Connecting IT and Transport

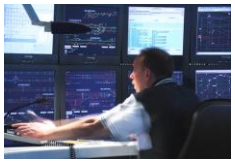
# Harmonising safety cases (INESS)

Carsten Trog

Munich, 9 November 2010

funkwerk
information technologies

# INESS




**European signalling systems need to be harmonised to facilitate the modernisation of the railways**

funkwerk
information technologies

# Overview

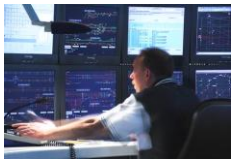
- Motivation behind INESS
- INESS Work packages
- Harmonising safety cases
- Achievements and prospects

funkwerk
information technologies

# Motivation behind INESS

funkwerk
information technologies

# National solutions for signalling systems incur high costs




- **Development of rail systems**
  - For 150 years regulations have been developed nationally
  - For 150 years technology has been developed nationally

**Consequences**

The supply industry has to provide many different small-scale systems

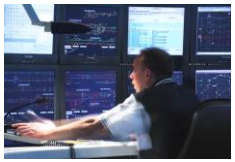
It is only cost-effective to produce electronic products in batches of thousands, not dozens

Until systems are standardised costs will remain high



funkwerk
information technologies

# Solutions

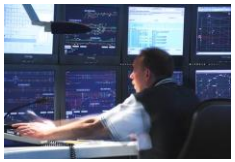



- Expand market-breadth of products
- Improve adaptability
- Implement open interfaces
- Implement practical modularity



funkwerk
information technologies

# Requirements for these solutions



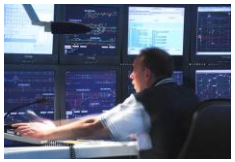

- Clear specifications
- Uniform specifications across national borders

**=> These are the main tasks for INESS**



funkwerk
information technologies

# INESS aims to harmonise signalling systems




"INESS – **In**tegrated **E**uropean **S**ignalling **S**ystem"

**Key statement:**

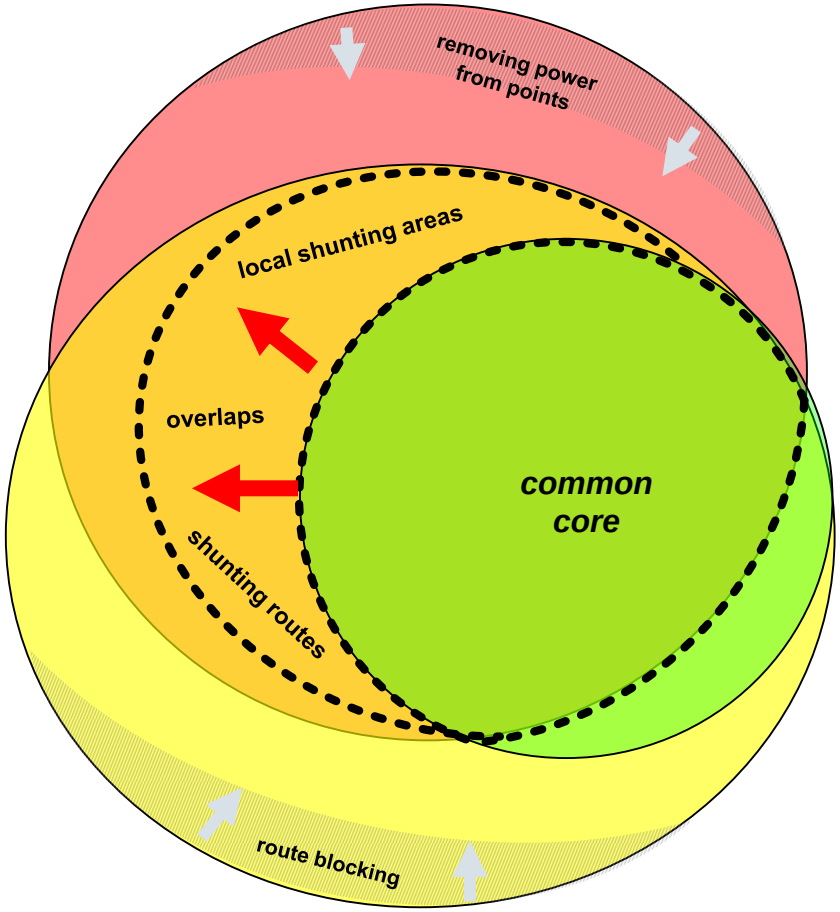
Railways and industry have a common objective: to harmonise those legal, safety-critical, operational and technical aspects that will reduce the barriers to cross-border transport



funkwerk
information technologies

# Main objective: Definition of a common core of functional requirements

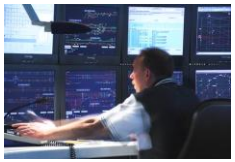
- Draw up proposal for harmonisation
- Define core functionalities
- Consider regulations






funkwerk information technologies

# Project details and participants



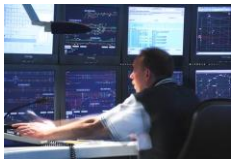

- Project budget: €16.6 million, including €10.3 million of EU funding
- 30 participating organisations (network operators, railway companies, universities)
- Project start date: 1 October 2008
- Project duration: 36 months

funkwerk
information technologies

# INESS Work packages

funkwerk
information technologies

# INESS Work packages




## Workstream B: Business Model

- WS B identifies the possible economical benefit of the measures

## Workstream C: System Design

- WS C specifies the data formats

## Workstream D: Generic Requirements

- WS D specifies the functional requirements

## Workstream E: Functional Architecture

- WS E specifies the interfaces

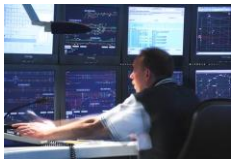
## Workstream F: Testing and Commissioning

- WS F harmonises the test process



funkwerk
information technologies

# INESS Work package: WS G




## Workstream G: Safety Case Process

**The goal is the standardisation of procedures for creating safety cases**

- Analysis of current procedures and problems
- Creation of an open-source tool to support the safety case process
- Validation via a pilot project

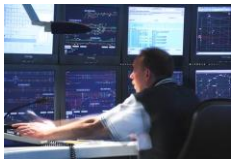


funkwerk
information technologies

# Workstream G: Harmonising safety cases

funkwerk
information technologies

# What is a safety case?

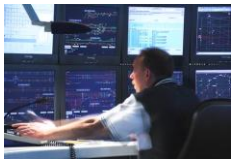



- UK Defence Standard: “A safety case is “A *structured argument*, supported by a *body of evidence* that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.”
- Odd Nordland, SINTEF: “The safety case is a line of argumentation, not just a collection of facts.”



funkwerk
information technologies

# What challenges does the Safety Case Process present?



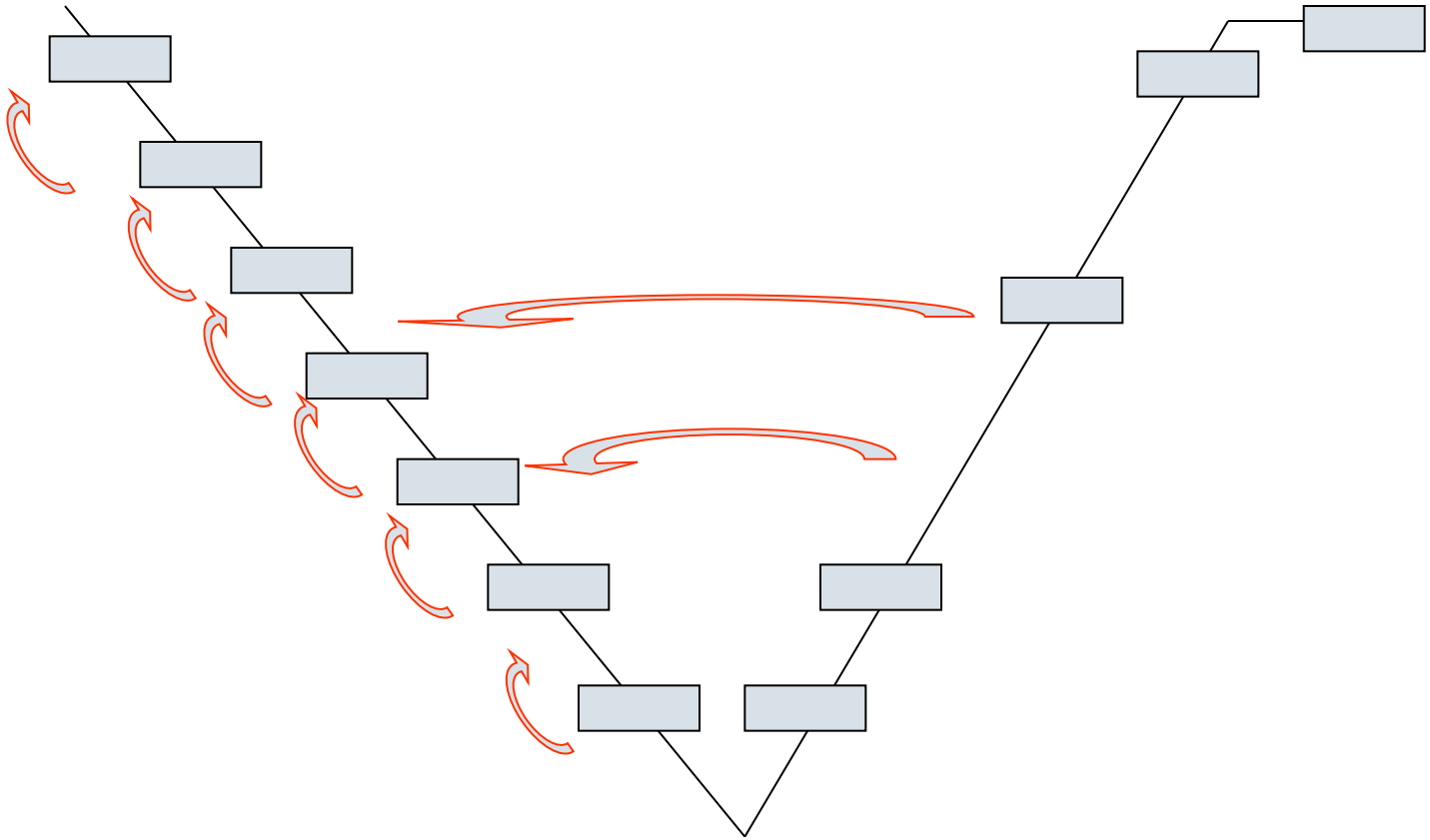

- Constructing safety arguments
- Keeping track of references
- Gathering and keeping track of safety-related conditions of use
- Keeping track of versions
- Keeping track of the effects of modifications
- Gathering and summarising reports
- …….

***In short: maintaining an overview***



funkwerk
information technologies

# Safety case: who has the overview of all the connections?

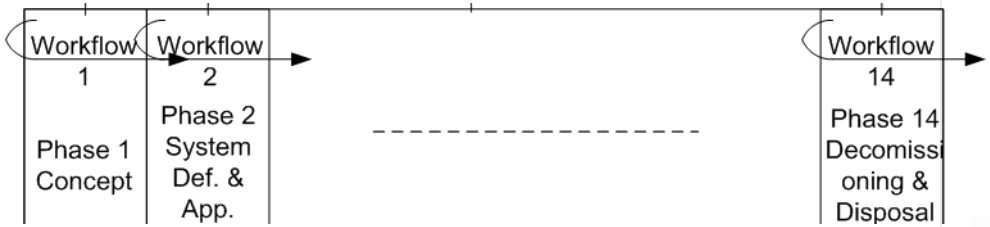




funkwerk
information technologies

# “Goal Structuring Notation”

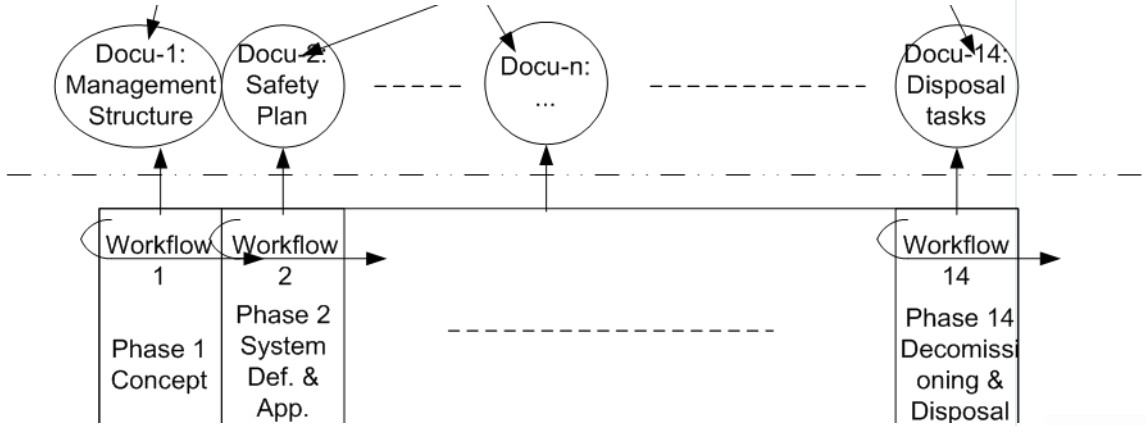
Document
Management System



# “Goal Structuring Notation”

Document database

Document Management System

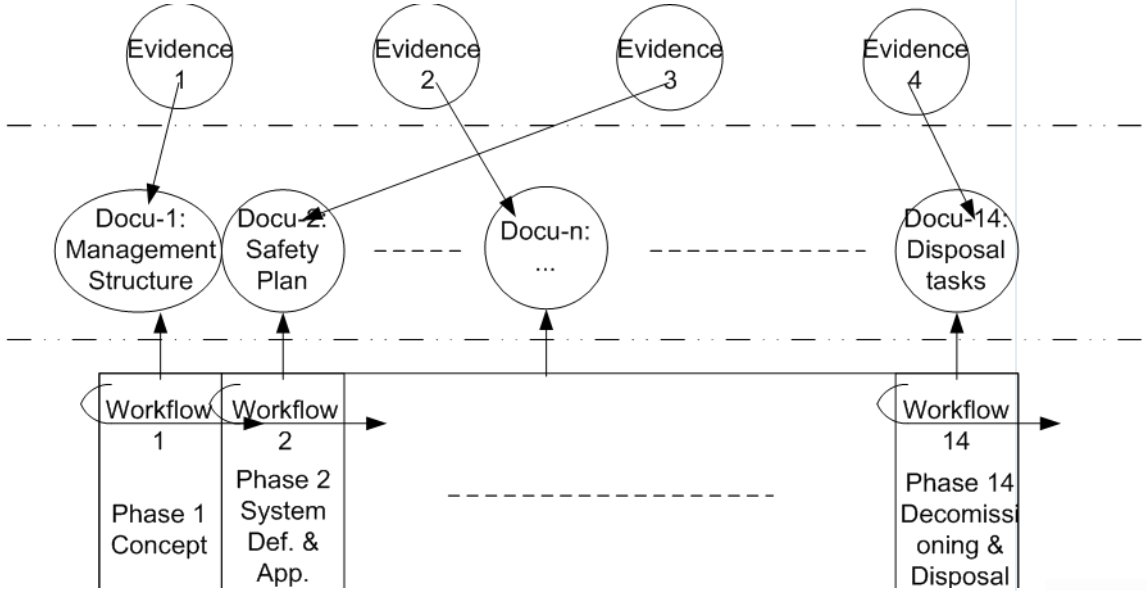


# “Goal Structuring Notation”

Evidence/proof

Document database

Document Management System



# “Goal Structuring Notation”

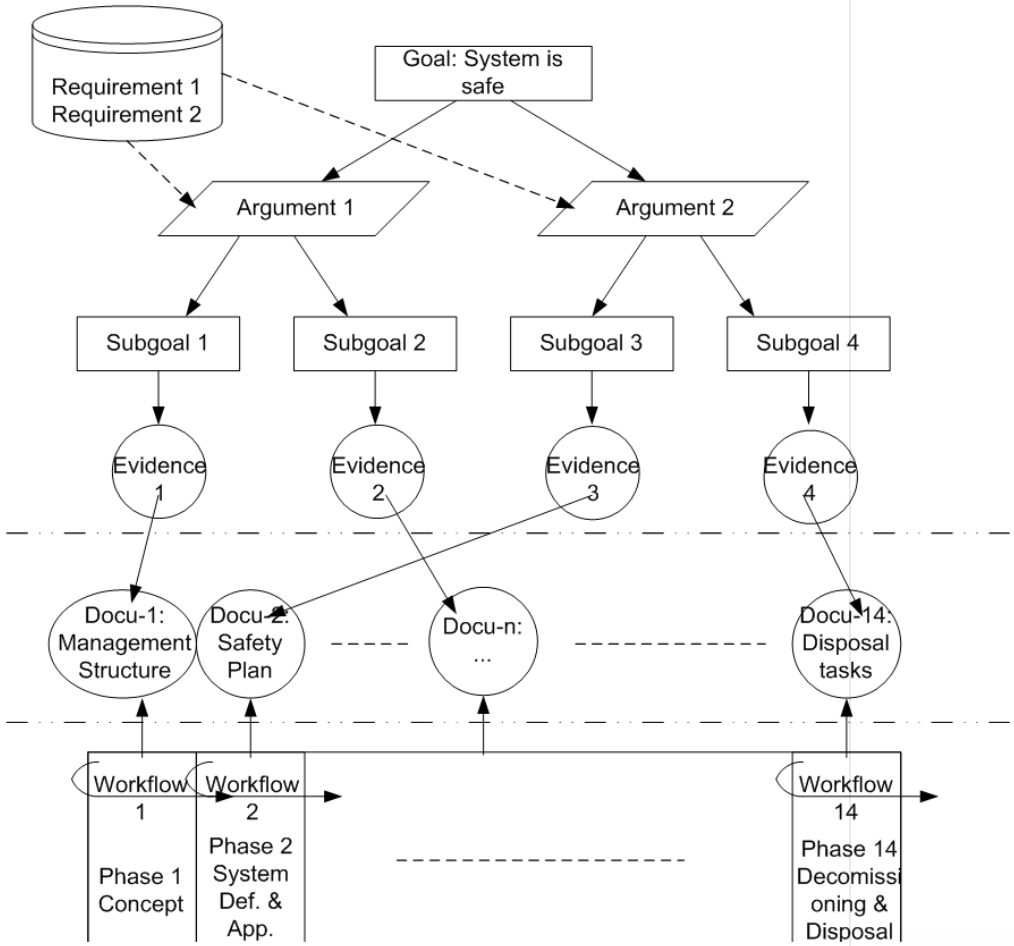
“Goal Structure”

Structured argument

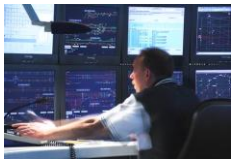
Evidence/proof

Document database

Document Management System



# Benefits of the application




- Offers the creators a clearer overview
- Makes the structured argument easier to understand for the assessor
- Authorities can understand the process more easily
- Modifications can be better identified



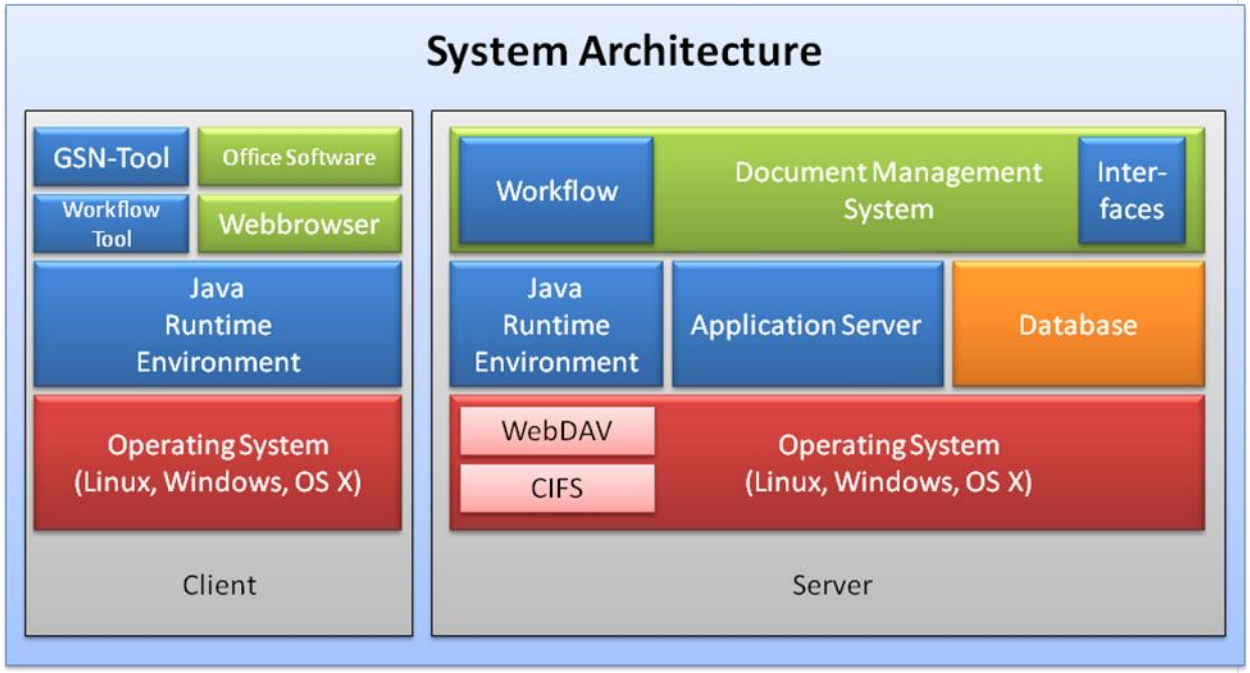
funkwerk
information technologies

# Workstream G's achievements so far

funkwerk
information technologies

# Client/Server System Architecture






GSN = Goal Structuring Notation The Goal-structuring Notation (GSN), developed by the University of York, provides a graphical means of setting out hierarchical Safety Arguments, with textural annotations and references to supporting Evidence

funkwerk information technologies

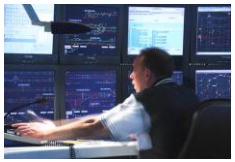
# Enterprise Content Management with Alfresco

- License-free, Java-based open source application for Enterprise Content Management (ECM)
- J2EE Architecture
- Scalable and expandable
- Document Management System (DMS)
- Integration with Microsoft Office products
- Access to documents via a web browser, Windows Explorer (WebDAV) or directly through Office programs
- Workflow tool jBPM (Business Process Management)
- CMIS interface (GSN tool connection)



funkwerk
information technologies

# Alfresco workflow tool

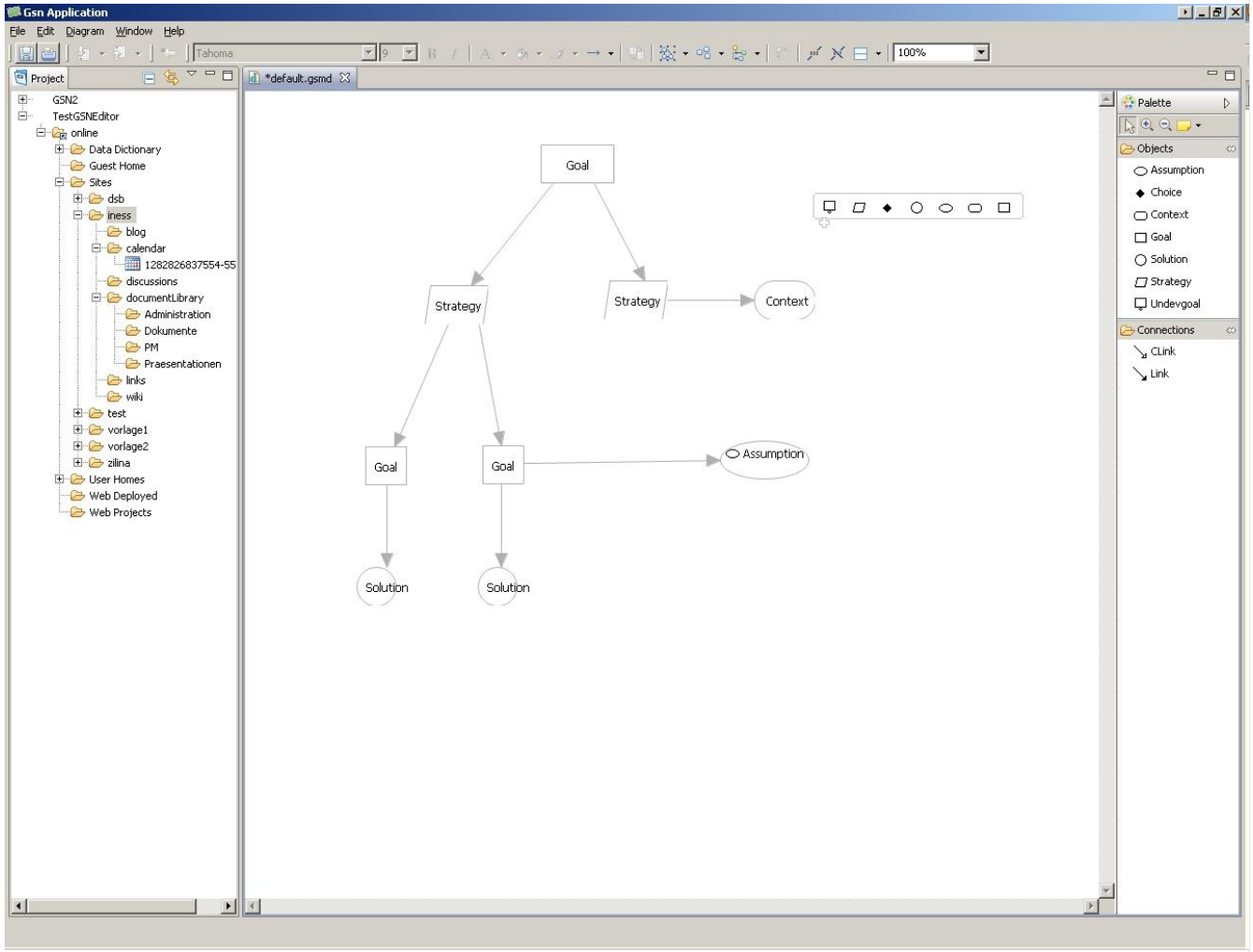



- Document management and control
- Individual workflows can be generated
- Related resources can be added (documents)
- Users can be defined and informed
- Processing status is displayed on the dashboard
- jBPM Graphical Designer facilitates the generation of workflows

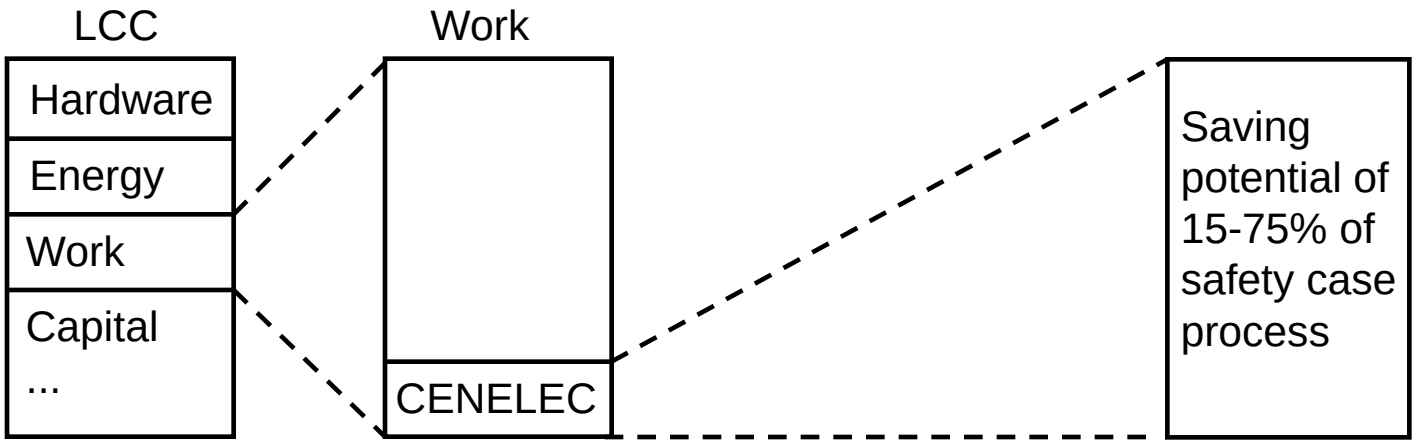


funkwerk
information technologies

# Example of the GSN tool via CMIS connected with Alfresco



# Estimation of economical benefit as part of the LCC




The estimated saving potential from safety case process amounts to between 15% and 75% (i.e. 10-15% of the total development costs)

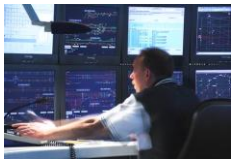
This saving depends on:

- Complexity, size and duration of the project
- Staff competence
- Basis of comparison, i.e. past experience with safety case process



funkwerk information technologies

# Prospects




- In the final year of INESS a prototype project will be adopted to identify useful applications
- The tool should above all be user-friendly and scalable. All the participants are looking for “actual” uses and not theoretical ones.

If the INESS tool is adopted and deployed, the process of creating a safety case will be standardised.

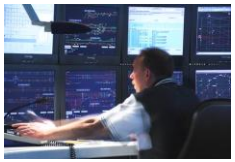
The overview will be more readily available.

**In consequence all participants will profit from reduced processing times.**



funkwerk
information technologies

# INESS




**INESS is thus contributing to the modernisation of the railways by harmonising safety cases**

funkwerk
information technologies

# Thank you very much for your attention!

funkwerk
information technologies