acceptable
Slower	The FailureRate is lower than required

Comments on the formed HAZOP sentences:

No The FailureRate of a NIC has to be known for the NIC to be integrated into the system. It is assumed, that this condition is true for the NIC used.

Less, slower A NIC with a FailureRate lower than required is wanted for the proper operation of the system.

As well as Other attributes of NIC will be present in addition to the FailureRate. They can influence the FailureRate but only in value not in any function.

Part of This leads to a experienced FailureRate either higher or lower than the proposed FailureRate. These deviations are identified by "More FailureRate" and "Less FailureRate"

Reverse The FailureRate is a value given for the chance of a device not to deliver its function. A reversal would lead to a value either higher or lower than the required value. It is assumed that a quality conformance test will guard against systematic mistakes in the estimation of the FailureRate.

Other than The FailureRate is required for the system development and cannot be replaced by a different concept.

Early, late, before, after It is important that the FailureRate of the NIC used in the system meets the requirements. The time when this FailureRate was estimated is not relevant as quality conformance tests will verify the actual FailureRate.

Faster This deviation is identical with "More FailureRate(NIC)".

Attribute:	**PowerRating(NIC)**
Guide word	Interpretation
No	No PowerRating for the NIC is known
More	The PowerRating for the NIC is bigger than required
Less	The PowerRating for the NIC is lower than needed

Guide word	Interpretation
As well as	Other attributes of NIC are present in addition to PowerRating
Part of	The PowerRating is only partially achieved
Reverse	The PowerRating is reversed
Other than	The PowerRating is replaced by different concept
Early	The PowerRating is determined early
Late	The PowerRating is determined late
Before	The PowerRating is determined early in sequence
After	The PowerRating is determined late in sequence
Faster	The PowerRating is reached faster than expected
Slower	The PowerRating is reached slower than expected

Comments on the formed HAZOP sentences:

No It is assumed, that a value for the maximal applicable current and voltage a NIC can process is known e.g. by the manufacturer or the specification.

More If the actual Load a NIC can process is bigger than the requirement, this is a potential decrease in the FailureRate of the NIC and welcome feature.

As well as Other attributes of the NIC will be present in addition to the PowerRating. As the PowerRating is an index for the NIC any possible influence by other attributes will have been integrated into its value.

Reverse, other than The PowerRating is an index for the NIC. This value cannot be reversed or replaced.

Early, late, before, after The only important issue regarding the determination of the PowerRating of a NIC is that a value for the PowerRating is identified. The timing or sequence of this process is not relevant.

Faster, slower The PowerRating is an index of the NIC. It is assumed that this value is not variable.

Attribute:	**Design(NIC)**
Guide word	Interpretation
No	The NIC has no design
More	The Design of the NIC is more elaborated than needed
Less	The Design of the NIC is less elaborated than needed
As well as	Other attributes of the NIC are present in addition to the Design
Part of	The Design of the NIC was only partially realised
Reverse	The Design of the NIC is reversed
Other than	The Design of the NIC is replaced by a different concept
Early	The Design is less elaborated than needed
Late	The Design is more elaborated than needed
Before	The Design was made early in sequence
After	The Design was made late in sequence
Faster	The Design was made faster than expected
Slower	The Design was made slower than expected

Comments on the formed HAZOP sentences:

No, other than Without a design the NIC could not have been constructed.

More, Late As long as the Design of the NIC includes all factors relevant for the system, additional features pose no threat to the system.

As well as Other attributes of the NIC will be present. It is assumed that they do not contradict the design.

Reverse The design will be fixed for the NIC used. It cannot be reversed.

Before, after, faster, slower The timing and speed of the definition the design was made by is not relevant for the system.

Early This deviation is identical with "Less Design(NIC)"

Attribute:	**Design(Wiring)**
Guide word	Interpretation
No	Wiring has no design
More	The Design of the Wiring is more elaborated than needed
Less	The Design of the Wiring is less elaborated than needed
As well as	Other attributes of the Wiring are present in addition to the Design
Part of	The Design of the Wiring was only partially realised
Reverse	The Design of the Wiring is reversed
Other than	The Design of the Wiring is replaced by a different concept
Early	The Design is less elaborated than needed
Late	The Design is more elaborated than needed
Before	The Design was made early in sequence
After	The Design was made late in sequence
Faster	The Design was made faster than expected
Slower	The Design was made slower than expected

Comments on the formed HAZOP sentences:

No, other than Without a design the Wiring could not have been constructed.

More, Late As long as the Design of the Wiring includes all factors relevant for the system, additional features pose no threat to the system.

As well as Other attributes of the Wiring will be present. It is assumed that they do not contradict the design.

Reverse The design will be fixed for the Wiring used. It cannot be reversed.

Before, after, faster, slower The timing and speed of the definition the design was made by is not relevant for the system.

Early This deviation is identical with "Less Design(Wiring)"

Attribute:	**FailureRate(Wiring)**
Guide word	Interpretation
No	No FailureRate for the Wiring is known
More	The FailureRate for the Wiring is too high
Less	The FailureRate for the Wiring is too low
As well as	Other attributes of the Wiring are present in addition to the FailureRate
Part of	The FailureRate is only partially known
Reverse	The FailureRate is reversed
Other than	The FailureRate is replaced by a different concept
Early	The FailureRate is determined early
Late	The FailureRate is determined late
Before	The FailureRate is determined early in sequence
After	The FailureRate is determined late in sequence
Faster	The FailureRate is bigger than acceptable
Slower	The FailureRate is smaller than required

Comments on the formed HAZOP sentences:

No The FailureRate of the Wiring has to be known for the Wiring to be integrated into the system. It is assumed, that this condition is true for the Wiring used.

Less, slower If the FailureRate of the Wiring is lower than required the proper operation of the system is not influenced.

As well as Other attributes of Wiring will be present in addition to the FailureRate. They can influence the FailureRate but only in value not in function.

Part of This leads to a experienced FailureRate either higher or lower than the proposed FailureRate. These deviations are identified by ”More FailureRate” and ”Less FailureRate”

Reverse The FailureRate is a value given for the chance of a device not to deliver its function. A reversal would lead to a value either higher or lower than the required value. It is assumed that a quality conformance test will guard against systematic mistakes in the estimation of the FailureRate.

Other than The FailureRate is required for the system development and cannot be replaced by a different concept.

Early, late, before, after It is important that the FailureRate of the Wiring used in the system meets the requirements. The time when this FailureRate was estimated is not relevant as quality conformance tests will verify the actual FailureRate.

Faster This deviation is identical with ”More FailureRate(Wiring)”.

Attribute:	**Overhead(Transmission)**
Guide word	Interpretation
No	The Transmission is done without Overhead
More	The Overhead of the Transmission is bigger than acceptable
Less	The Overhead of the Transmission is smaller than expected
As well as	Other attributes of Transmission are present in addition to the Overhead
Part of	The Overhead of the Transmission is only partially achieved

Guide word	Interpretation
Reverse	The Overhead of the Transmission is reversed
Other than	The Overhead is replaced by a different concept
Early	The Overhead of the Transmission occurs early
Late	The Overhead of the Transmission occurs late
Before	The Overhead of the Transmission occurs early in sequence
After	The Overhead of the Transmission occurs late in sequence
Faster	The Overhead occurs faster than expected
Slower	The Overhead occurs slower than expected

Comments on the formed HAZOP sentences:

No A value for the Overhead of the Transmission can always be identified. Its minimal value is 0.

Less, part of If the Overhead of the Transmission would be lower than the expected value this would not influence the operation of the system as long as the Transmission is done without error.

As well as Other attributes of the Transmission will be present. If they influence the Overhead of the Transmission, it would lead to the deviation of an invalid Transmission which was already identified.

Reverse A reversal in the Overhead of a Transmission would render the Transmission invalid. This deviation is already identified.

Other than The determination of the Overhead is a process that can be done for every kind of communication. It cannot be replaced.

Early, late, before, after, faster, slower These deviations correspond directly with the deviations identified for the Transmission itself.

Attribute:	**Header(Transmission)**
Guide word	Interpretation
No	The Transmission is done without Header
More	The Header is bigger than expected
Less	The Header is smaller than expected
As well as	Other attributes of Transmission are present in addition to the Header
Part of	The Header is only partially achieved
Reverse	The Header is reversed
Other than	The Header is replaced by a different concept
Early	The Header occurs early
Late	The Header occurs late
Before	The Header occurs early in sequence
After	The Header occurs late in sequence
Faster	The Header occurs faster than expected
Slower	The Header occurs slower than expected

Comments on the formed HAZOP sentences:

No, other than The Transmission without Header in a Network that does more than one way communication to only one Host, a header is required and cannot be omitted or replaced by a different concept as long as the Transmission is not corrupted.

More, less, part of The header of a transmission has a fixed size. If this size would be varied the Transmission would be corrupted, which is already identified.

As well as Other attributes of the Transmission will be present. If they influence the Header of the transmission the Transmission would be corrupted, which is already identified.

Reverse If the Header is reversed the Transmission would be corrupted.

Early, late, before, after, faster, slower These deviations correspond directly with the deviations identified for the Transmission itself.

ATTRIBUTE:	**Energy(Transmission)**
GUIDE WORD	INTERPRETATION
No	The Transmission is done without Energy involved
More	The Energy of the Transmission is bigger than expected
Less	The Energy of the Transmission is smaller than expected
As well as	Other attributes of the Transmission are present in addition to the Energy
Part of	The Energy is only partially achieved
Reverse	The Energy is reversed
Other than	The Energy is replaced by a different concept
Early	The Energy is measured early
Late	The Energy is measured late
Before	The Energy is measured early in sequence
After	The Energy is measured late in sequence
Faster	The Energy is measured faster than expected
Slower	The Energy is measured slower than expected

Comments on the formed HAZOP sentences:

No This is identical with "No Transmission" as the Transmission cannot be done without use of Energy.

As well as Other attributes of the Transmission will be present. They can only influence the value of the Energy but not its function.

Other than The transmission of information utilises Energy. The concept of Energy cannot be replaced.

Early, late, before, after, faster, slower It is assumed, that the Energy used for the Transmission can be measured instantaneously.

ATTRIBUTE:	**Shielding(Network)**
GUIDE WORD	INTERPRETATION
No	The Network has no Shielding
More	The Shielding is more elaborated than needed

Guide word	Interpretation
Less	The Shielding is less elaborated than needed
As well as	Other attributes of the Network are present in addition to the Shielding
Part of	The Shielding is only partially achieved
Reverse	The Shielding is reversed
Other than	The Shielding is replaced by a different concept
Early	The Shielding occurs early
Late	The Shielding occurs late
Before	The Shielding occurs early in sequence
After	The Shielding occurs late in sequence
Faster	The Shielding occurs faster than expected
Slower	The Shielding occurs slower than expected

Comments on the formed HAZOP sentences:

More If the shielding of the Network is more elaborate than needed, the Network is protected against all identified Influences and additional Influences. The required function is ensured.

As well as Other attributes of the Network will be present. It is assumed, that the do not influence the functionality of the Shielding.

Reverse A reversal of the function of the Shielding would be equal with "No Shielding".

Other than Influencing factors from outside will have to be mitigated. This function is fulfilled by the Shielding. The facilities of the Shielding may be replaced, but not their function.

Early, late, before, after, faster, slower The only important question regarding the Shielding is the implementation of its function. The timing, sequence or speed the implementation is done by, is of no concern.

Attribute:	**EmissionRegulation(Network)**
Guide word	Interpretation
No	No regulations concerning emissions are available
More	The regulations are more elaborated than needed
Less	The regulations are less elaborated than needed
As well as	Other attributes of the Network are present in addition to the EmissionRegulation
Part of	The regulations are only partially achieved
Reverse	The regulations are reversed
Other than	The regulations are replaced by a different concept
Early	The regulations are applied early
Late	The regulations are applied late
Before	The regulations are applied early in sequence
After	The regulations are applied late in sequence
Faster	The regulations are applied faster than expected
Slower	The regulations are applied slower than expected

Comments on the formed HAZOP sentences:

No If no regulations are made concerning the emission no limit value has to be maintained.

More Regulations more elaborated than needed have to be met. This does not change the procedure.

Less If the regulations are less elaborated than needed, the demanded parts of the regulations have to be met and additional parts can be implemented freely.

As well as Other attributes of the Network will be present. They cannot influence the regulations.

Reverse Reversed regulations are regulations nevertheless.

Other than Regulations can be defined or not. A replacement of the concept is not possible.

Early, late, before, after, faster, slower The important question regarding the regulations is the compliance of the system with them. The timing, sequence or speed of an application of the regulations to the system is not relevant.

ATTRIBUTE:	**Load(Network)**
GUIDE WORD	INTERPRETATION
No	The Network has no Load
More	The Load of the Network is greater than expected
Less	The Load of the Network is smaller than expected
As well as	Other attributes of the Network in addition to the Load are present
Part of	The Load is only partially achieved
Reverse	The Load is reversed
Other than	The Load of the Network is replaced by a different concept
Early	The Load of the Network is measured early
Late	The Load of the Network is measured late
Before	The Load of the Network is measured early in sequence
After	The Load of the Network is measured late in sequence
Faster	The Load of the Network is measured faster than expected
Slower	The Load of the Network is measured slower than expected

Comments on the formed HAZOP sentences:

No The Network can only have "No Load" if no information is transmitted. This is already identified.

Less If the Load of the Network is lower than expected the transmission of information is hindered less than expected. This is no threat to the system.

As well as Other attributes of the Network can only influence the value of the Load not its function.

Reverse, other than The Load is an index for the performance of the Network. It cannot be reversed or replaced.

Early, late, before, after, faster, slower It is assumed, that the value of the Load can be

measured instantaneously. In this case the timing, sequence or speed of measurement is not relevant.

Attribute:	**Design(Network)**
Guide word	Interpretation
No	The Network has no Design
More	The Design of the Network is more elaborated than needed
Less	The Design of the Network is less elaborated than needed
As well as	Other attributes of the Network in addition to the Design are present
Part of	The Design of the Network is only partially achieved
Reverse	The Design of the Network is reversed
Other than	The Design is replaced by a different concept
Early	The Design of the network is defined early
Late	The Design of the network is defined late
Before	The Design of the network is defined early in sequence
After	The Design of the network is defined late in sequence
Faster	The Design of the network is defined faster than expected
Slower	The Design of the network is defined slower than expected

Comments on the formed HAZOP sentences:

No, other than Without a design the Network could not have been constructed.

More As long as the Design of the Network includes all factors relevant for the system, additional features pose no threat to the system.

As well as Other attributes of the Network will be present. It is assumed that they do not contradict the design.

Reverse The design will be fixed for the Network used. It cannot be reversed.

Early, late, before, after, faster, slower The timing, sequence and speed of the definition the design was made by is not relevant for the system.

Attribute:	**Intact(Device)**
Guide word	Interpretation
No	The Device is not intact
More	The Device is more intact than needed
Less	The Device is less intact than needed
As well as	Other attributes of the Device are present in addition to Intact
Part of	The Device is only partially intact
Reverse	The Device is not intact
Other than	The concept of Intact is replaced by a different concept
Early	The Device is intact early
Late	The Device is intact late
Before	The Device is intact early in sequence
After	The Device is intact late in sequence
Faster	The Device is intact faster than expected
Slower	The Device is intact slower than expected

Comments on the formed HAZOP sentences:

More A device more than intact is still intact.

As well as Other attributes can only change the value of intact but not the status.

Reverse This deviation is identical to "No Intact(Device).

Other than The status of Intact(Device) cannot be replaced by a different concept.

Early, late, before, after, faster, slower As long as the status of Intact(Device) can be evaluated at the time it is used, the time, sequence or speed with which the status was reached is not important.

ATTRIBUTE:	**OutputEnergy(Device)**
GUIDE WORD	INTERPRETATION
No	The Device has no OutputEnergy
More	The OutputEnergy of the Device is bigger than expected
Less	The OutputEnergy of the Device is smaller than expected
As well as	Other attributes of the Device are present in addition to the OutputEnergy
Part of	The OutputEnergy is only partially achieved
Reverse	The OutputEnergy is reversed
Other than	The OutputEnergy is replaced by a different concept
Early	The OutputEnergy is measured early
Late	The OutputEnergy is measured late
Before	The OutputEnergy is measured early in sequence
After	The OutputEnergy is measured late in sequence
Faster	The OutputEnergy is measured faster than expected
Slower	The OutputEnergy is measured slower than expected

Comments on the formed HAZOP sentences:

As well as Other attributes can influence the value of the OutputEnergy but not the function. Changes in the value are identified with "More" and "Less".

Other than The concept of OutputEnergy cannot be replaced.

Early, late, before, after, faster, slower It is assumed, that the value of OutputEnergy can be measured instantaneously. Timing, sequence and speed are not relevant in this case.

ATTRIBUTE:	**Connection(NIC, Device)**
GUIDE WORD	INTERPRETATION
No	The Device is not connected to the NIC
More	More than one connection between NIC and Device exists
Less	Less connections between NIC and Device than expected exist
As well as	Other relations between NIC and Device are present in addition to the connection
Part of	The connection between NIC and Device are only partially achieved

Guide word	Interpretation
Reverse	The connection between NIC and Device is reversed
Other than	The connection between NIC and Device is replaced by a different concept
Early	The connection between NIC and Device is established early
Late	The connection between NIC and Device is established late
Before	The connection between NIC and Device is established early in sequence
After	The connection between NIC and Device is established late in sequence
Faster	The connection between NIC and Device works faster than expected
Slower	The connection between NIC and Device works slower than expected

Comments on the formed HAZOP sentences:

As well as Other relations between the NIC and the Device will be present. It is assumed, that they do not influence the concept of Connection(NIC, Device), at most its value.

Reverse If an existing connection is reversed it is separated. This deviation is identified with "No Connection".

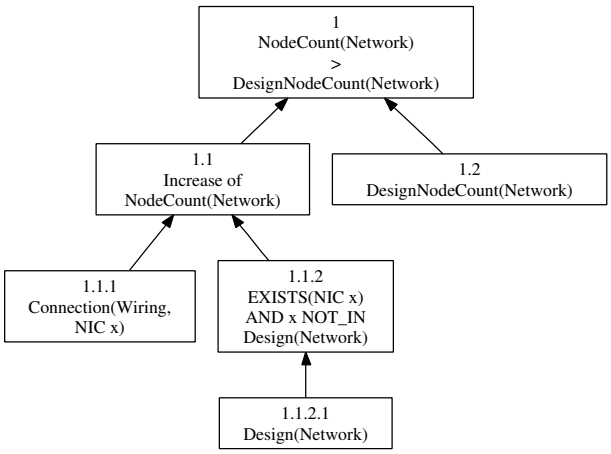
Other than The concept of Connection cannot be replaced.

Early, late, before, after If a connection between NIC and Device is established, the timing or sequence is of no concern. If no connection is established, this is already identified by "No Connection".

B Causal Influence Diagrams

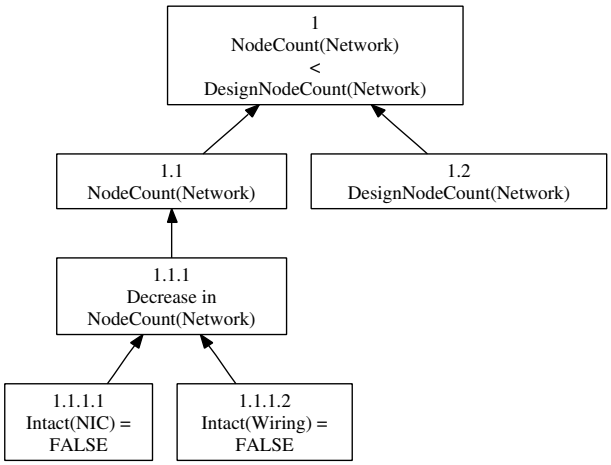
B.1 CIDs from 2^{nd} iteration

Deviation 1.a More NICs in system than expected



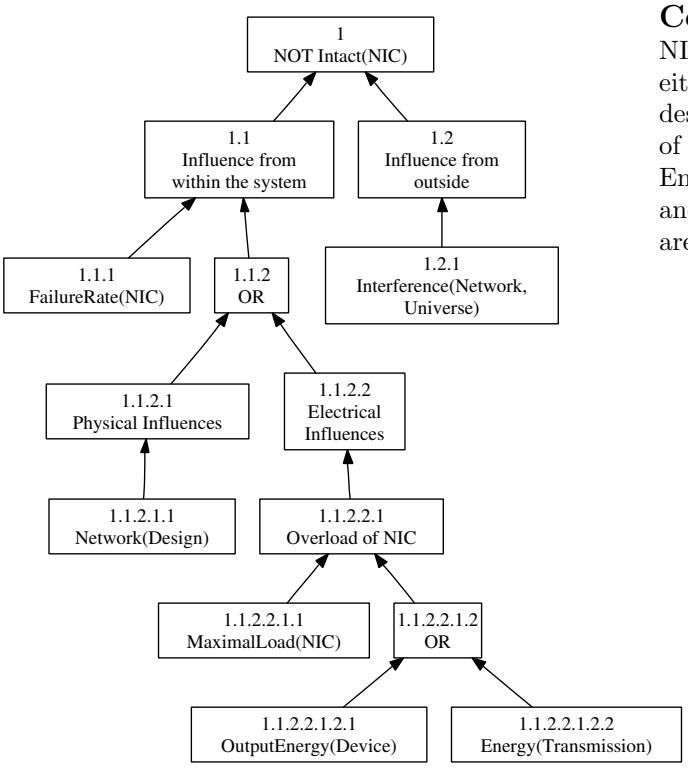
Comments: To be able to identify a NIC as an addition to the system the element Design(Network) has to be included in the ontology.

Deviation 1.b Less NICs in system than expected



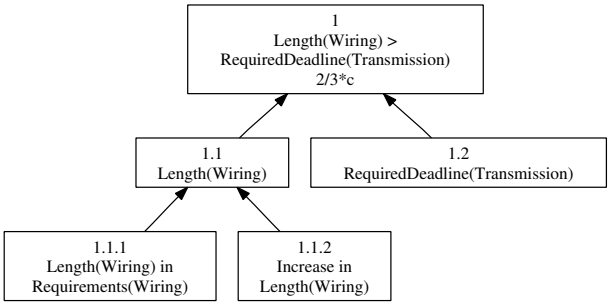
Comments: Less NICs in the system can be either caused by failure of a NIC or of the wiring. If 'expected' is interpretable as the Network's DesignNodeCount this value has to be defined. If 'expected' is interpreted as the number of nodes connected to the wiring at a given previous time, this value has to be taken. In both cases the number of nodes in the system will be a fixed value that cannot be influenced and therefore does not influence the probability of the deviation to occur.

Deviation 1.c A NIC is fragmented



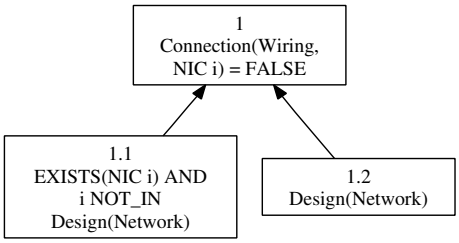
Comments: The event of the NIC not being intact can be caused either from within the system. To describe this deviation the elements of FailureRate(NIC), Energy(Wiring), Energy(Device), MaximalLoad(NIC) and ExternalInfluence(NIC, Universe) are needed.

Deviation 2.a Wiring is too long



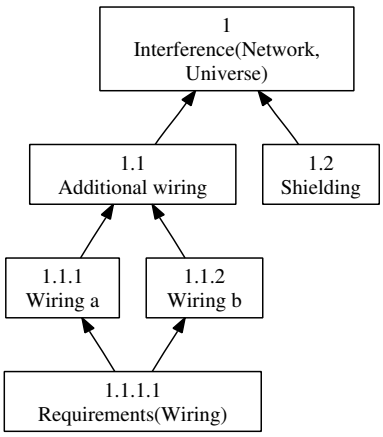
Comments: Too long wiring can either caused by the specification's RequiredDeadline being too low to be achievable or the actual length of the Wiring being too long. This can be caused either by the required Length of the Wiring being too great or the Wiring being elongated.

Deviation 2.b Wiring is too small



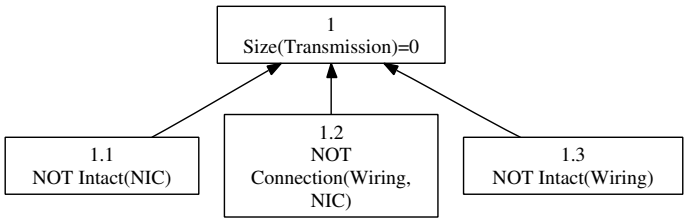
Comments: Deviation 2.b leads to not all NIC can be connected to the Network. Length(Wiring) is part of Design(Wiring). If Design(Wiring) allows for all intended NIC than follows, that either the unconnectable NIC is not intended or the Design is incomplete. Design(Network) has to be introduced in the ontology for the analysis' next iteration.

Deviation 2.c Other medium in addition to wiring present

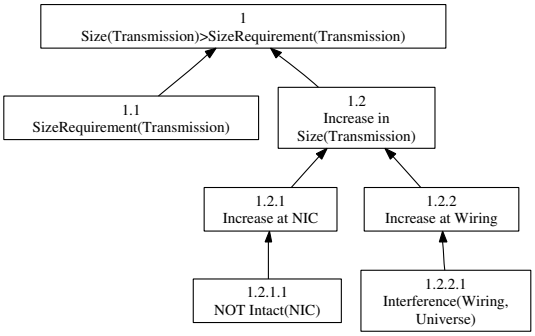


Comments: The actual deviation, the occurrence of *Additional Wiring*, can be explained by requirements of the system. Only in combination with another factor, e.g. lack of shielding, *Additional Wiring* can lead to a hazardous situation.

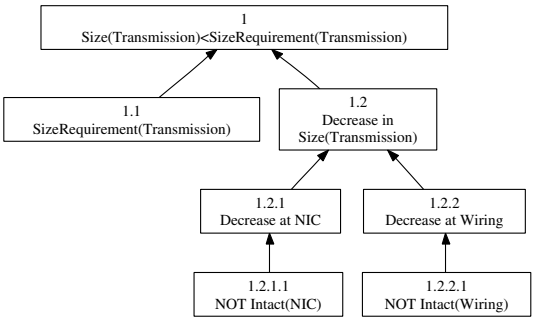
Deviation 3.a No information is transmitted



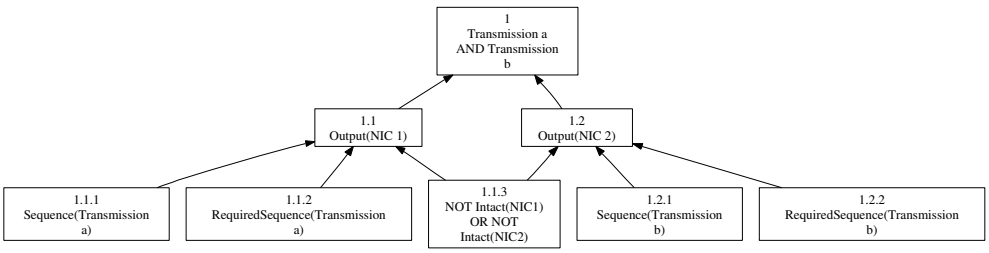
Deviation 3.b More information than intended is transmitted



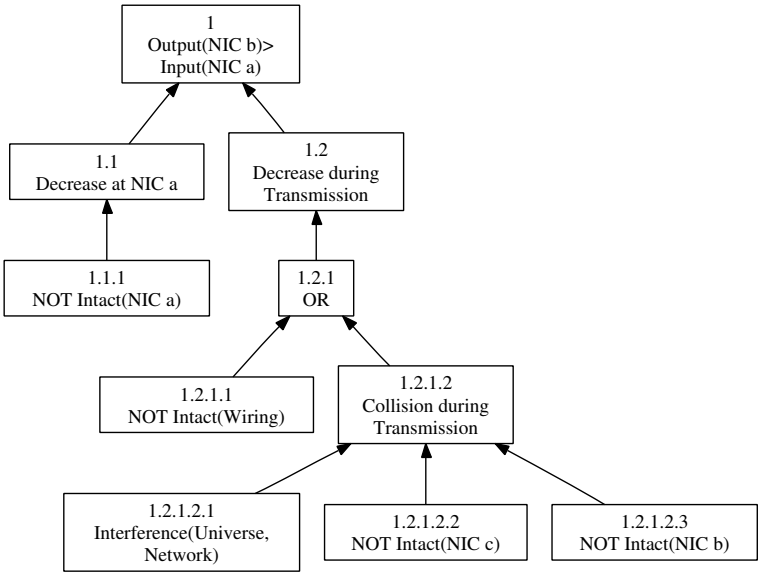
Deviation 3.c Less information than intended is transmitted



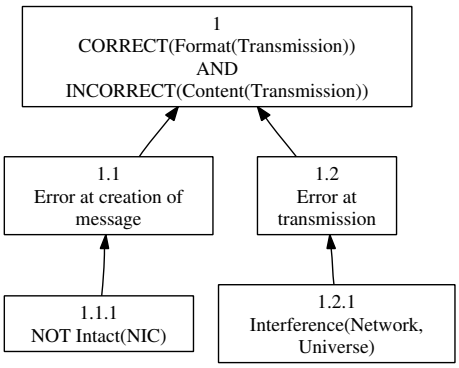
Deviation 3.d Additional information is transmitted



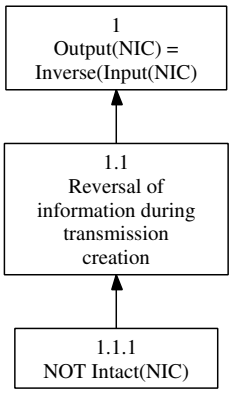
Deviation 3.e Information is only partially transmitted



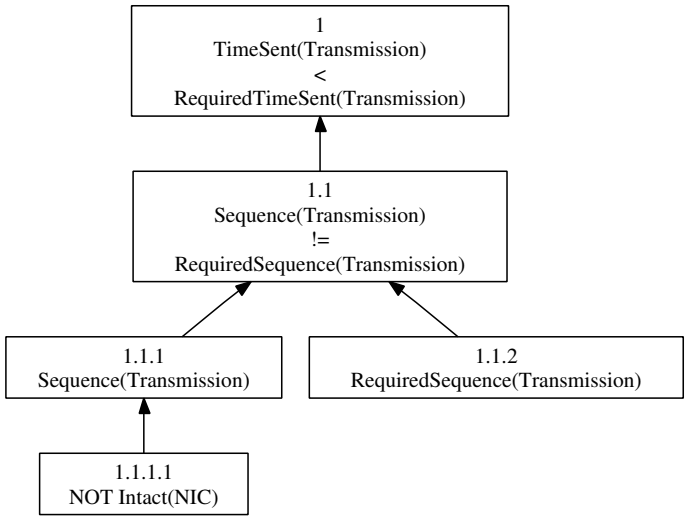
Deviation 3.f Information is well formed but carries wrong content



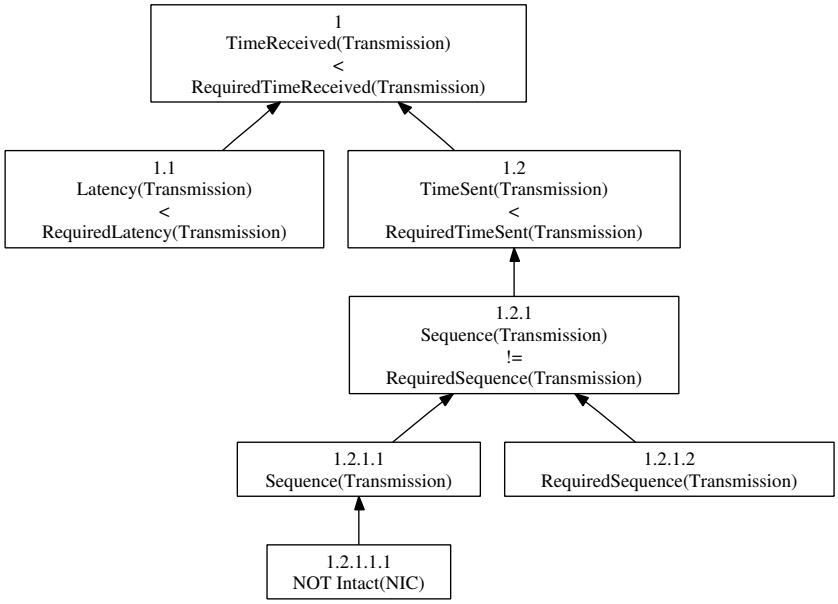
Deviation 3.g Information is reversely transmitted



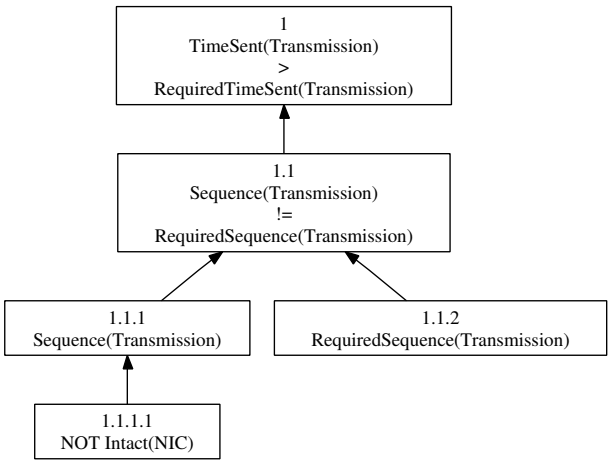
Deviation 3.h Information is sent too early



Deviation 3.i Information is received too early

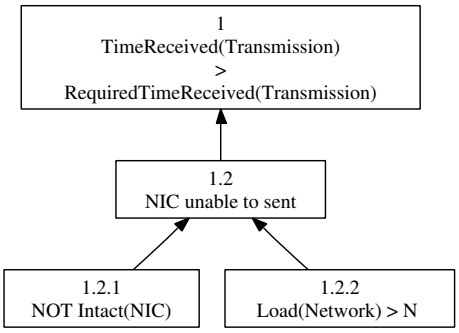


Deviation 3.j Information is sent too late



Comments: This CID is identical to the CID of deviation 3.h with the exemption of the deviation itself. 3.h and 3.j can therefore be fused by renaming the deviation into *TimeSent(Transmission) != RequiredTimeSent(Transmission).*

Deviation 3.k Information is received too late

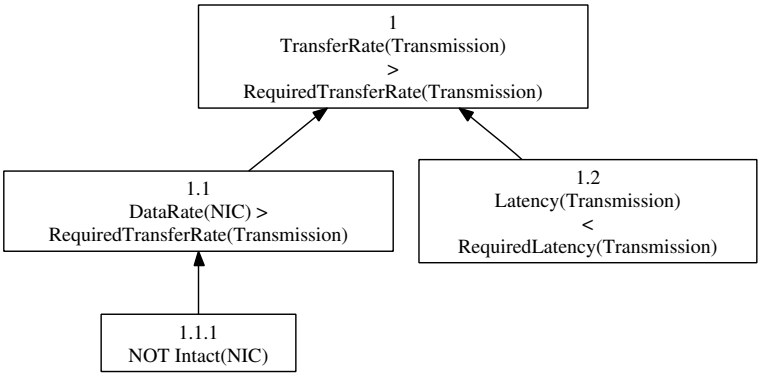


Comments: If the network load is greater than a critical value the transmission is delayed longer than allowed. The element Load(Network) has to be added to the ontology.

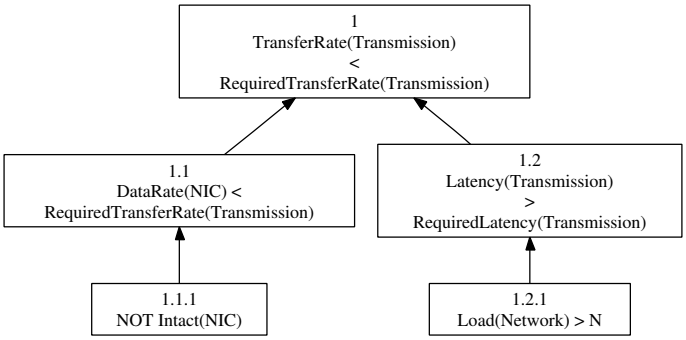
Deviation 3.l Information is sent ahead of sequence
Deviation 3.l is part of deviation 3.h.

Deviation 3.m Information is sent behind sequence
Deviation 3.m is part of deviation 3.h.

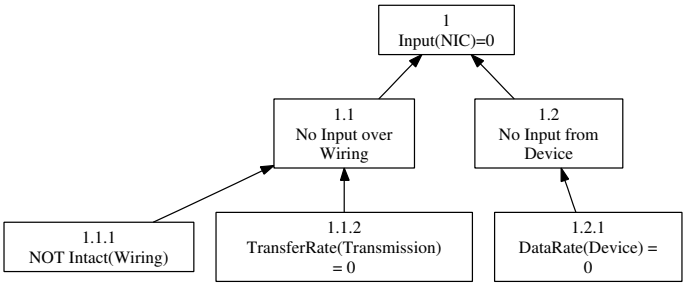
Deviation 3.n Transfer rate greater than intended



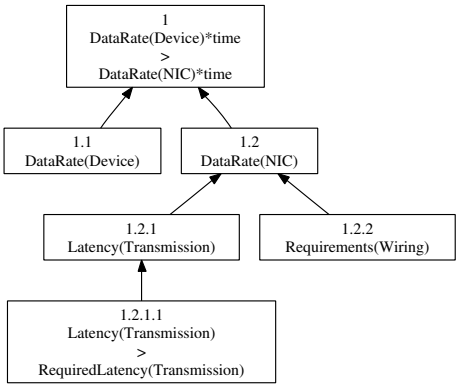
Deviation 3.o Transfer rate lower than intended



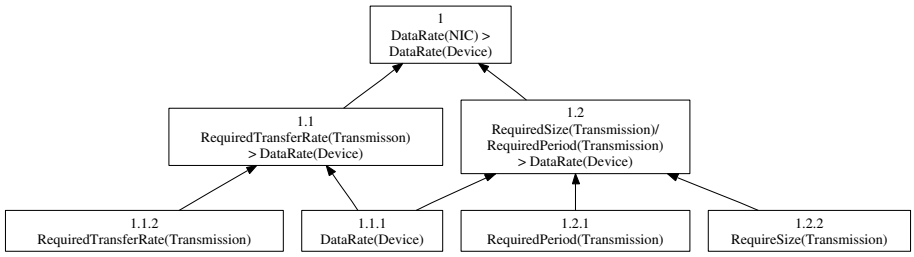
Deviation 4.a NIC does not get input



Deviation 4.b NIC receives more input from the device than expected



Deviation 4.c NIC receives more input from the network than expected



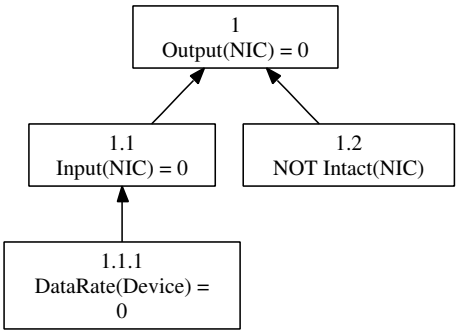
Deviation 4.d NIC receives input from more sources than intended
Deviation 4.d is identical with deviation 1.a.

Deviation 4.e NIC reverses received input
Deviation 4.e is identical with deviation 3.g.

Deviation 4.f NIC receives input early
Deviation 4.f is identical with deviation 3.i.

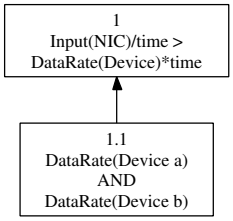
Deviation 4.g NIC receives input late
Deviation 4.g is identical with deviation 3.k.

Deviation 5.a NIC has no output

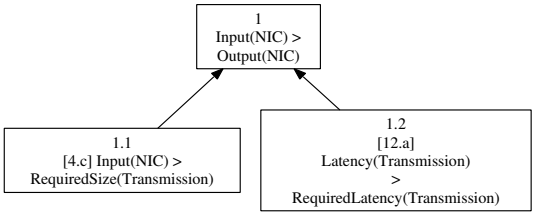


Deviation 5.b NIC has more output to the device than expected
Deviation 5.b is identical with deviation 3.b.

Deviation 5.c NIC has more data to transmit than expected

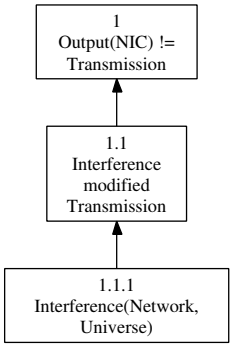


Deviation 5.d NIC transmits only part of the output



Deviation 5.e NIC transmits inverted output
Deviation 5.e is identical with deviation 3.g.

Deviation 5.f Output is replaced

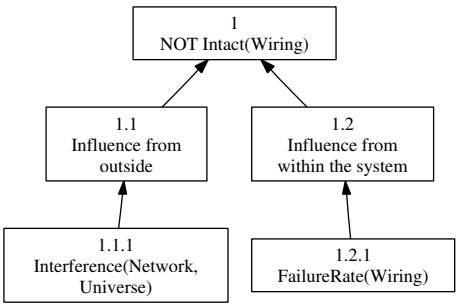


Deviation 5.g Output is sent early
Deviation 5.g is identical with deviation 3.h.

Deviation 5.h Output is sent late
Deviation 5.h is identical with deviation 3.j.

Deviation 6.a The NIC is not intact
Deviation 6.a is identical with deviation 1.c.

Deviation 7.a The wiring is not intact

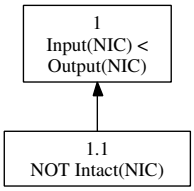


Comments: The event of the Wiring not being intact can be caused either from within the system. To describe this deviation the elements of FailureRate(NIC), Influence(Universe, Wiring) are needed.

Deviation 8.a Transmission has no size
Deviation 8.a is identical with deviation 3.a.

Deviation 8.b Transmitted information is bigger than sent message
Deviation 8.b is identical with deviation 4.c.

Deviation 8.c Transmitted information is smaller than sent message



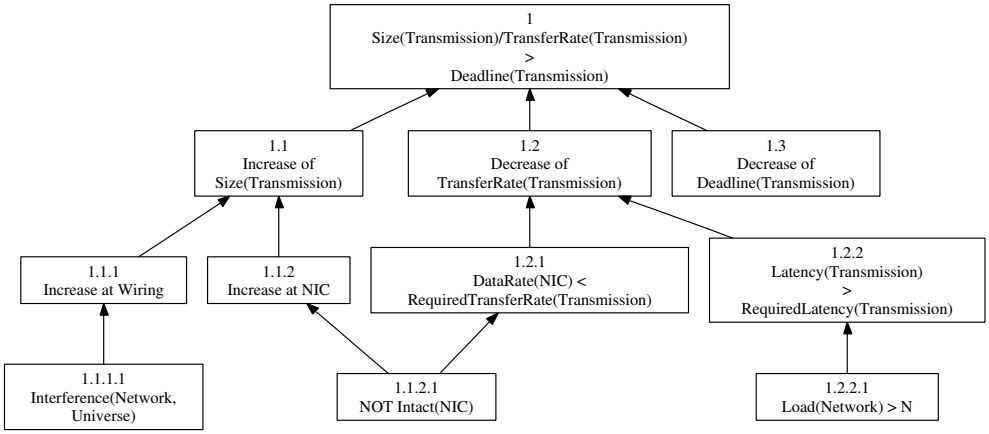
Comments: Input(NIC) includes all information received by the NIC, Output(NIC) all information that is transmitted by the NIC. A reduction in size of the transmission can only be caused by the NIC itself.

Deviation 8.e Additional transmission of content
Deviation 8.e is identical with deviation 8.d.

Deviation 8.f Only part of the information size is transmitted
Deviation 8.f is identical with deviation 5.d.

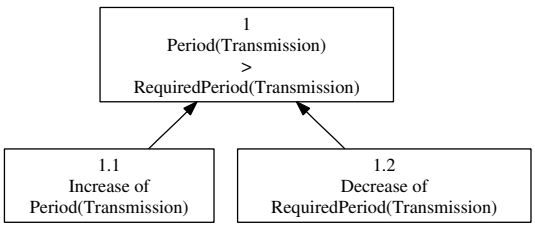
Deviation 9.a The information is not transmitted in time
Deviation 9.a is identical with deviation 3.k.

Deviation 9.b Deadline value is too small

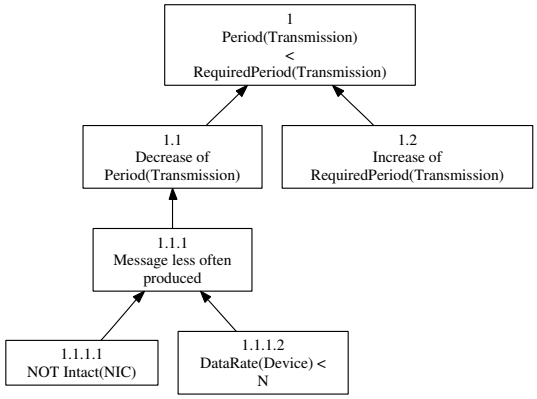


Comments: This deviation can be caused by an increase of the Size(Transmission), which is identified in deviation 3.b, an decrease of the TransferRate(Transmission), which is identified in deviation 3.o or an decrease in the Deadline(Transmission). As it does not seem possible to influence the Deadline(Transmission) only the decrease itself is included in the graph without further causes.

Deviation 10.a A class of transmission occurs more often than defined

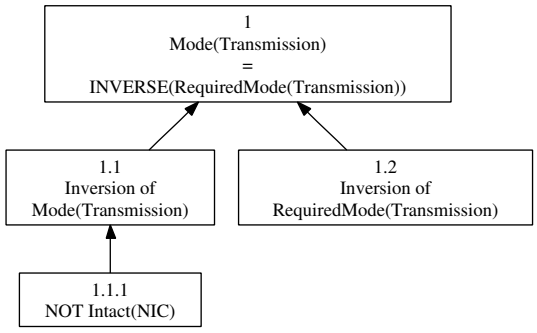


Deviation 10.b A class of transmission occurs less often than defined



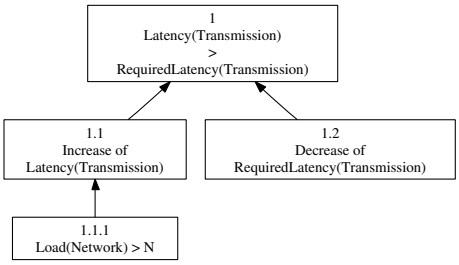
Deviation 11.a Information is not transmitted
Deviation 11.a is identical with deviation 3.a.

Deviation 11.b Event-triggered transmission is sent in time-triggered mode

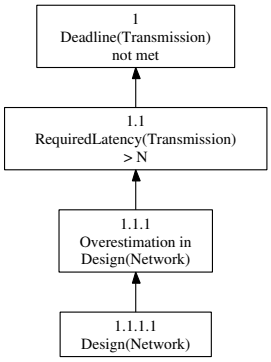


Deviation 11.c Time-triggered transmission is sent in event-triggered mode
Deviation 11.c is identical with deviation 11.b.

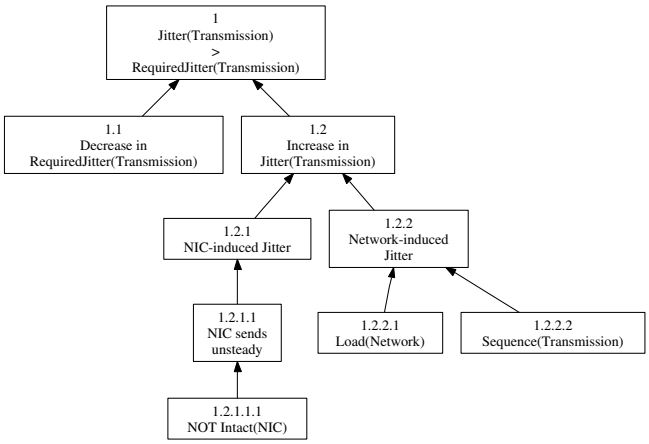
Deviation 12.a Transmission latency is bigger than intended



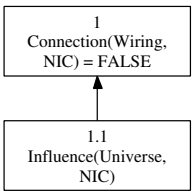
Deviation 12.b Latency is defined too big



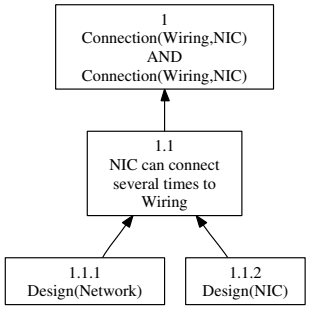
Deviation 13.a Jitter is bigger than intended



Deviation 14.a No connection between wiring and NIC exists



Deviation 14.b More connections between wiring and NIC exist than designed for



Deviation 15.a The network is vaster than intended Deviation 15.a is identical with deviation 1.a.

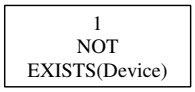
Deviation 15.b The network is smaller than intended
Deviation 15.b is identical with deviation 1.b.

Deviation 15.c Only part of the network exists
Deviation 15.c is identical with deviation 1.b.

Deviation 15.d The network works faster than intended
Deviation 15.d is identical with deviation 3.n.

Deviation 15.e The network works slower than intended
Deviation 15.e is identical with deviation 3.n.

Deviation 16.a The Device does not exist

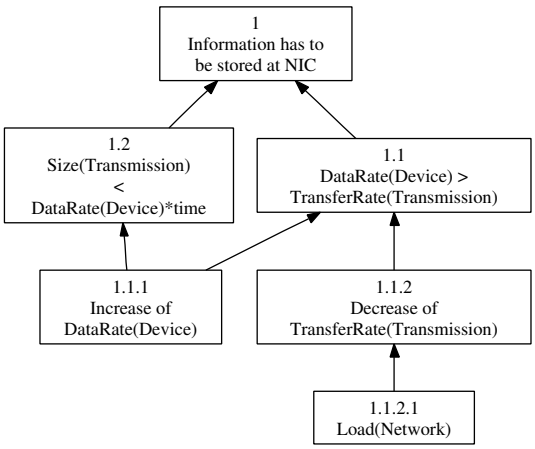


Deviation 16.b There are more devices than intended
Deviation 16.b cannot be described with the current ontology.

Deviation 16.c There are less devices than intended
Deviation 16.c cannot be described with the current ontology.

Deviation 16.d The device only exists in part
Deviation 16.d cannot be described with the current ontology.

Deviation 16.e The device works faster than expected



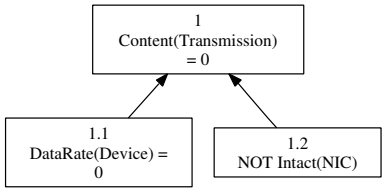
Deviation 17.a The length of the Wiring is greater than expected
Deviation 17.a is identical with deviation 2.a.

Deviation 17.b The length of the Wiring is smaller than expected
Deviation 17.b is identical with deviation 2.b.

Deviation 17.c Only part of the length of the Wiring is achieved
Deviation 17.c is identical with deviation 2.b.

Deviation 18.a Less requirements of the Wiring than needed were defined
During the refinement of the ontology all requirements needed for the description until a level of confidence is reached will be identified. If every element needed for this level of confidence is present this deviation becomes irrelevant.

Deviation 19.a The Transmission carries no content



Deviation 19.b The Transmission carries more content than expected
Deviation 19.b cannot be described with the current ontology.

Deviation 19.c The Transmission carries less content than expected
Deviation 19.c cannot be described with the current ontology.

Deviation 19.d The content is only transmitted in part
Deviation 19.d cannot be described with the current ontology.

Deviation 19.e The content of the Transmission is inverted
Deviation 19.e cannot be described with the current ontology.

Deviation 19.f The content is transmitted early
Deviation 19.f is identical with deviation 3.h.

Deviation 19.g The content is transmitted late
Deviation 19.g is identical with deviation 3.j.

Deviation 19.h The content is transmitted early in sequence
Deviation 19.h is identical with deviation 3.l.

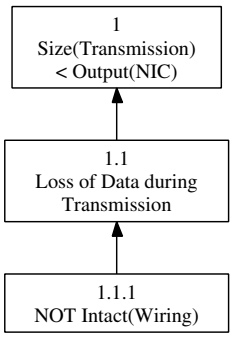
Deviation 19.i The content is transmitted late in sequence
Deviation 19.i is identical with deviation 3.l.

Deviation 19.j The content is transmitted faster than expected
Deviation 19.j is identical with deviation 3.n.

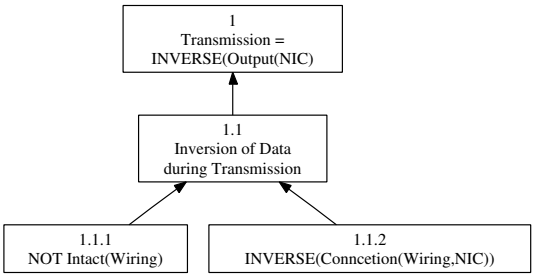
Deviation 19.k The content is transmitted slower than expected
Deviation 19.k is identical with deviation 3.o.

Deviation 20.a The format is too restricted for fulfilling the needs of the communication
Deviation 20.a cannot be described with the current ontology.

Deviation 20.b The format is only achieved in part



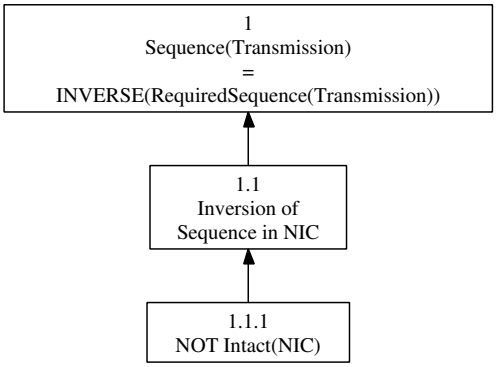
Deviation 20.c The format is reversed



Deviation 21.a The sequence is to restricted for fulfilling the needs of the communication
Deviation 21.a cannot be described with the current ontology.

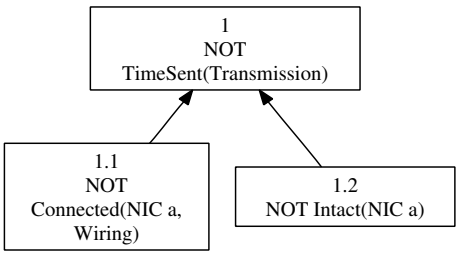
Deviation 21.b The sequence of transmission is only partially achieved
Deviation 21.b is identical with the union of deviations 3.l and 3.m.

Deviation 21.c The sequence of transmission is reversed



Deviation 21.d The sequence does not provide enough room for transmission
Deviation 21.d is identical with deviation 3.b.

Deviation 22.a The transmission is not sent



Deviation 22.b The time of sending is greater than expected
Deviation 22.b is identical with deviation 3.j.

Deviation 22.c The time of sending is smaller than expected
Deviation 22.c is identical with deviation 3.h.

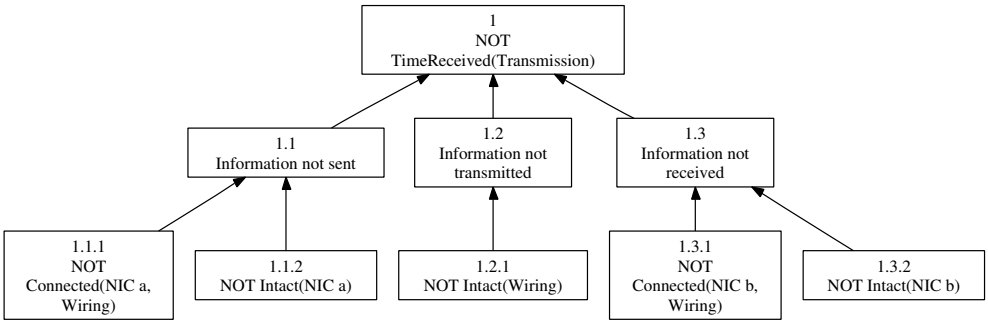
Deviation 22.d The transmission is sent early
Deviation 22.d is identical with deviation 3.h.

Deviation 22.e The transmission is sent late
Deviation 22.e is identical with deviation 3.j.

Deviation 22.f The transmission is sent early in sequence
Deviation 22.f is identical with deviation 3.l.

Deviation 22.g The transmission is sent late in sequence
Deviation 22.g is identical with deviation 3.m.

Deviation 23.a The transmission is not received



Comments:

Deviation 23.b The time of receiving is greater than expected
Deviation 23.b is identical with deviation 3.k.

Deviation 23.c The time of receiving is smaller than expected
Deviation 23.c is identical with deviation 3.i.

Deviation 23.d The transmission is received early
Deviation 23.d is identical with deviation 3.i.

Deviation 23.e The transmission is received late
Deviation 23.e is identical with deviation 3.k.

Deviation 23.f The transmission is received early in sequence
Deviation 23.f is identical with deviation 3.l.

Deviation 23.g The transmission is received late in sequence
Deviation 23.g is identical with deviation 3.m.

Deviation 24.a The transfer rate is greater than expected
Deviation 24.a is identical with deviation 3.n.

Deviation 24.b The transfer rate is smaller than expected
Deviation 24.b is identical with deviation 3.o.

Deviation 24.c The transfer rate is only partially achieved
Deviation 24.c is identical with deviation 3.o.

Deviation 24.d The transfer rate is faster than expected
Deviation 24.d is identical with deviation 3.n.

Deviation 24.e The transfer rate is slower than expected
Deviation 24.e is identical with deviation 3.o.

Deviation 25.a Value required for jitter greater than needed
Deviation 25.a is identical with deviation 3.k.

Deviation 25.b Value required for jitter only partially achieved
Deviation 25.b is identical with deviation 3.k.

Deviation 26.a Value required for latency is greater than needed
Deviation 26.a is identical with deviation 3.k.

Deviation 26.b Value required for latency is only partially achieved
Deviation 26.b is identical with deviation 3.k.

Deviation 27.a Required mode of transmission is greater than needed
Deviation 27.a is identical with deviation 11.b.

Deviation 27.b Required mode of transmission is smaller than needed
Deviation 27.b is identical with deviation 11.b.

Deviation 27.c The mode requirement of transmission is reversed
Deviation 27.c is identical with deviation 11.b.

Deviation 28.a Required frequency of transmission is smaller than needed
Deviation 28.a is identical with deviation 10.a.

Deviation 28.b The period requirement of transmission is only partially achieved
Deviation 28.b is identical with deviation 10.a.

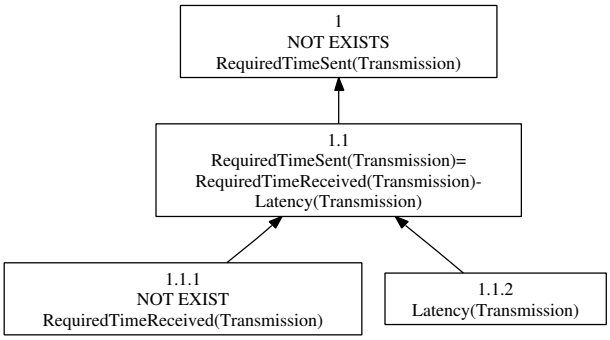
Deviation 28.c Period requirement of transmission is slower than in reality
Deviation 28.c is identical with deviation 10.a.

Deviation 29.a Required sequence of transmission is less elaborated than needed
Deviation 29.a cannot be described with the current ontology.

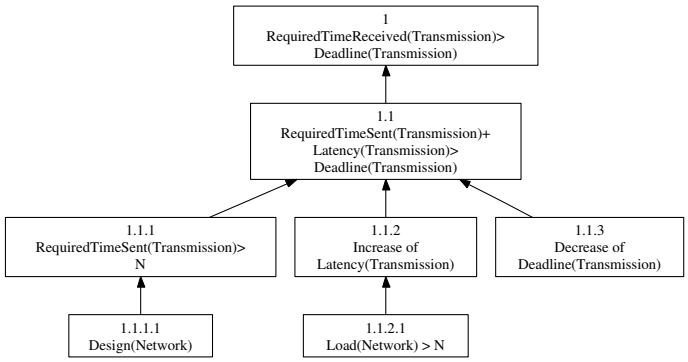
Deviation 29.b Sequence requirement is reversed
Deviation 29.b is identical with deviation 21.c.

Deviation 30.a The required size of the Transmission too small
Deviation 30.a is identical with deviation 3.b

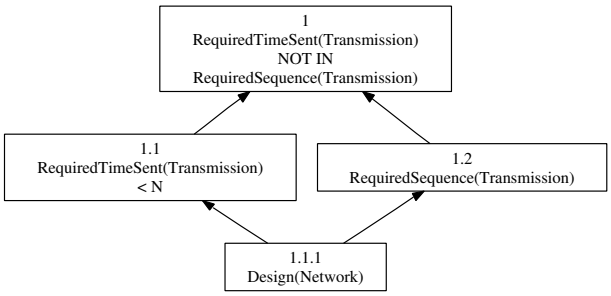
Deviation 31.a No maximal acceptable value of TimeSent(Transm.) can be derived



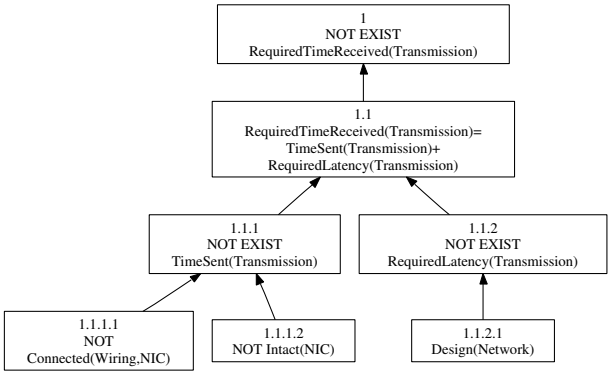
Deviation 31.b The maximal acceptable value of TimeSent(Transmission) is too large



Deviation 31.c The maximal acceptable value of TimeSent(Transmission) is too small



Deviation 32.a No maximal acceptable value of TimeReceived(Transm.) can be derived



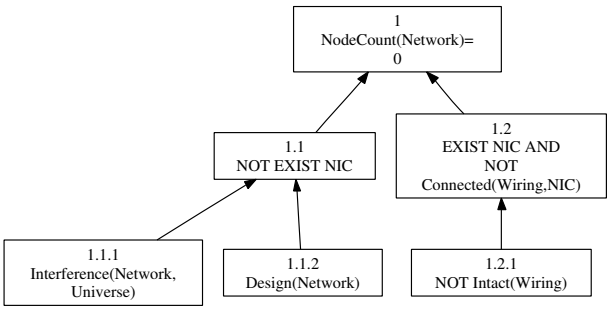
Deviation 32.b The maximal acceptable value of TimeReceived(Transm.) is too large
Deviation 32.b is identical with deviation 31.b.

Deviation 32.c The maximal acceptable value of TimeReceived(Transm.) is too small
Deviation 32.c is identical with deviation 3.h.

Deviation 33.a The value acceptable for the TransferRate(Transmission) is too large
Deviation 33.b will lead to deviation 16.e.

Deviation 33.b The value acceptable for the TransferRate(Transmission) is too small
Deviation 33.d will lead to deviation 16.e.

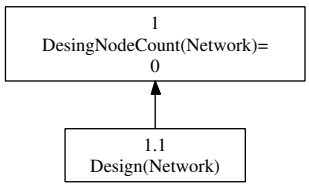
Deviation 34.a No nodes connected to the Wiring



Deviation 34.b The count of nodes is too large
Deviation 34.b is identical with deviation 1.a.

Deviation 34.c The count of nodes is too small
Deviation 34.c is identical with deviation 1.b.

Deviation 35.a Network design does not specify count of nodes in network

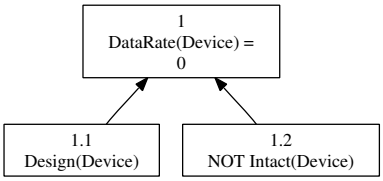


Deviation 35.b The count of nodes used in network design is too large
Deviation 35.b is identical with deviation 1.b.

Deviation 35.c The count of nodes used in network design is too small
Deviation 35.c is identical with deviation 1.a.

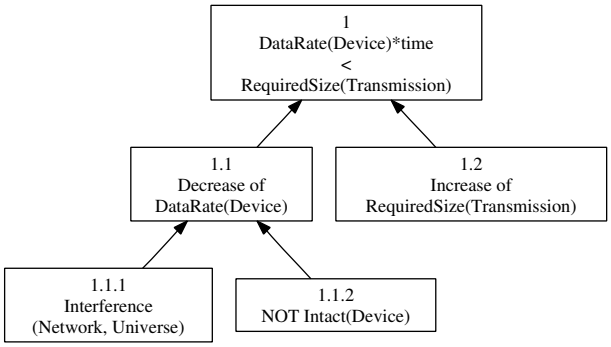
Deviation 35.d The count of nodes used in network design is only partially achieved
Deviation 35.d is identical with deviation 1.a.

Deviation 36.a The device does not produce data



Deviation 36.b The data rate of the device is too great
Deviation 36.b is identical with deviation 4.b.

Deviation 36.c The data rate of the device is too small



Deviation 36.d The data rate of the device is only partially achieved
Deviation 36.d is identical with deviation 36.c.

Deviation 36.e The data rate of the device is too fast
Deviation 36.e is identical with deviation 36.b.

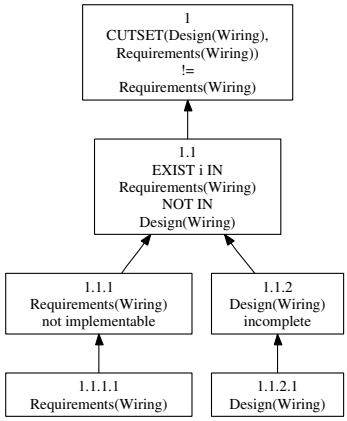
Deviation 36.f The data rate of the device is too slow
Deviation 36.f is identical with deviation 36.c.

Deviation 37.a The interference between Universe and Network is bigger than expected
Deviation 37.a cannot be described with the current ontology.

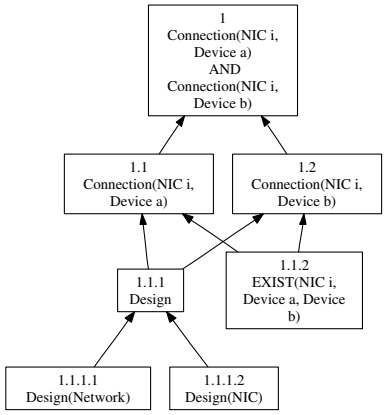
Deviation 37.b The interference between Universe and Network is reversed
Deviation 37.b cannot be described with the current ontology.

B.2 CIDs from 3^{rd} iteration

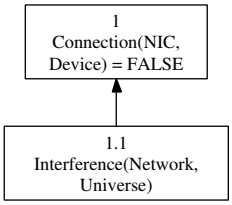
Deviation 2.d Wiring meets design intention only in part



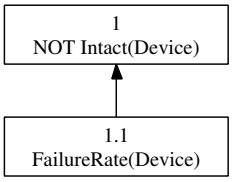
Deviation 16.b There are more devices than intended



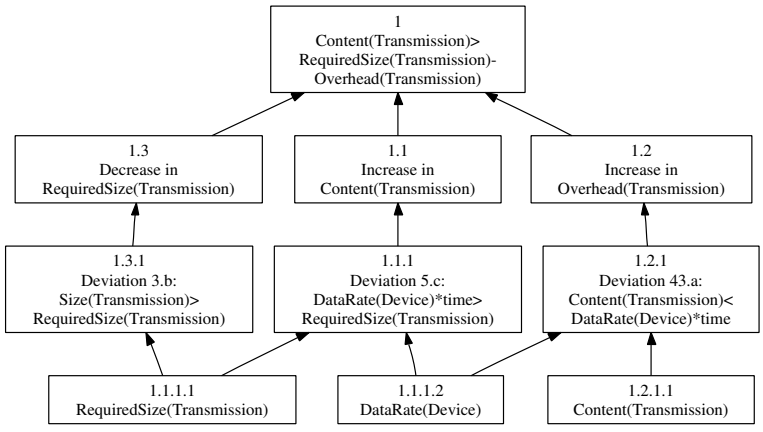
Deviation 16.c There are less devices than intended



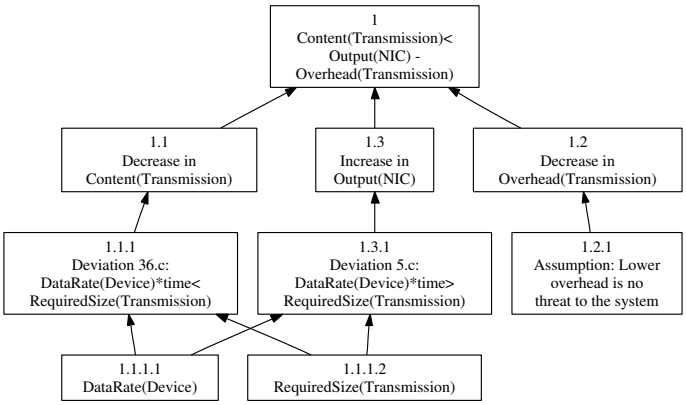
Deviation 16.d The device only exists in part



Deviation 19.b The Transmission carries more content than expected

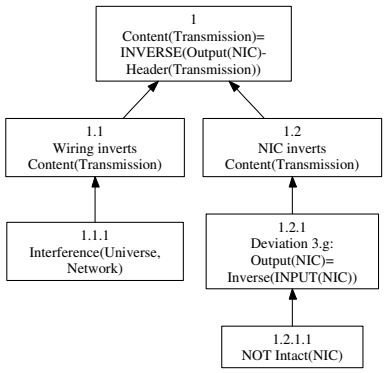


Deviation 19.c The Transmission carries less content than expected

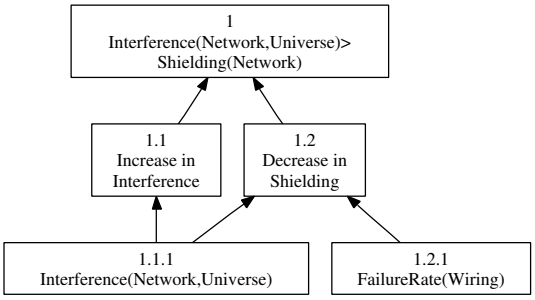


Deviation 19.d The content is only transmitted in part
Deviation 19.d is identical with deviation 19.c.

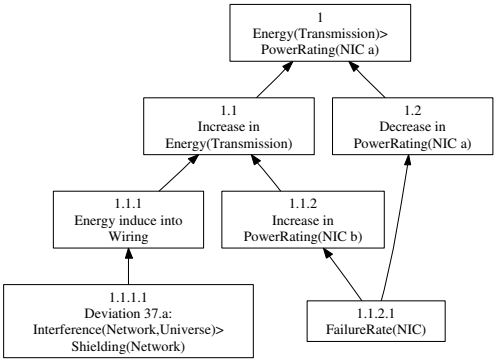
Deviation 19.e The content of the Transmission is inverted



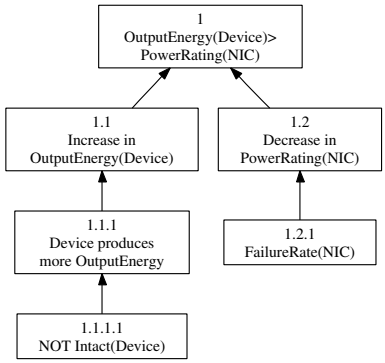
Deviation 37.a The interference between Universe and Network is bigger than expected



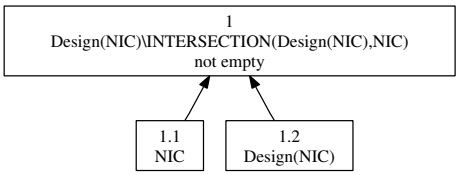
Deviation 39.a.1 The PowerRating for the NIC is lower than intended



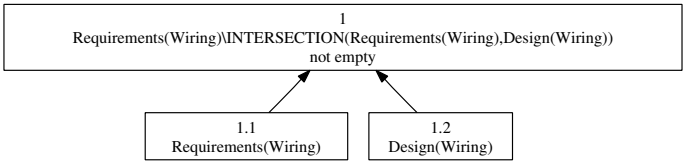
Deviation 39.a.2 The PowerRating for the NIC is lower than intended



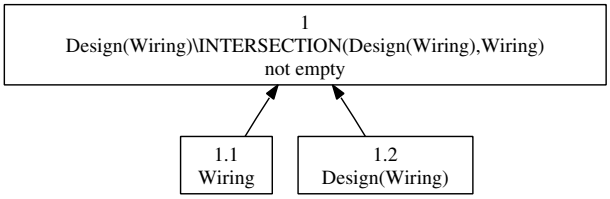
Deviation 40.b The Design of the NIC was only partially realised



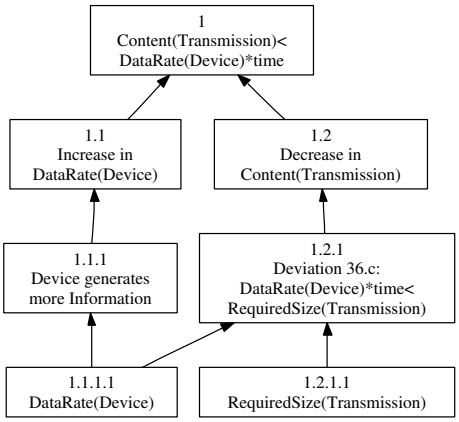
Deviation 41.a The Design of the Wiring is less elaborated than needed



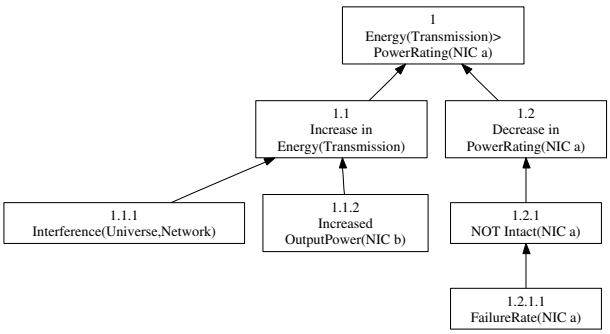
Deviation 41.b The Design of the Wiring was only partially realised



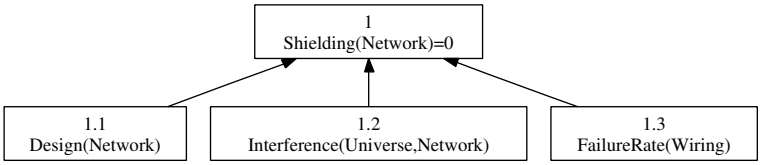
Deviation 43.a The Overhead of the Transmission is bigger than acceptable



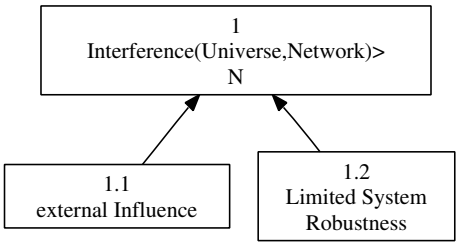
Deviation 44.a The Energy of the Transmission is bigger than expected



Deviation 45.a The Network has no Shielding



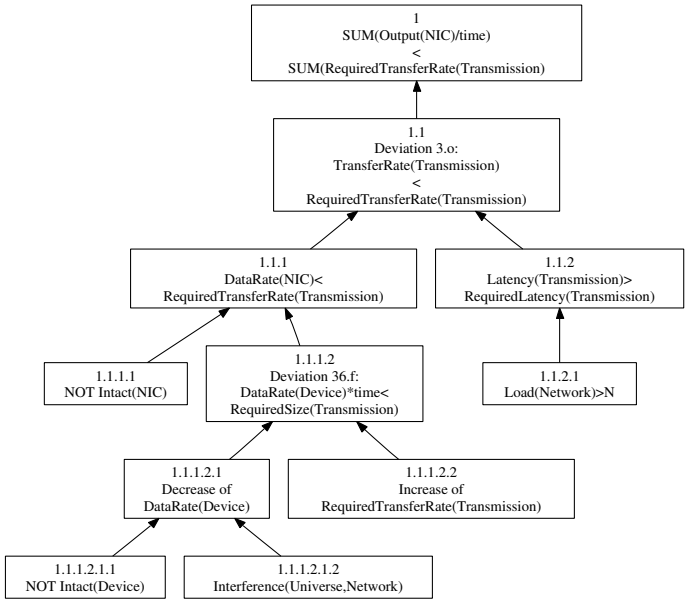
Deviation 45.b The Shielding is less elaborated than needed



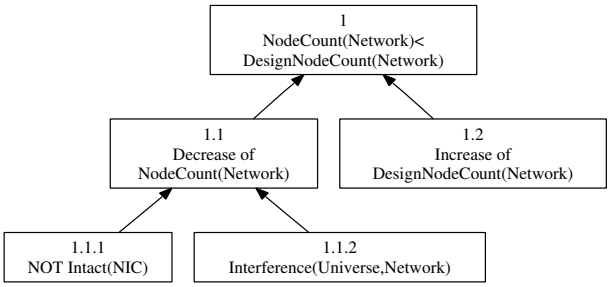
Deviation 45.c The Shielding is only partially achieved
Deviation 45.c is identical with deviation 45.b.

Deviation 47.a The Load of the Network is greater than expected
Deviation 47.a is identical with deviation 13.a.

Deviation 47.b The Load is only partially achieved



Deviation 48.a The Design of the Network is less elaborated than needed



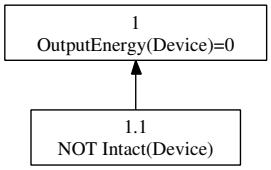
Deviation 48.b The Design of the Network is only partially achieved
Deviation 48.b is identical with deviation 48.a.

Deviation 49.a The Device is not intact
Deviation 48.a is identical with deviation 16.d.

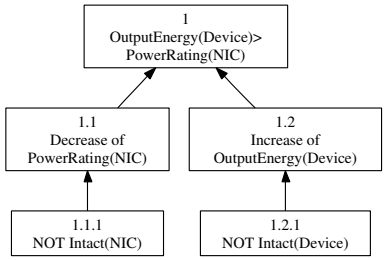
Deviation 49.b The Device is less intact than needed
Deviation 48.b is identical with deviation 16.d.

Deviation 49.c The Device is only partially intact
Deviation 48.c is identical with deviation 16.d.

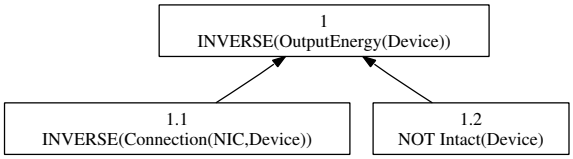
Deviation 50.a The Device has no OutputEnergy



Deviation 50.b The OutputEnergy of the Device is bigger than expected

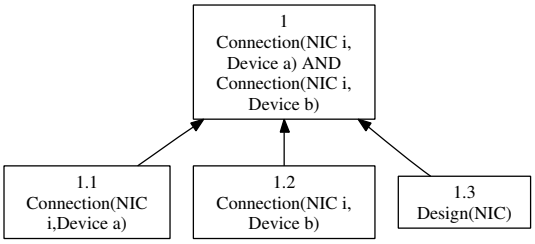


Deviation 50.e The OutputEnergy of the Device is reversed



Deviation 51.a The Device is not connected to the NIC
Deviation 51.a is identical with deviation 16.c.

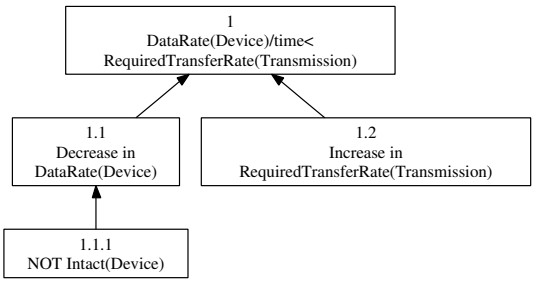
Deviation 51.b More than one connection between NIC and Device exists



Deviation 51.c.1 Less connections than expected exist between NIC and Device
Deviation 51.c.1 is identical with deviation 16.c.

Deviation 51.c.2 Less connections than expected exist between NIC and Device
Deviation 51.c.2 is identical with deviation 16.c.

Deviation 51.c.3 Less connections than expected exist between NIC and Device



Deviation 51.d.1 The connection between Device and NIC is only partially achieved
Deviation 51.d.1 is identical with deviation 16.c.

Deviation 51.d.2 The connection between Device and NIC is only partially achieved
Deviation 51.d.2 is identical with deviation 16.c.

Deviation 51.d.3 The connection between Device and NIC is only partially achieved
Deviation 51.d.3 is identical with deviation 16.c.

Deviation 51.e The connection between Device and NIC works faster than expected
Deviation 51.e is identical with deviation 16.e.

Deviation 51.f The connection between Device and NIC works slower than expected
Deviation 51.e is identical with deviation 16.e.

Bibliography

[All53] Allais, M.: *Le Comportement de l'Homme Rationnel devant le Risque, Critique des Postulats et Axiomes de l'Ecole Americaine.* Econometrica, 21:503–546, 1953. (cited after [KT79]).

[Ass02] Association des Constructeurs Européens d'Automobiles: *ACEA's CO_2 Commitement.* Rue du Noyer 211, B-1000 Bruxelles, November 2002. URL: http://www.acea.be/ACEA/brochure_co2.pdf (last verified: 13 Jun 2005).

[BC04] Bedford, Tim and Roger M. Cooke: *Probabilistic Risk Analysis - Foundations and Methods.* Cambridge University Press, 2004.

[Bel01] Bell, Jon: *Other automotive industry protocols*, November 2001. URL: http://www.aber.ac.uk/compsci/Research/mbsg/fmeaprojects/SoftFMEAtechreports/systems/other_protocols.doc (last verified: 16 Jun 2005).

[BOS05] BOSCH Engineering: *The intelligent powertrain - Innovation from Bosch Engineering*, 2005. URL: http://www.bosch-engineering.de/en/work/work_powertrain.shtm (last verified: 13 Jun 2005).

[Bou04] Bouder, Frederic: *Social Dialogue and the Tolerability of Risk Framework.* The IPTS Report, 82, March 2004. URL: http://www.jrc.es/home/report/english/articles/vol82/ (last verified 02 Jun 2005).

[Bra05] Braband, Jens: *Author's notes on the Lecture "Risikoanalyse, Allgemeiner Ansatz", held in the 3day course "Riskoanalyse technischer Systeme", TU Braunschweig*, Febuary 2005.

[Bri98] Brite-EuRam III: *Safety Related Fault Tolerant Systems in Vehicles (X-By-Wire)*, 1996-1998. URL:

http://www.vmars.tuwien.ac.at/projects/xbywire/projects/new-main.html (last verified: 10 Jun 2005).

[Bun67] Bundesgesetzblatt II: *Eisenbahn-Bau und Betriebsordnung*, Mai 1967. (cited after http://www.wedebruch.de/gesetze/betrieb/ebo1.htm (last verified: 02 Jul 2005)).

[BvHH+04] Bechhofer, Sean, Frank van Harmelen, Jim Hendler, Ian Horrocks, Deborah L. McGuinness, Peter F. Patel-Schneider and Lynn Andrea Stein: *OWL - Web Ontology Language Reference*. W3C - World Wide Web Consortium, 2004. URL: http://www.w3.org/TR/owl-ref/ (verified: 23 Jun 2005).

[CAN91] *CAN Specification, Version 2.0*. Robert Bosch GmbH, 1991. URL: http://www.semiconductors.bosch.de/pdf/can2spec.pdf (last verified: 04 Jul 2005).

[CIS77] CISHEC: *A Guide to Hazard and Operability Studies (HAZOP)*. The Chemical Industry Safety and Health Council of the Chemical Industries Associations Ltd., Chemical Industries Association, London, UK, 1977.

[Cou49] Court of Appeal: *Edwards v. National Coal Board*, 1949. (1949) 1 K.B. 704, (1949) 1 All E.R. 743, pp712, 714 (cited after http://www.hse.gov.uk/risk/theory/alarpglance.htm, last verified: 15 Jul 2005).

[CS79] Combs, B. and P. Slovic: *Causes of death: iased newspaper coverage and biased judgments*. Journalism Quaterly, 56:837–843, 849, 1979. (cited after [SFL82]).

[CZKL01] Chand, Ching-Yao, Wei-Bin Zhang, El Miloudi El Koursi and Etienne Lemaire: *Safety Assessment of Advanced Vehicle Control and Safety Systems (AVCSS): A Case Study*, October 2001. URL: http://www.path.berkeley.edu/PATH/Publications/PDF/PRR/2001/PRR-2001-30.pdf (last verfied: 1 Jul 2005).

[Dep02] Department of Education and the Arts, State of Queensland: *ALARP principle*, 2002. URL: http://education.qld.gov.au/strategic/policy/guidelines/risk/pdf/rm-6.pdf (last verified: 02 Jun 2005).

[DFMP97] Dilger, Elmar, Thomas Führer, Bernd Müller and Stefan Poledna: *The X-By-Wire Concept:*

Time-Triggered Information Exchange and Fail Silence Support by new System Services, 1997. URL: http://www.vmars.tuwien.ac.at/projects/xbywire/projects/new-bosch.htm (last verified: 16 Jun 2005).

[ESM00] *Engineering Safety Management 3 - Yellow Book 3: Volumes 1 and 2 - Fundamentals and Guidance*. Railtrack PLC, London, January 2000. URL: http://www.yellowbook-rail.org.uk/site/the_yellow_book/yellow%20book.pdf (last verified: 15 Jul 2005).

[Eur96] European Commission DG III/F: *TTA (23396)*, 1996. URL: http://www.cordis.lu/esprit/src/omi23396.htm (last verified: 04 Jul 2005).

[Fin68] Finger, Dr. Hans-Joachim: *Eisenbahngesetze, 5., neubearbeitete Auflage*. C.H. Beck'sche Verlagsbuchhandlung, München, 1968.

[Fle04] *FlexRay Communications System - Protocol Specification, Version 2.0*. FlexRay Consortium, 2004. URL: http://www.flexray-group.com/specification_request.php (last verified: 04 Jul 2005).

[FMD+00] Führer, Thomas, Bernd Müller, Werner Dieterle, Florian Hartwich, Robert Hugel and Michael Walther: *Time Triggered Communication on CAN (Time Triggered CAN- TTCAN)*, October 2000. URL: http://www.can-cia.org/can/ttcan/fuehrer.pdf (last verified: 04 Jul 2005).

[GN87] Genesereth, Michael and Nils Nilsson: *Logical foundations of artificial intelligence*. Morgan Kaufmann Publishers, Inc., Los Altos, Californiato, 1987.

[GO94] Gruber, Thomas R. and Gregory R. Olsend: *An Ontology for Engineering Mathematics*. Fourth International Conference on Principles of Knowledge Representation and Reasoning, 1994. URL: ftp://ftp.ksl.stanford.edu/pub/KSL_Reports/KSL-94-18.ps.gz (last verified: 24 Jun 2005).

[Gru93] Gruber, Thomas R.: *Toward Principles for the Design of Ontologies Used for Knowledge Sharing*, August 1993. URL: http://ksl-web.stanford.edu/KSL_Abstracts/KSL-93-04.html (last verified: 23 Jun 2005).

[Hea92] Health & Safety Executive: *The Tolerability of Risk from Nuclear Power Stations*. HSE Books, 1988 (revised 1992). (cited after [Hea01]).

[Hea01] Health & Safety Executive: *Safety Assessment Principles for Nuclear Plants*, March 2001. URL: http://www.hse.gov.uk/nsd/saps.htm (last verified: 02 Jun 2005).

[HMW01] Hazell, R.W., G.V. McHattie and I. Wrightson: *Note on Hazard and Operability Studies [HAZOP].* Burlington House, Piccadilly, London W1J 0BA, 2001. URL: http://www.rsc.org/pdf/ehsc/HAZOP.pdf (last verified 04 Mar 2005).

[HSA74] *Health and Safety at Work Act*, 1974. cited after http://www.swarb.co.uk/acts/1974HealthandSafetyAct.shtml (last verified: 20 Jun 2005).

[Hum99] Hume, David: *An Enquiry Concerning Human Understanding.* Oxford University Press, 1748/1999.

[I2C00] *The I^2C-Bus Specification, Version 2.1.* Philips Seminconductors, January 2000. URL: http://www.semiconductors.philips.com/markets/mms/protocols/i2c/ (last verified: 04 Jul 2005).

[iA04] Automation, CAN in: *Milestones of CAN history*, May 2004. URL: http://www.can-cia.org/can/protocol/history/index.html (last verified: 18 Jul 2005).

[Int93] International Organisation for Standardisation: *ISO 11898. Road vehicles - Interchange of digital information - Controller area network (CAN) for high-speed comunication*, 1993.

[Int97] International Electrotechnical Commission: *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems*, December 1997. Version 4.0.

[Int01] International Electrotechnical Commission: *IEC 61882, Hazard and operability studies (HAZOP studies) - Application guide*, May 2001. First edition.

[JLL99] Johansson, Lars-Ake, Hanna Larsson and Sten Lundgren: *QWIK vs. CAN - efficiency comparison.* August 1999. URL: http://www.qrtech.se/Downloads/1999.0001.pdf (last verified: 14 Jun 2005).

[Ker05] Kerry, Steward J.: *IEEE 802.11^{TM} WIRELESS LOCAL AREA NETWORKS*, 2005. URL: http://www.ieee802.org/11/ (last verified: 18 Jul 2005).

[KH02] Kelling, Nico A. and Worthy Heck: *The BRAKE Project - Centralized Versus Distributed Redundancy for Brake-by-Wire Systems*, 2002.

[KT79] Kahneman, Daniel and Amos Tversky: *Prospect Theory: An Analysis of Decision under Risk.* Econometrica, 47(2):263–292, March 1979.

[Kuh81] Kuhlmann, Albert: *Einführung in die Sicherheitswissenschaft.* Friedr. Vieweg&Sohn, Wiesbaden; Verlag TÜV Rheinland, Köln, 1981.

[Lad01] Ladkin, Peter B.: *Causal System Analysis - Formal Reasoning About Safety and Failure.* Technische Fakultät, Universität Bielefeld, Germany, 2001.

[Lad05] Ladkin, Peter B.: *Ontological Analysis.* Safety Systems, volume 14(3), May 2005. URL: http://www.rvs.uni-bielefeld.de/publications/Reports/Ladkin-SafetySystemsMay05.pdf (last verified: 17 Jun 2005).

[Law05] Law, David: *IEEE 802.3 CSMA/CD (ETHERNET)*, March 2005. URL: http://www.ieee802.org/3/ (last verified: 18 Jul 2005).

[Lew73] Lewis, David: *Causation.* The Journal of Philosophy, LXX:556–567, The Journal of Philosophy Inc., New York, 1973.

[LSF+78] Lichtenstein, S., P. Slovic, B. Fischhoff, M. Layman and B. Combs: *Judged frequency of lethal events.* Journal of Experimental Psychology: Human Learning and Memory, 4:551–578, 1978. (cited after [SFL82]).

[Lup03] Lupini, Christopher A.: *Multiplex Bus Progression 2003.* In-Vehicle Networks, Safety Critical Systems, Accelerated Testing, and Reliability, SP-1783/SP-1783CD, 2003. URL: www.delphi.com/pdf/techpapers/2003-01-0111.pdf (last verified: 03 Jul 2005).

[Mes04] Messanger, John: *IEEE 802.5 Web Site*, March 2004. URL: http://www.ieee802.org/5/ (last verified: 18 Jul 2005).

[Min94] Ministry of Defence: *DefStan 00-58: "HAZOP Studies on Systems Containing Programmable Electronics".* UK Defence Standardization, 1994. cited after [ESM00].

[Nat] National Archives: *Committee on Safety and Health at Work (Robens Committee): Report and Papers.* URL: http://www.catalogue.nationalarchives.gov.uk/displaycataloguedetails.asp?CATID=8976&CATLN=3&Highlight=&FullDetails=True (last verified: 02 Jun 2005).

[Por13] Porter, Noah (editor): *Webster's Revised Unabridged Dictionary.* G & C. Merriam Co., 1913. URL: http://machaut.uchicago.edu/?resource=Webster%27s&word=ontology (last verified: 23 Jun 2005).

[RCC99] Redmill, Felix, Morris Chudleigh and James Catmur: *System Safety: HAZOP and Software HAZOP.* John Wiley & Sons, Chichester, 1999.

[SFL82] Slovic, Paul, Baruch Fischoff and Sarah Lichtenstein: *Judgement under uncertainty: Heuristics and biases*, chapter 33. Facts versus fears: Understanding perceived risk, pages 463–489. Camebridge University Press, 1982.

[Sie05] Sieker, Bernd: *A Procedure for Safety-Requirements Analysis for Train Dispatching Systems.* Proceedings of the Fifth Bieleschweig Workshop on System Engineering, Garching bei München, April 2005.

[Soa03] Soanes, Catherine (editor): *Compact Oxford English Dictionary of Current English.* Oxford University Press, 2003. URL: http://www.askoxford.com/concise_oed/failsafe?view=uk (last verified: 10 Jun 2005).

[Soc93a] Society of Automotive Engineers: *J2056 I.R. Class C Multiplexing, Part 1, Applications Requirements.* SAE Technical Report J2056/1, June 1993. (cited after [JLL99]).

[Soc93b] Society of Automotive Engineers: *J2056 I.R. Class C Multiplexing, Part 2, Survey of Known Protocols.* SAE Technical Report J2056/1, April 1993. (cited after [DFMP97]).

[Sto78] Stoll, W.: *Technischer Fortschritt oder heile Umwelt - eine Frage an unser Gewissen?* Manuskript vom 18.07.1978, Hanau, ALKEM GmbH, July 1978. (cited after [Kuh81]).

[Sto80] Stoll, W.: *Warum wird gerade an der Kernenergie die Technophobie exemplifiziert?* Manuskript vom 21.04.1980, Hanau, ALKEM GmbH, April 1980. (cited after [Kuh81]).

[TTP03] *Time-Triggered Protocol TTP/C - High-Level Specification Document, Protocol Version 1.1.* TTTech Computertechnik AG, 2003. URL: http://www.ttagroup.org/technology/specification.htm (last verified: 04 Jul 2005).

[VAN94] *ISO 11519-3: Road vehicles - Low-speed serial data communication - Part 3: Vehicle area network (VAN)*, 1994. (cited after [DFMP97]).

[vNM53] Neumann, John von and Oskar Morgenstern: *Theory of Games and Economic Behavior.* Princeton University Press, third edition, 1953.

[vW03] Wense, H.-Chr. v.d. (editor): *LIN Specification Package, Revision 2.0.* LIN Consortium, September 2003. URL: http://www.lin-subbus.org/ (last verified: 04 Jul 2005).

[Web28] Webster, Noah (editor): *American Dictionary of the English Language.* S. Converse, New York, 1828. republished in facsimile edition by Foundation for American Christian Education, San Francisco, Calif., 1989.

[WF00] Ward, Daniel K. and Harold L. Fields: *A Vision of the Future of Automotive Electronics.* Intelligent Vehicle Systems, SP-1538, 2000.

[Whi01] Whitfield, Kermit: *Solve for X*, December 2001. URL: http://www.autofieldguide.com/articles/120105.html (last verified: 11 Jun 2005).