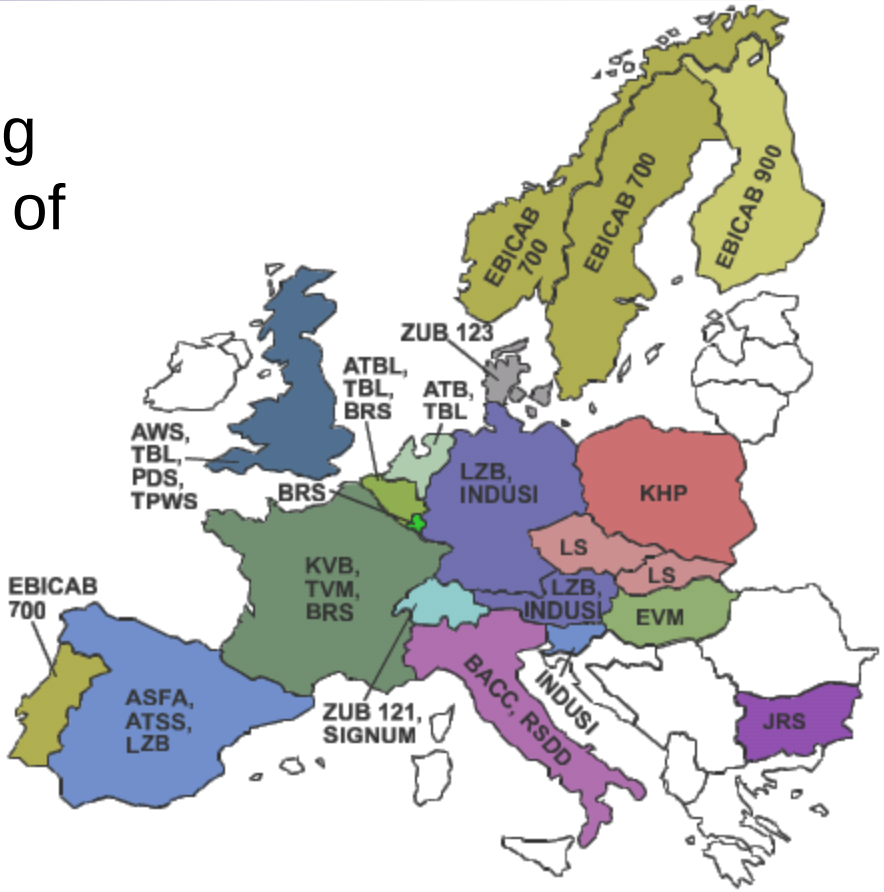
Supporting the Safety Management – Automated Safety Case Processes

Jörg R. Müller, Eckehard Schnieder
Institute for Traffic Safety and Automation Engineering
Technical University Braunschweig, Germany

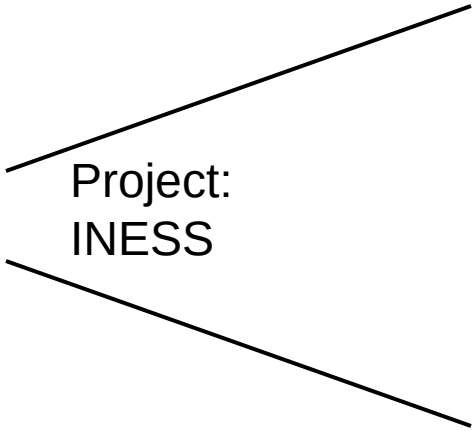
The work has been funded by the 7th framework program of the EU

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit

- 20 nation-specific rail signalling and speed control systems all of which are completely incompatible with each other.
- This leads to additional costs and increased risks of breakdowns.
- ERTMS aims to remedy this lack of unification in the signalling and speed control.

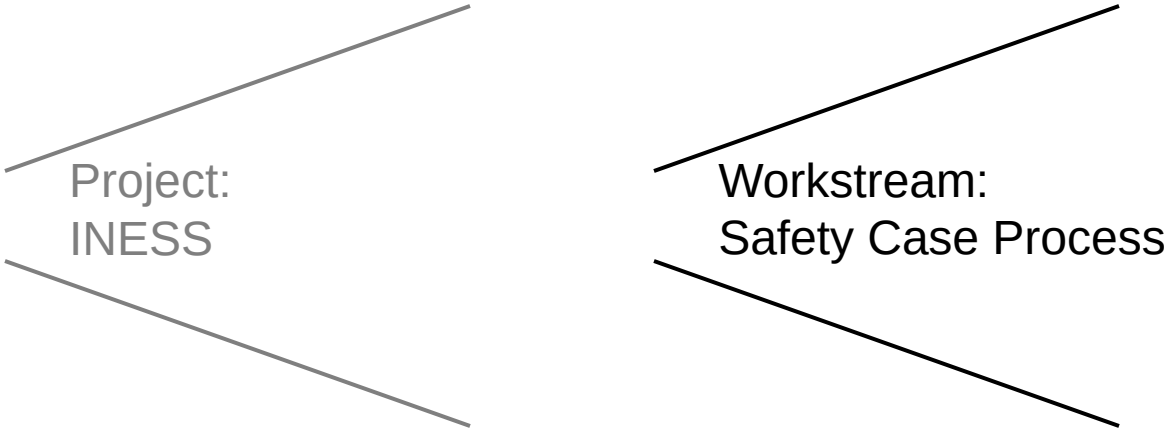


- One important method for reducing costs (of signalling renewal) is considered to be the introduction of a greater degree of standardisation.



The European project called “INESS – **In**tegrated **E**uropean **S**ignalling **S**ystem“ aims at defining and developing specifications for a new generation of interoperable interlocking systems suitable to be integrated in ERTMS systems, with the objective of making the migration to ERTMS more cost-effective.

→ Standardize the core of interlocking systems.



One part of INESS deals with the safety case process.

The aim of this “workstream” is to reduce time and money for the development of the safety case in industry, i.e. operators as well as suppliers, by avoiding unnecessary or redundant procedures.

→ Improve the performance of the Safety Case Process.

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit

EUROPEAN STANDARD **EN 50126**

NORME E

EUROPÄ

ICS 29.280; 45.

EUROPEAN STANDARD **EN 50128**

NORME EUROPÉENNE

EUROPÄI

ICS 29.280; 45.060.1

EUROPEAN STANDARD **EN 50129**

NORME EUROPÉENNE

EUROPÄISCHE NORM February 2003

ICS 93.100 Supersedes ENV 50129:1998

English version

Railway applications –
Communication, signalling and processing systems –
Safety related electronic systems for signalling

Applications ferroviaires –
Systèmes de signalisation,
de télécommunications et de traitement -
Systèmes électroniques de sécurité
pour la signalisation

Bahnanwendungen -
Telekommunikationstechnik,
Signaltechnik und
Datenverarbeitungssysteme -
Sicherheitsrelevante elektronische
Systeme für Signaltechnik

This European Standard was approved by CENELEC on 2002-12-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Ref. No. EN 50129:2003 E

For the approval process of railway operating systems the CENELEC norms EN 50126, 50128 and 50129 are obligatory standards for European countries. The norms describe the life cycle process for safety relevant railway systems that is integrated into the development process.

Even though the norms have been published and used for about 10 years now, there seem time consuming difficulties that hinder an efficient handling of the safety case process.

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

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.”
[3, UK Defence Standard]

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

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.”
[3, UK Defence Standard]

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

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.”
[3, UK Defence Standard]

?

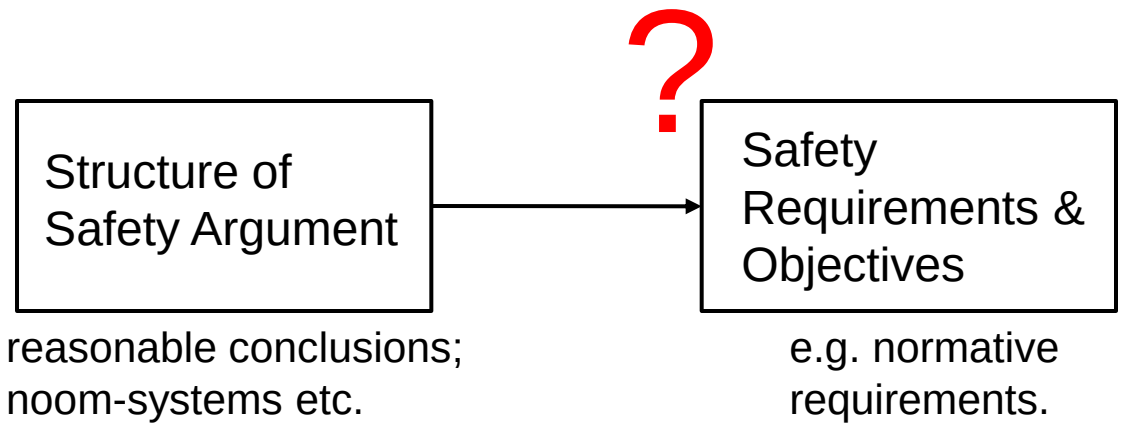
Safety Requirements & Objectives

e.g. normative requirements.

A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

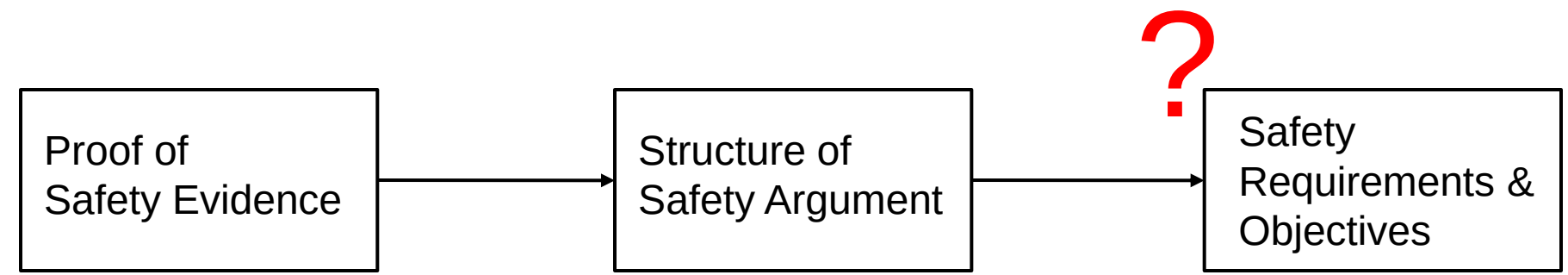
A safety case is “A *structured argument*, supported by a *body of evidence* that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.”
[3, UK Defence Standard]



A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

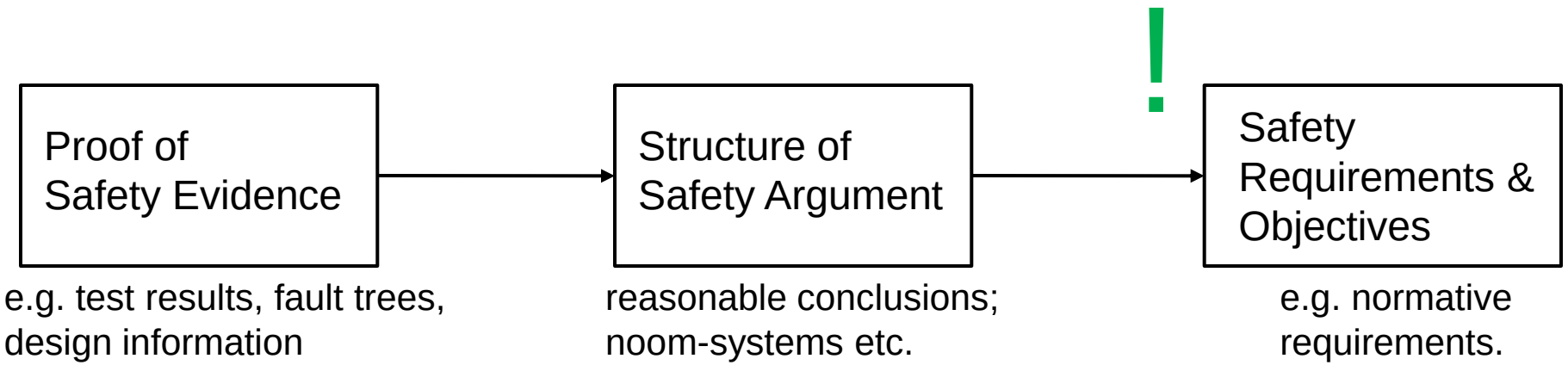
A safety case is “A *structured argument*, supported by a *body of evidence* that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.”
[3, UK Defence Standard]



A safety case is “the documented demonstration that the product complies with the specified safety requirements.” [1, EN 50129]

“The safety case is a line of argumentation, not just a collection of facts.”[2]

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.”
[3, UK Defence Standard]



The advocate convinces the judge of the innocence of the defendant.

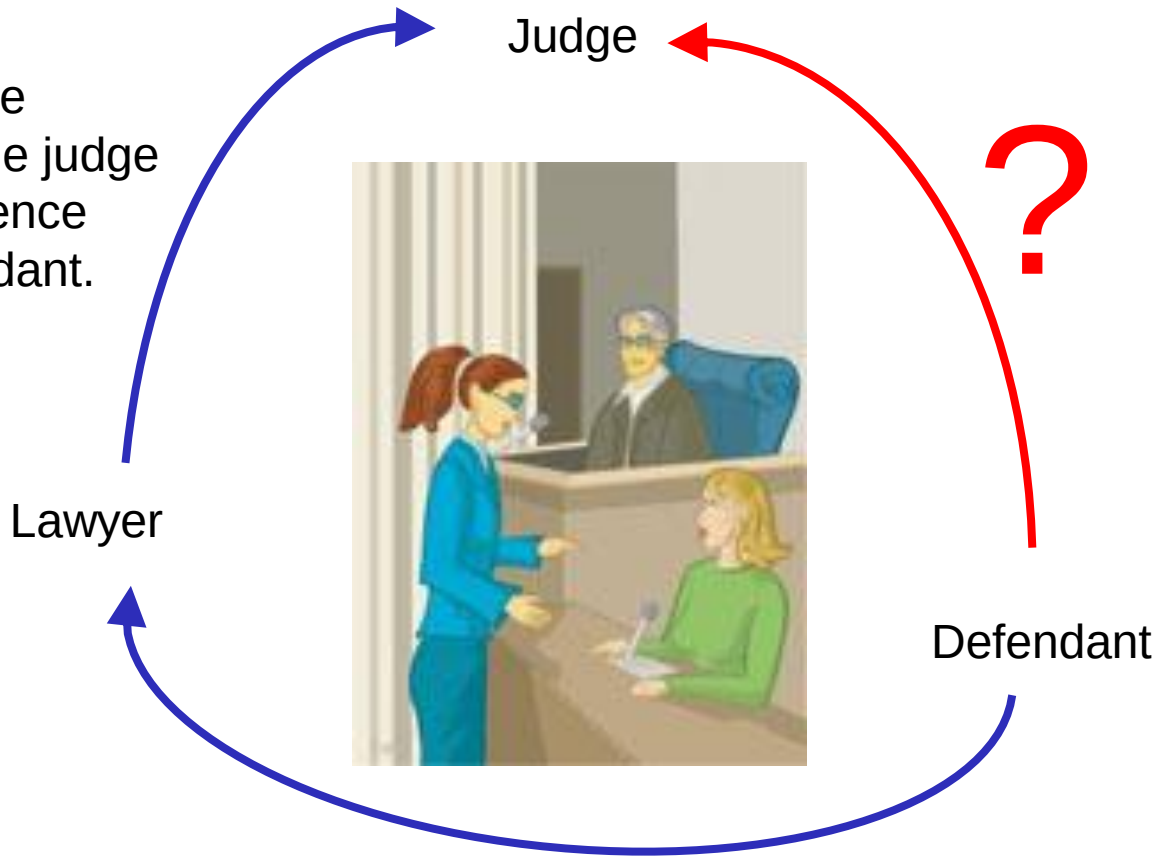
Judge

Lawyer

Defendant

The defendant convinces the lawyer of his innocence.

The advocate convinces the judge of the innocence of the defendant.



The defendant convinces the lawyer of his innocence.

Judge

Conclusion:
Innocent!

Lawyer

arg_1 arg_2

$fact_1$ $fact_2$ $fact_3$ $fact_4$

legislative
background

Defendant

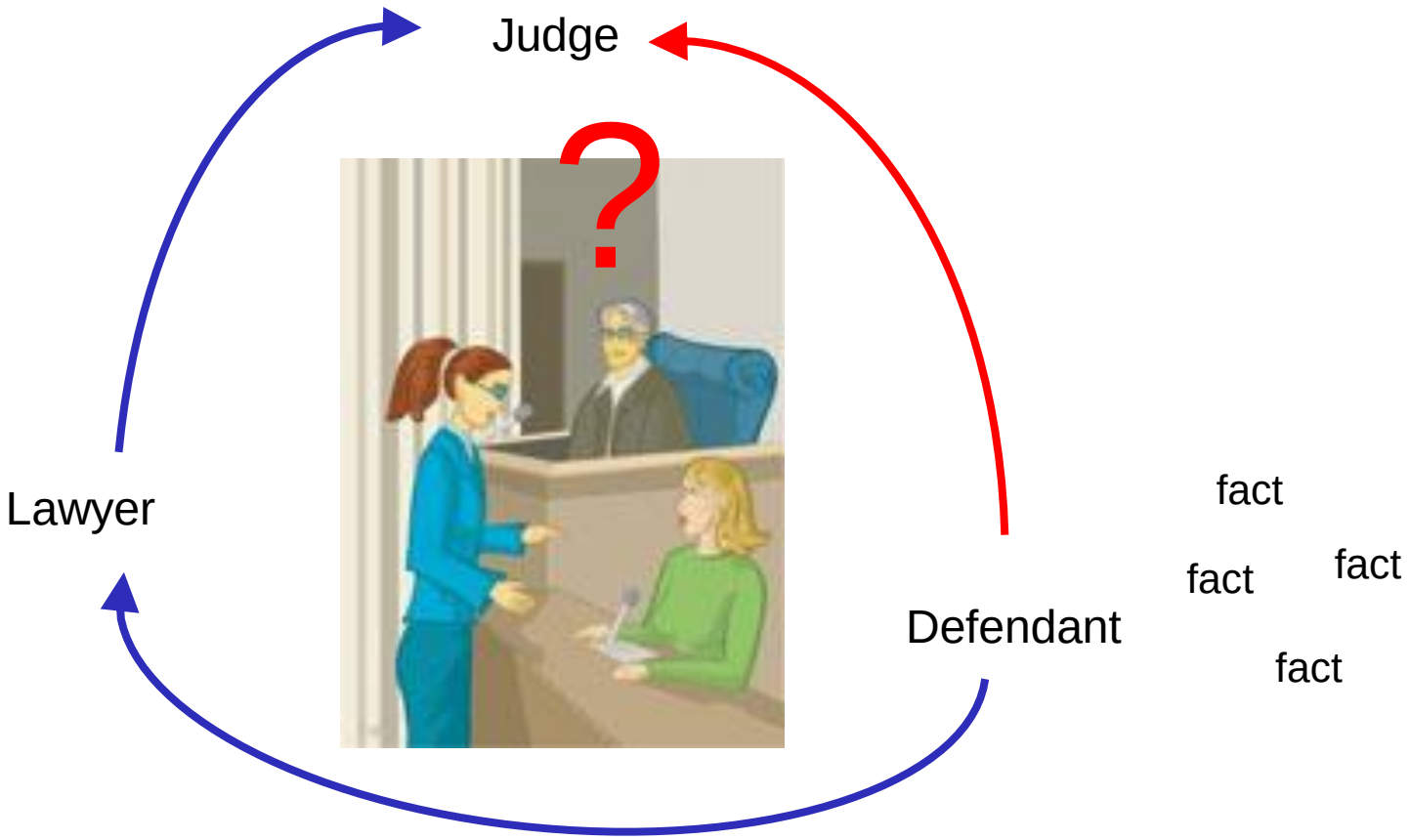
fact

fact fact

fact

structured argument ← body of evidence

The relation between safety cases and court cases



Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
iVA

Conclusion:
Safe!

arg_1 arg_2

$rslt_1$ $rslt_2$ $rslt_3$ $rslt_4$

normative background

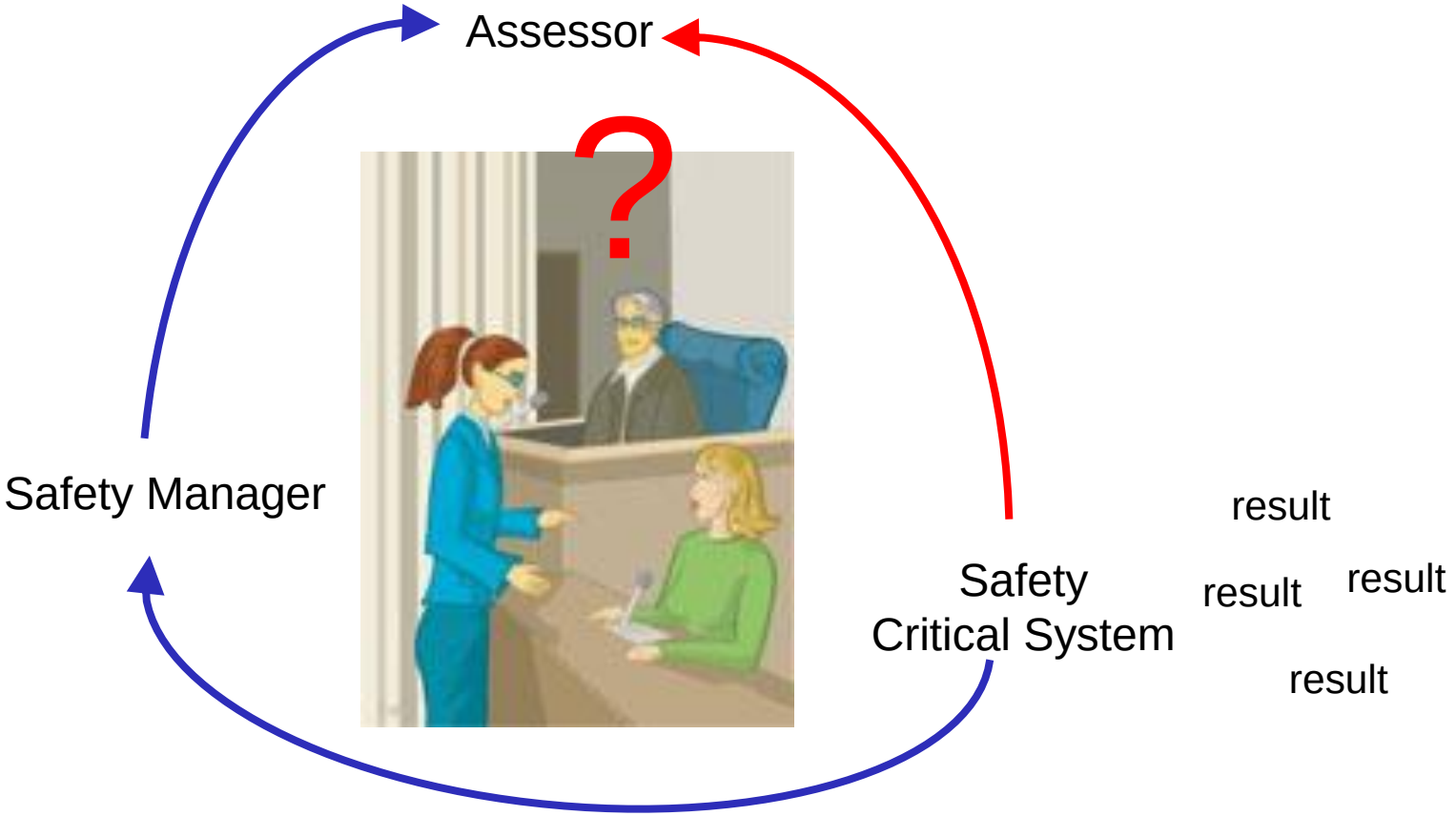
Safety Manager

Safety Defendant

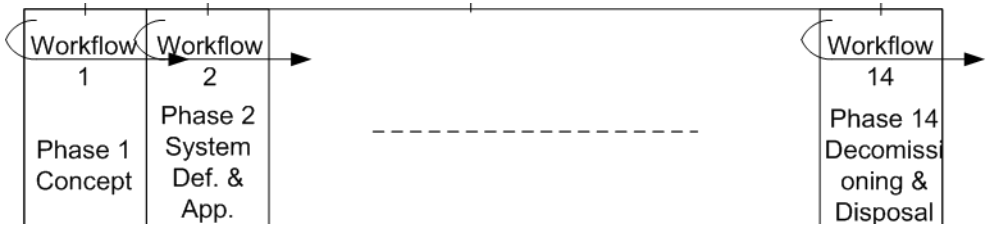
Critical System

structured argument

body of evidence

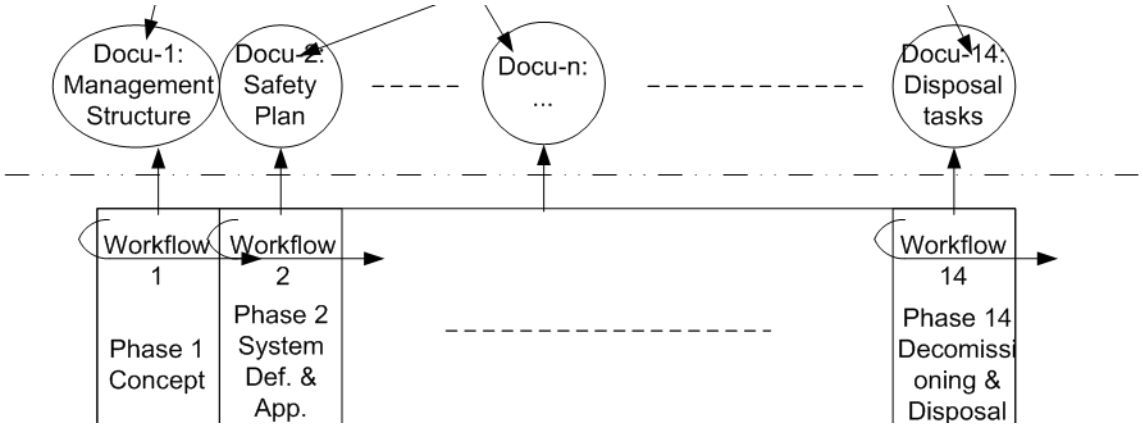

Assessor
?
Safety Manager
Safety Critical System
result
result
result
result

Document
Management System



Database of Documents

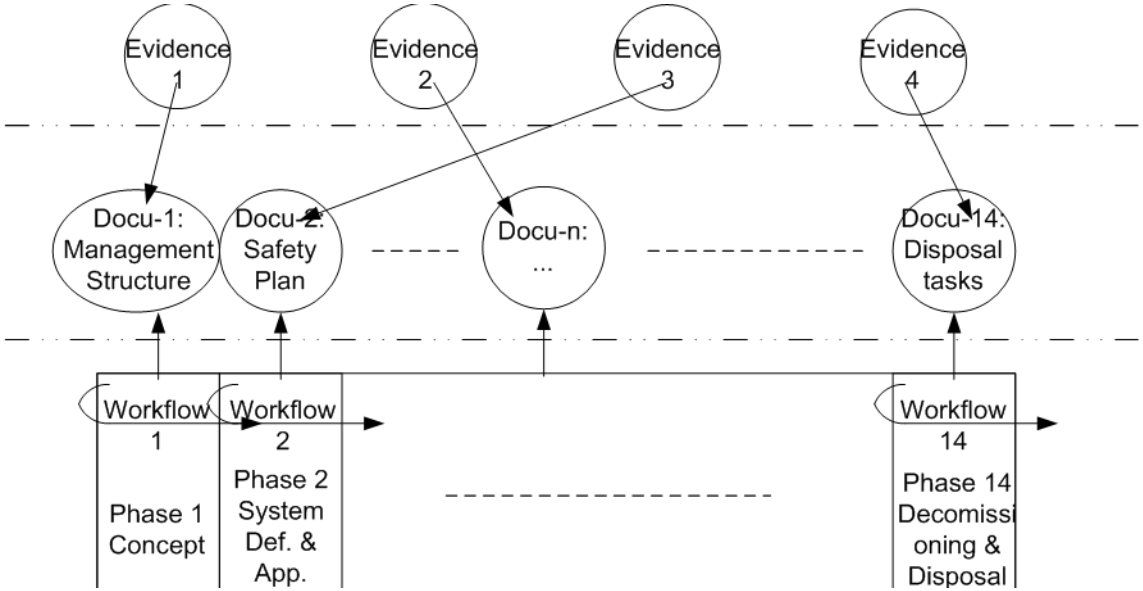
Document Management System



body of evidence

Database of Documents

Document Management System



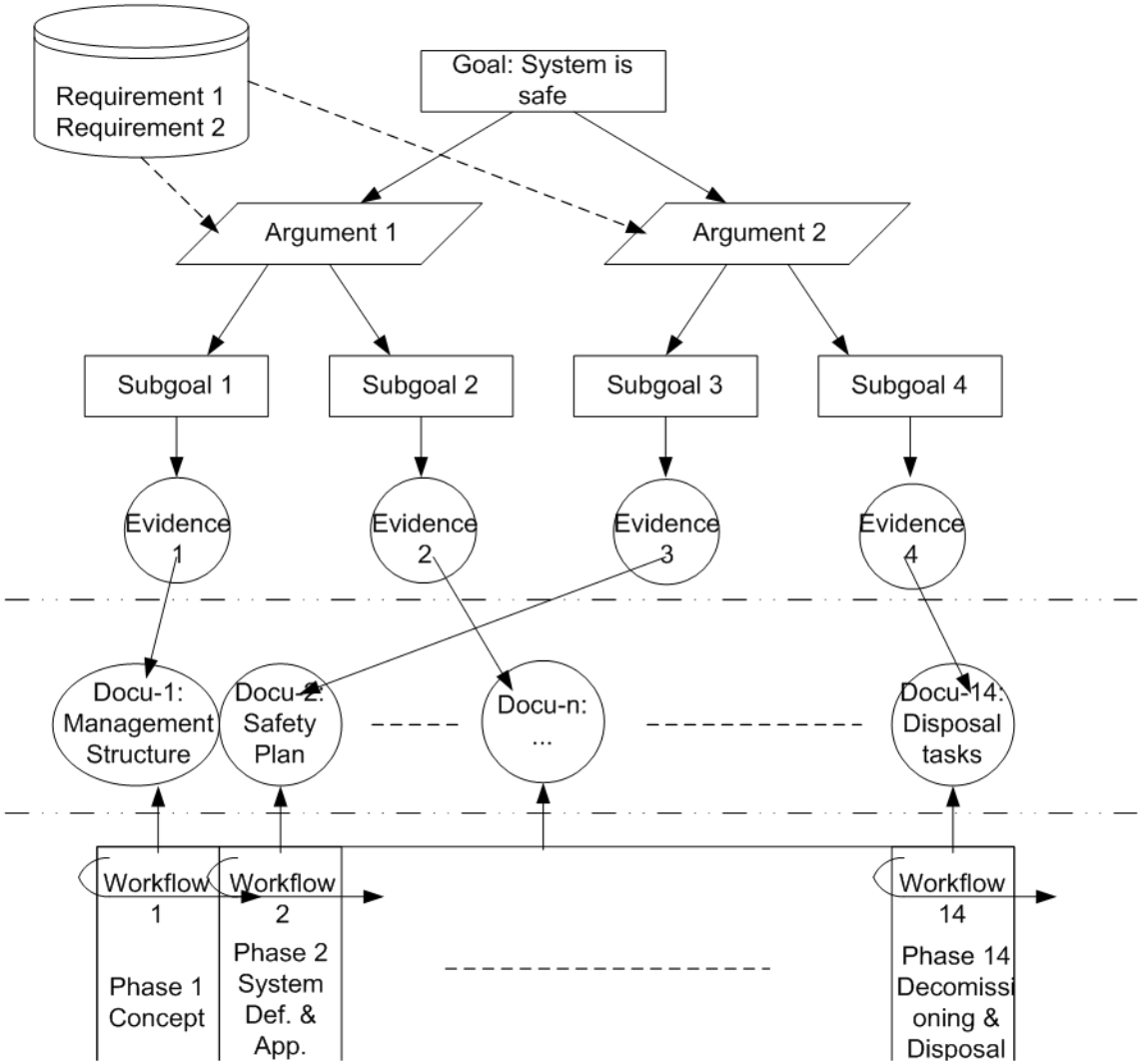
“Goal Structure“

structured argument

body of evidence

Database of Documents

Document Management System



- Legal authorities get a quick overview over the structure of the safety argumentation.
- The safety case writer knows more pecisely what to do and why.

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit

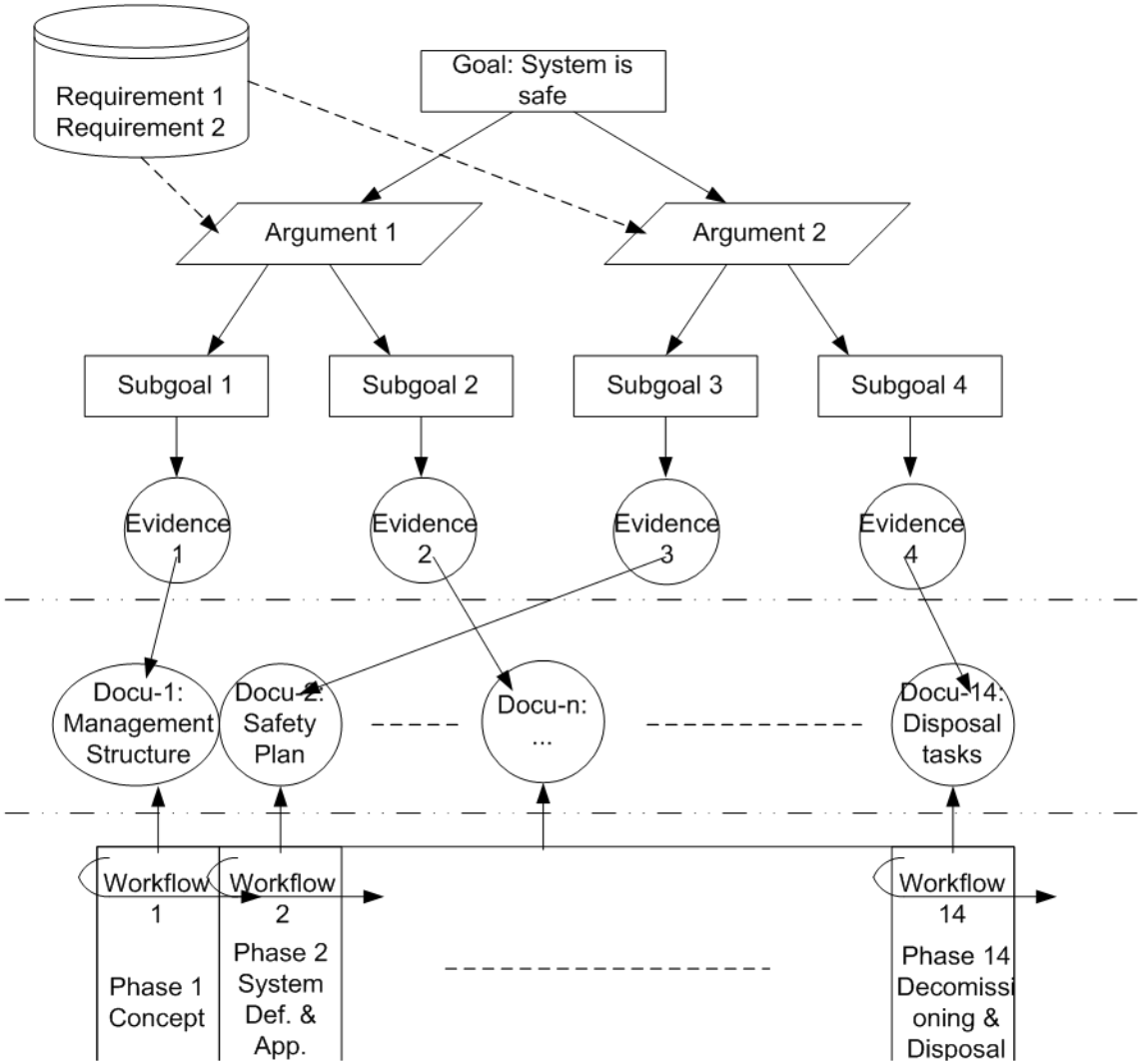
“Goal Structure“

structured argument

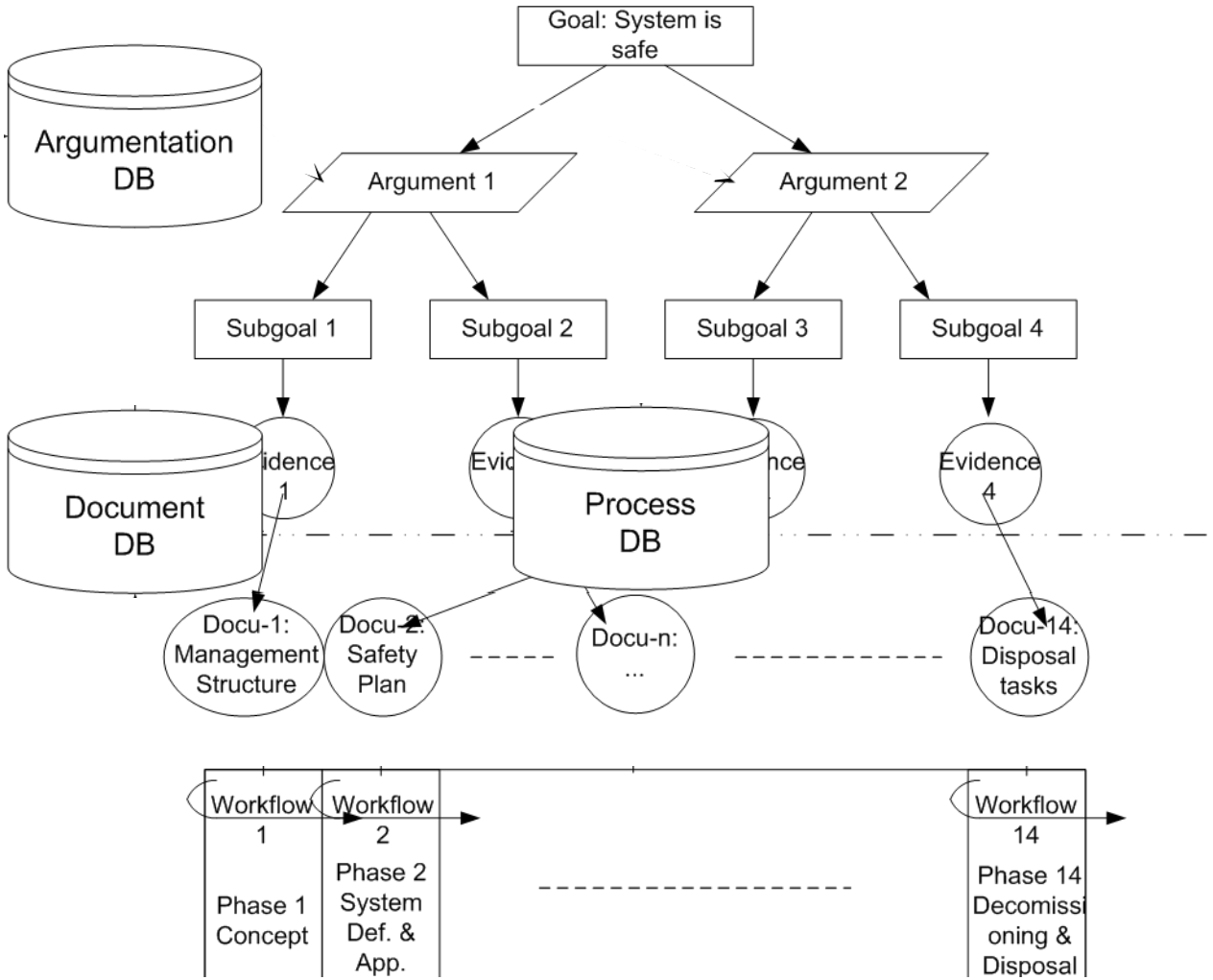
body of evidence

Database of Documents

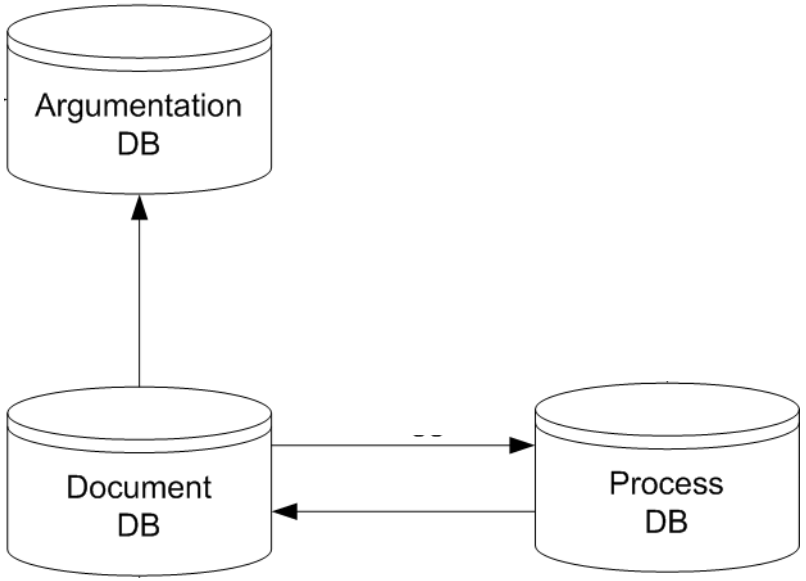
Document Management System

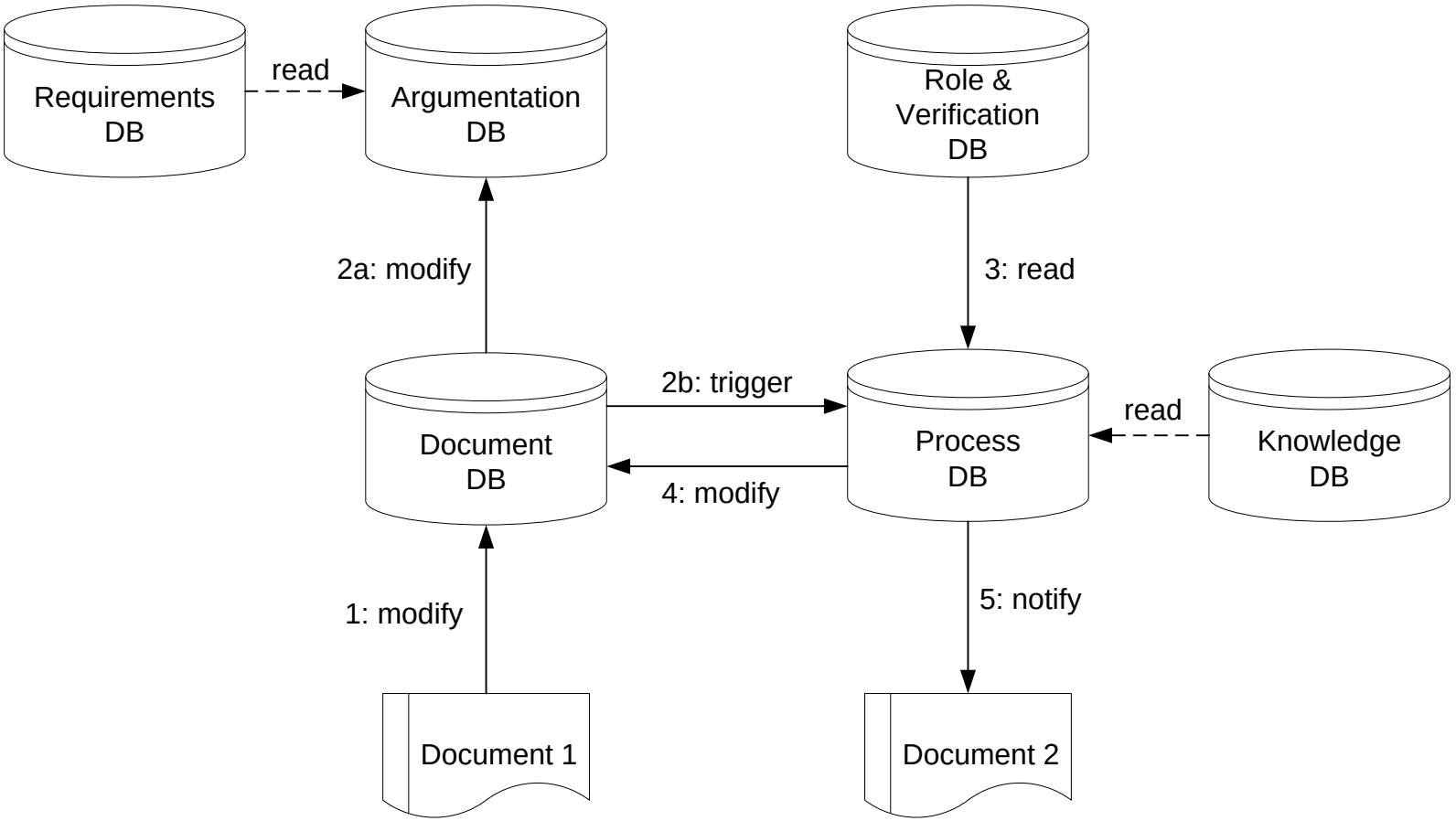


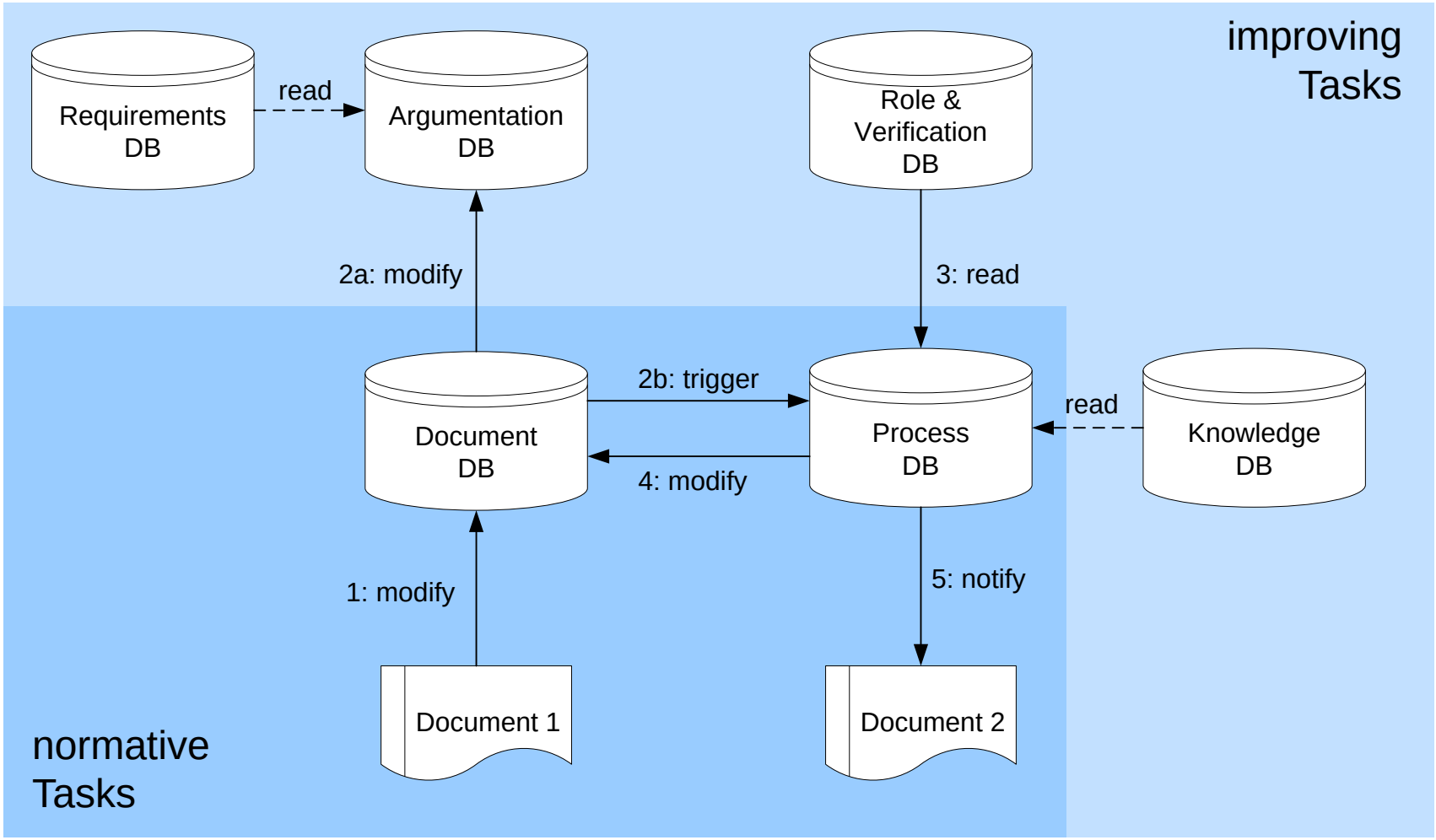
Using various sources of knowledge to support safety case related workflows



Using various sources of knowledge to support safety case related workflows




Requirements DB
read
Argumentation DB
Role & Verification DB
2a: modify
3: read
Document DB
2b: trigger
4: modify
Process DB
read
Knowledge DB
1: modify
5: notify
Document 1
Document 2


improving Tasks
Requirements DB
read
Argumentation DB
Role & Verification DB
2a: modify
3: read
Document DB
2b: trigger
4: modify
Process DB
read
Knowledge DB
1: modify
5: notify
Document 1
Document 2
normative Tasks

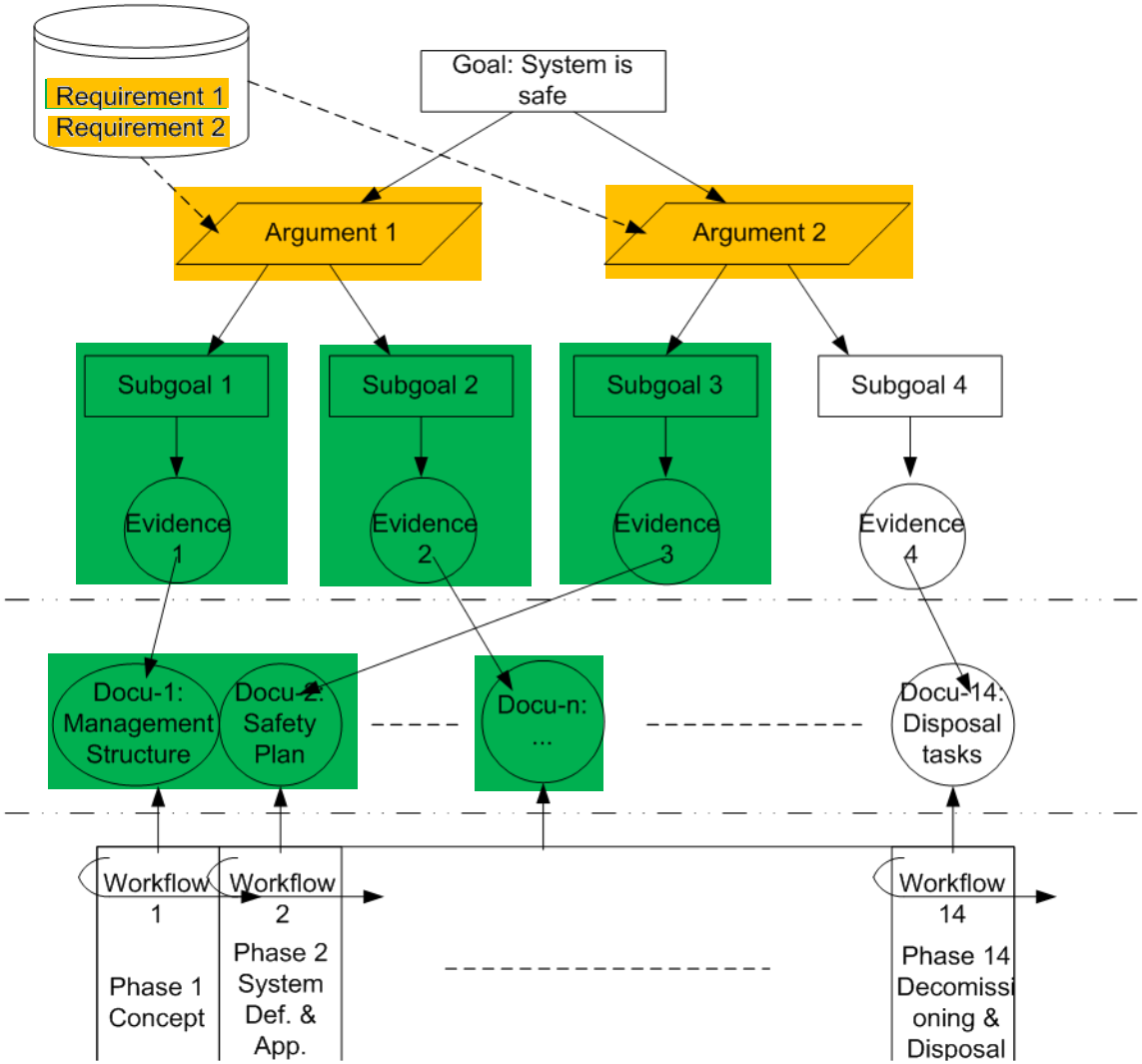
“Goal Structure“

structured argument

body of evidence

Database of Documents

Document Management System

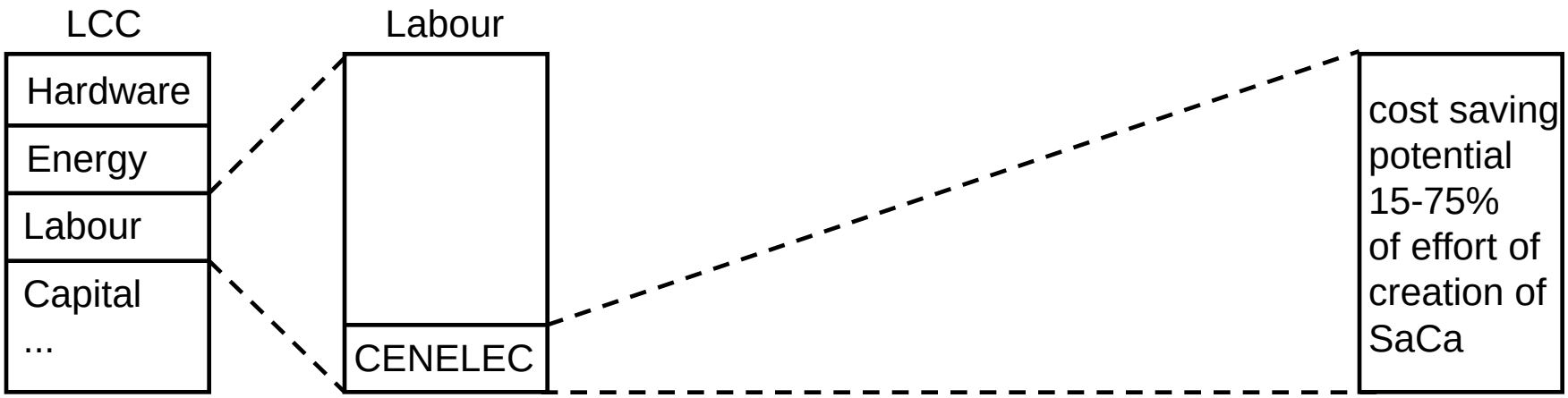


Technical University of Braunschweig
Institute for Traffic Safety and Automation Engineering
iVA

- The safety manager is continuously informed of the actual state of the safety case through continuous and automated update of the safety case status.
- “high level“ requirement tracing.
- The access to the documents is given through links.
- Consistent referencing and versioning.

- Context of the presented work
- Introduction to the 5012x-CENELEC Standards
- Transparency of the Safety Argumentation
- Automated Processes
- Results – estimated economical benefit

What is the expected economical benefit?



The cost saving potential for the creation of the Safety Case varies between 15% and 75% (that means 10-15 % of the overall CENELEC costs).

The broadness of the margin is explained through the following influences:

- The complexity and duration of a project
- The basis of comparison: The benefit of a company following even today exactly the CENELEC processes and using sophisticated SW-tools will be lower than that of the most interviewed partners.

[1] EN 50129: Railway Applications – Communications, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling, 1999.

[2] Odd Nordland: “Safety Case Categories – Which One When?”, Redmill F., Anderson T.(Eds.):”Current Issues in Safety-critical Systems”, 11th Safety-critical Systems Symposium, February 2003 in Bristol, UK, Springer-Verlag London Ltd. 2003.

[3] Ministry of Defence, “Safety Management Requirements for Defence Systems”, Defence Standard 00-56 (Issue 4), U.K. Ministry of Defence, 2007.