



Technische
Universität
Braunschweig

Institut für Verkehrssicherheit
und Automatisierungstechnik **iva**

Prof. Dr.-Ing. Dr. h.c. mult. E. Schnieder



7.2. Secondary Tools: Safety Tools

Goal Structured Notation Language

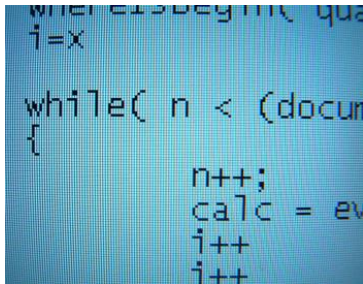
Jan Welte (TU-BS)

14.11.2013

Safety Case Process - Objectives



- Bring integrity to the Safety Case

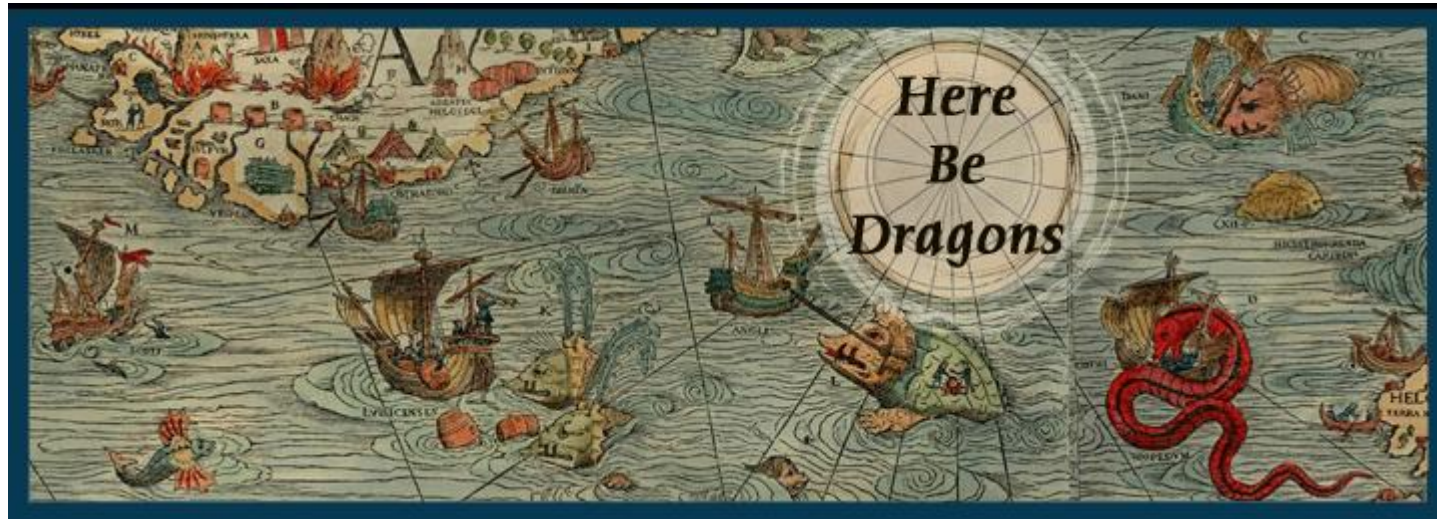


- Develop Tool



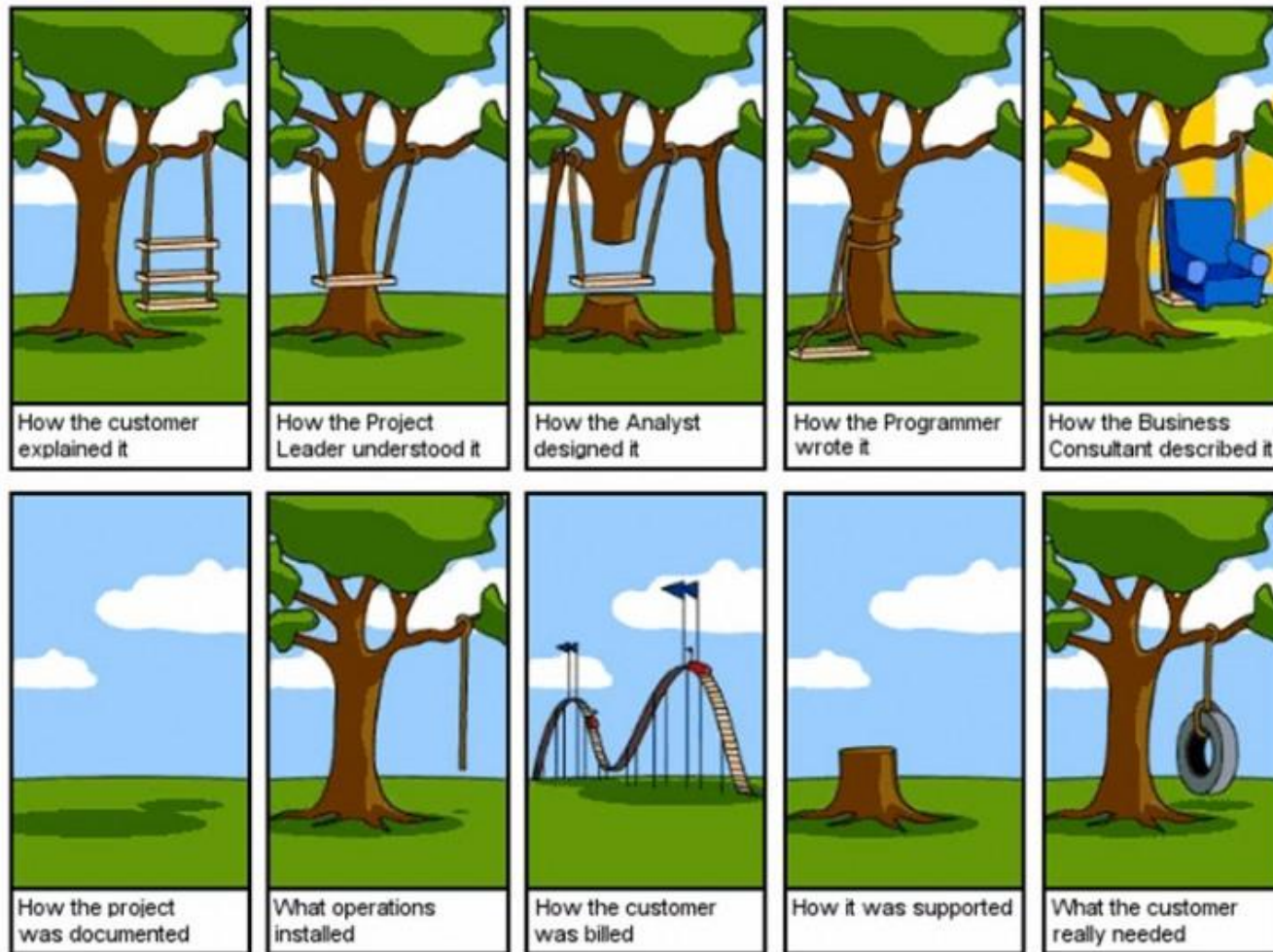
- Save Time and Money

Understanding EN 5012x



Feedback: Who are you? ... and what do you know about the Safety Case?

What we did not want ...



EN 5012x misconceptions

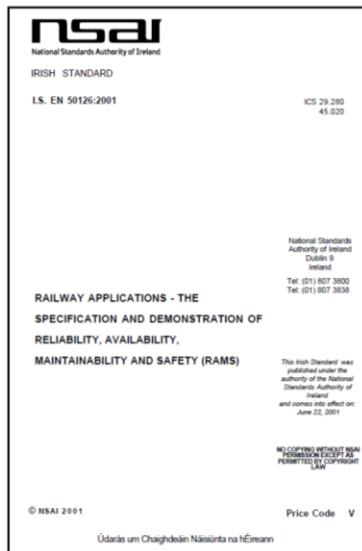
- „You do the Safety Case for the OpenETCS software, don't you?“
- „When we are ready to deliver our product we write the Safety Case Report to get a certification“

Safety Case Process – CENELEC interpretation

Before

Written Norm

- EN 50126 (76 pages)
- EN 50128 (106 pages)
- EN 50129 (97 pages)

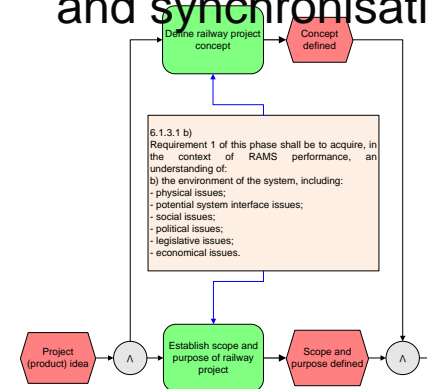


After

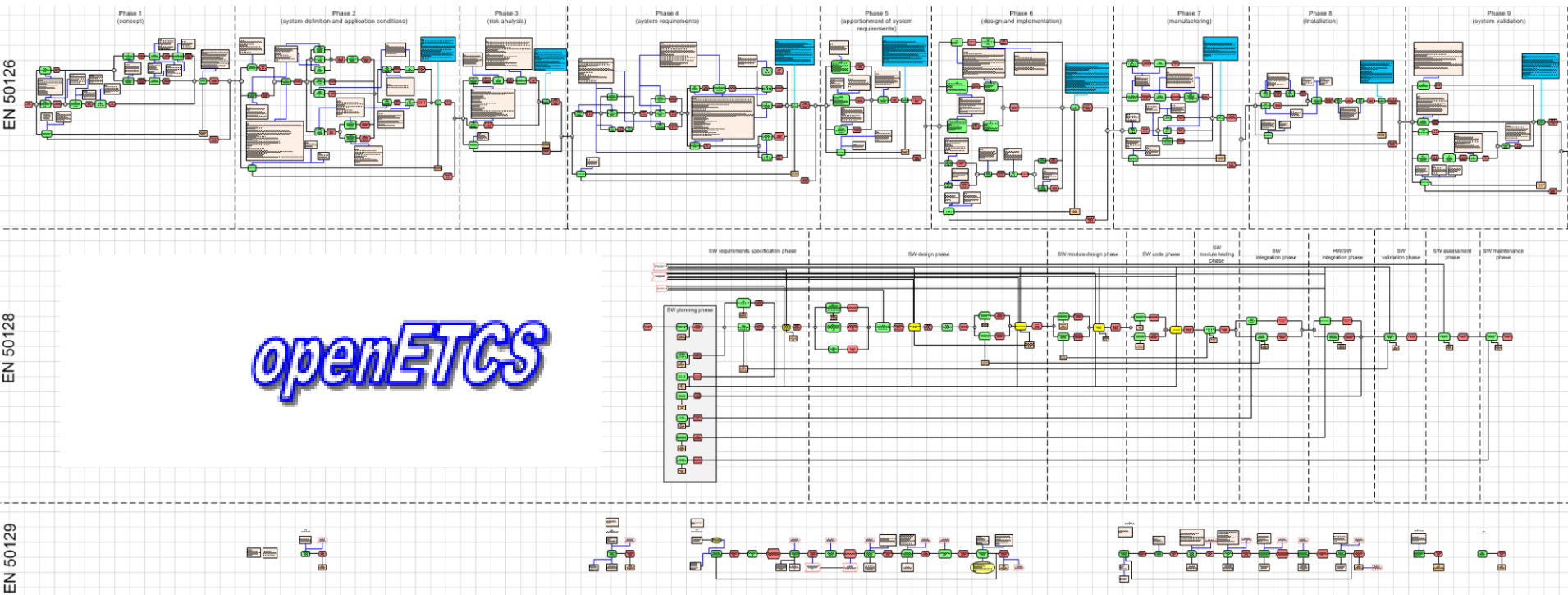
EPC Model of EN 5012x

- 185 states
- 192 activities
- 189 requirements
- 805 arcs
- 80 parallelisations

and synchronisations



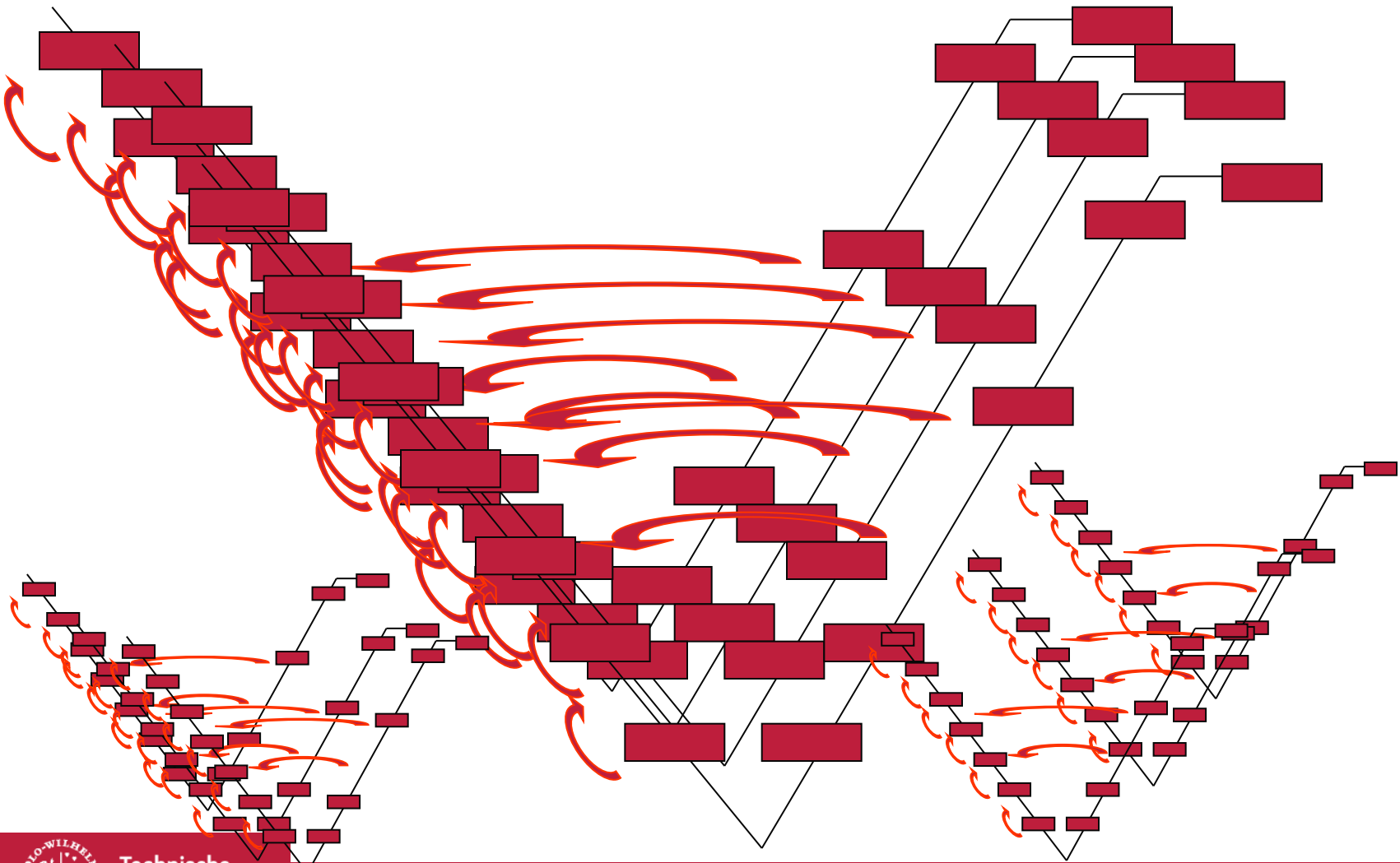
EN 5012x EPC Model









Transparency of the Safety Argumentation

- A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [EN 50129]
- “The safety case is a line of argumentation, not just a collection of facts.”[Odd Nordland, SINTEF]
- A safety case is “A *structured argument*, supported by a *body of evidence* that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.” [UK Defense Standard]

Safety Case: who overviews the links?



Goal Structuring Notation Elements

Element	Description
	A goal is a requirement, target or constraint to be met by the system. The term goal hierarchy refers to the collection of goals produced by the hierarchical decomposition of goals into sub-goals.
	A goal (or set of goals) can be solved by a strategy, which breaks a goal into a number of sub-goals. The satisfactory solution of the sub-goals then entails the solution of the original goals. A strategy can be regarded as a rule to be invoked in the solution of goals.
	Some goals may be solved directly by what we term solutions, rather than by decomposition into sub-goals. This is where the high level argument links to and uses the supporting evidence. Solutions will be individual pieces of analysis, evidence, results of audit reports, or references to design material including models. In fact we are not restrictive at all of the form that solutions can take.
	Strategies often need some justification for their use. It may be that the strategy is laid down in some standard followed by the developers: it may be common practice; or it may be a more elaborate argument as to the validity of the use of the strategy. Alternatively a justification may call upon evidence from analysis of the model or be a structured proof.
	Any assumption on which the strategy or goal is being put forward as a solution to the parent goal.
	Additional contextual information to a goal, a strategy or any other element can be couched in a context element.

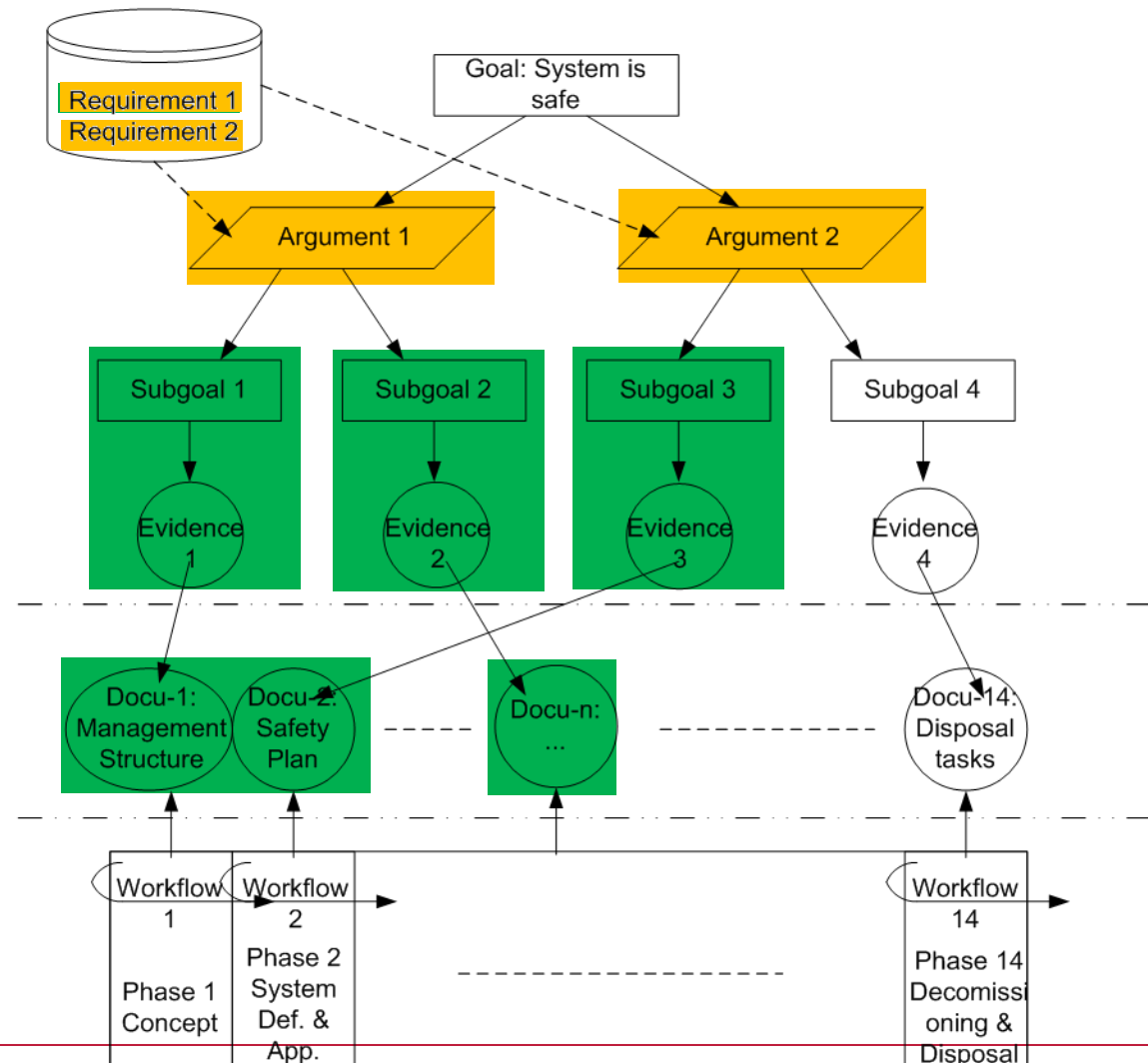
Goal Structuring Notation Example

“Goal Structure”
structured argument

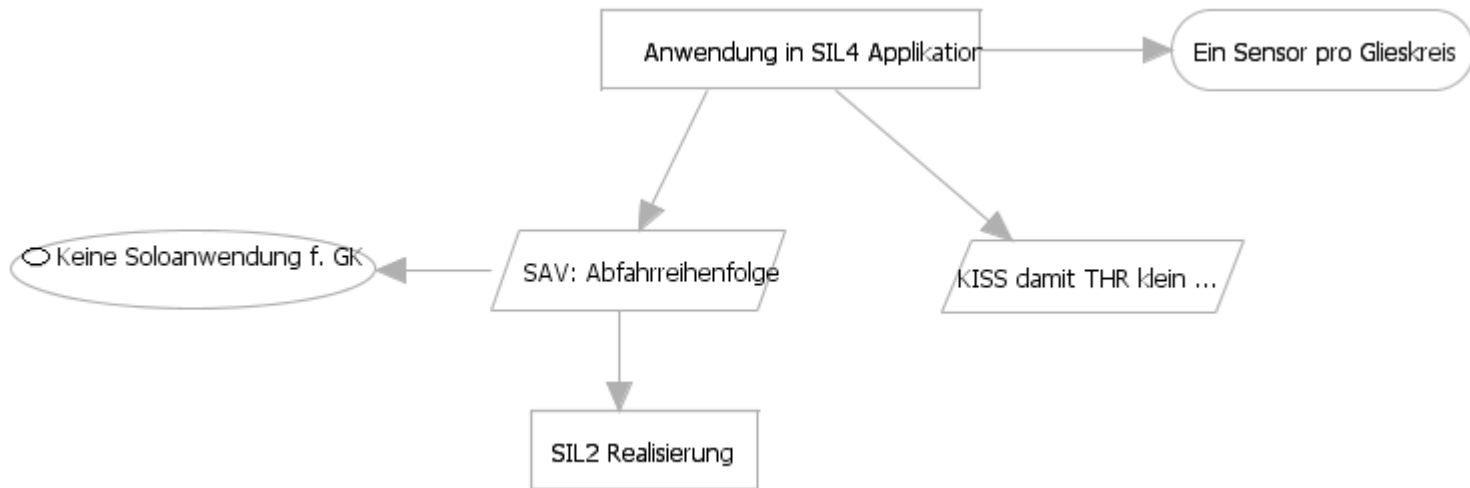
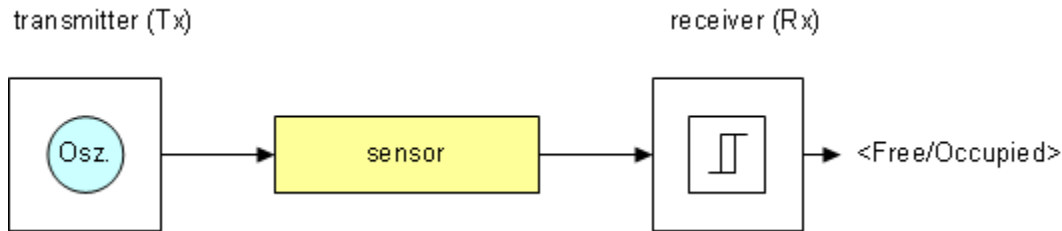
body of evidence

Database of
Documents

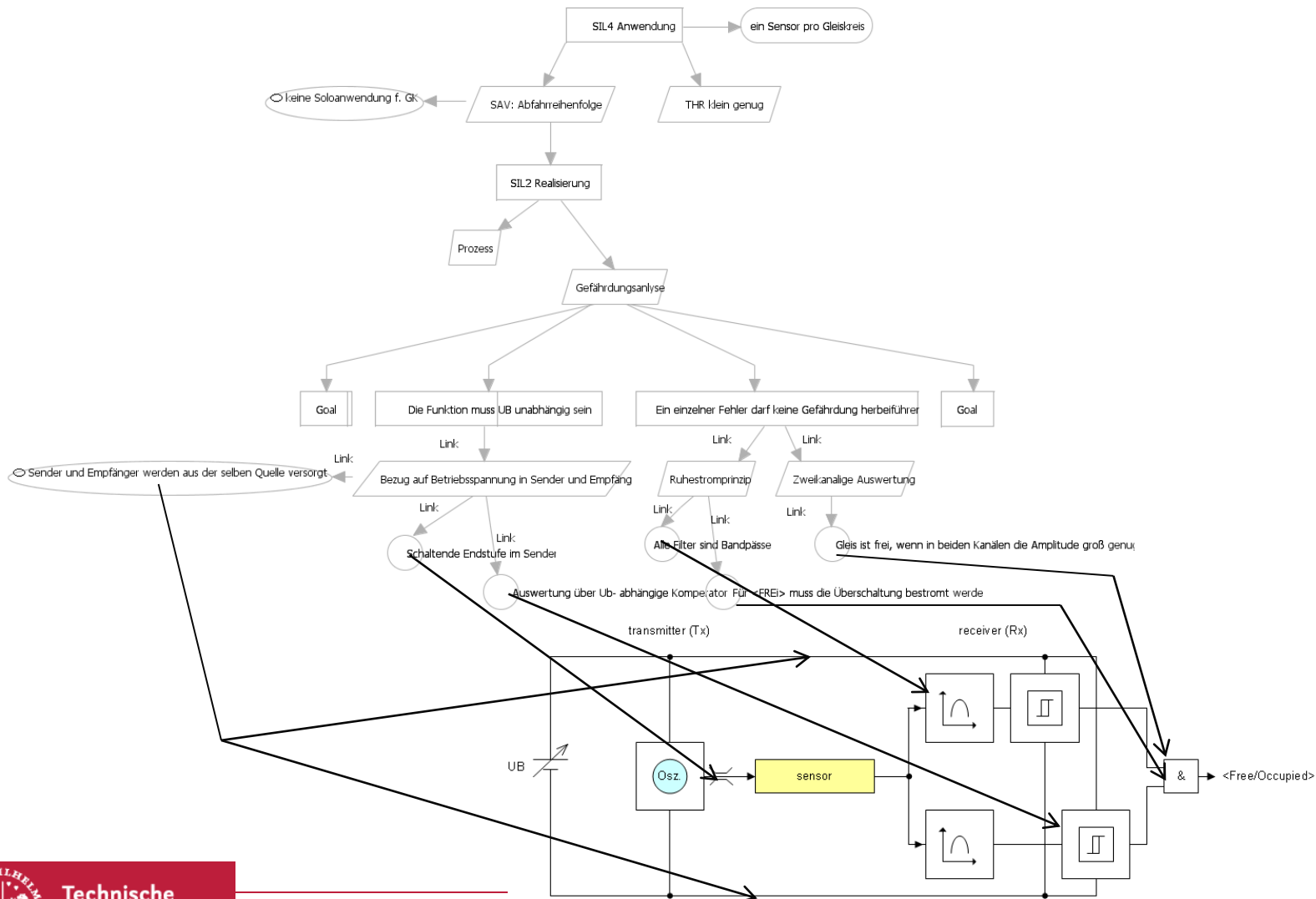
Document
Management System



Using GSN in system architecture



Using GSN in system implementation



The Power of GSN

- a) GSN is suitable to clarify the chain of arguments
- b) The arguments focus on the essentials.
- c) The GSN thus reduces the overhead
- d) It improves the overview
- e) facilitate the maintenance of durable Safety's case, since it gives a good summary.
- f) If the security argument is well known and standardized, even larger development projects carried out in parallel.
- g) contains implicitly the structure of the project schedule.

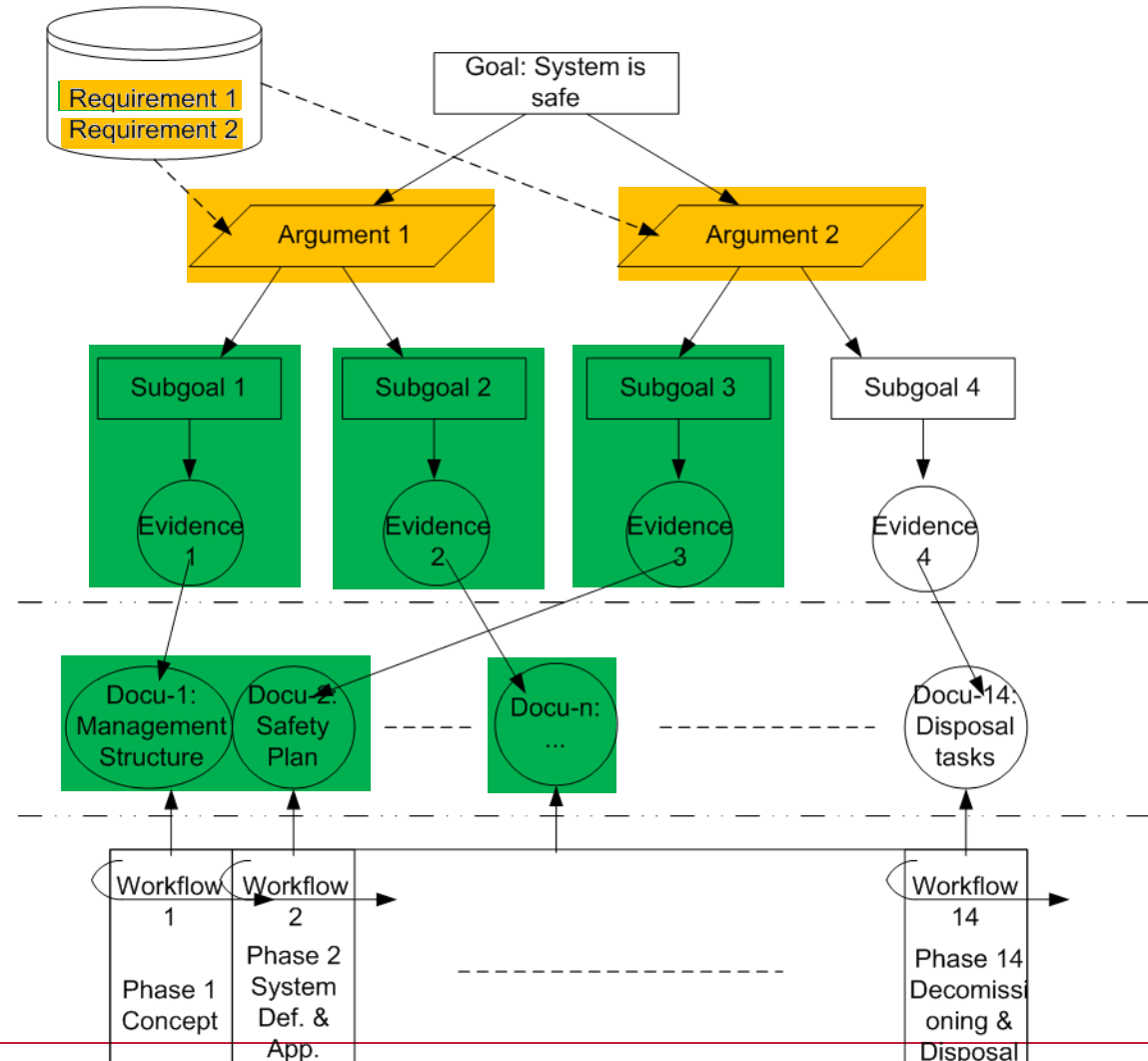
Goal Structuring Notation Example

“Goal Structure”
structured argument

body of evidence

Database of
Documents

Document
Management System

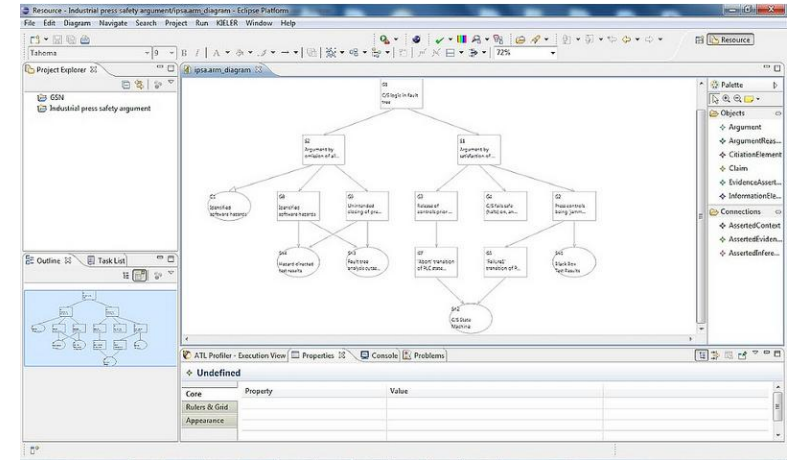
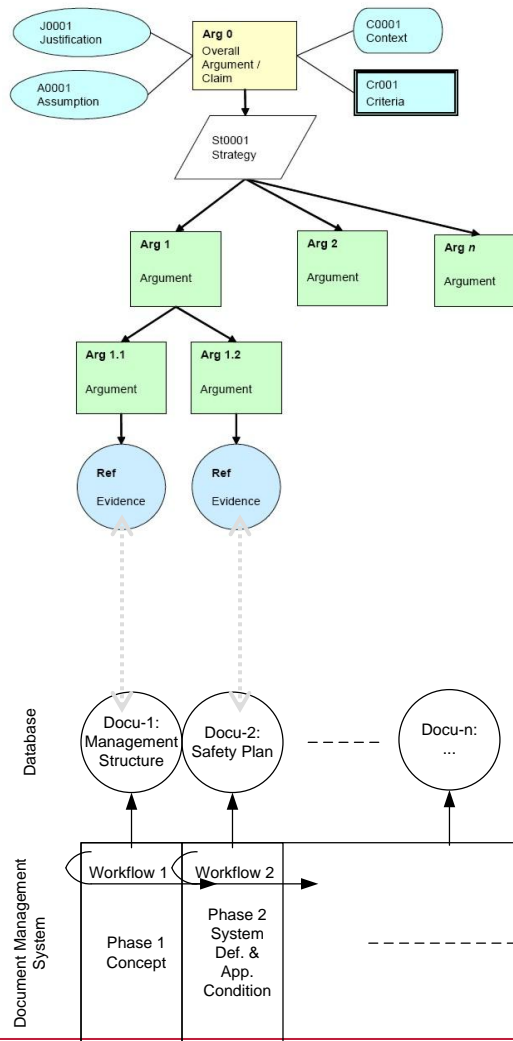


GSN & DMS implementation

GSN

Interface

DMS



14.11.2013

Jan Welte | Safety Tools -Goal Structured Notation Language

Seite 16

Eclipse based GSN Tool

- Acedit:
 - Developed by University of York
 - Eclipse plug-in
 - Under open source license



Project Home	Downloads	Wiki	Issues	Source
Search	Current pages	▼	for	Search
PageName ▼	Summary + Labels ▼			
ToolInstructionsUser	Instructions for users on how to install acedit			
ToolInstructionsDeveloper	Instructions for developers on how to install acedit			
GSNandARMmetamodels	presentation of the GSN and ARM metamodels			
InModelTransformation	The in-model transformation functionality of the tool			
ModelValidation	The model validation functionality of the tool			
ModelToModelTransformation	The model to model transformation functionality of acedit			
ChangesOverGMFGeneratedCode	The changes done over the GMF generated code			
ToolFeatures	A conclusion of the tool's features			
ToolArchitecture	The architecture of acedit is presented			
FutureWork	Recommendations for future work			

