Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Unterstützung des Zulassungsverfahrens von Bahnsystemen durch ontologiebasierte Systemmodelle

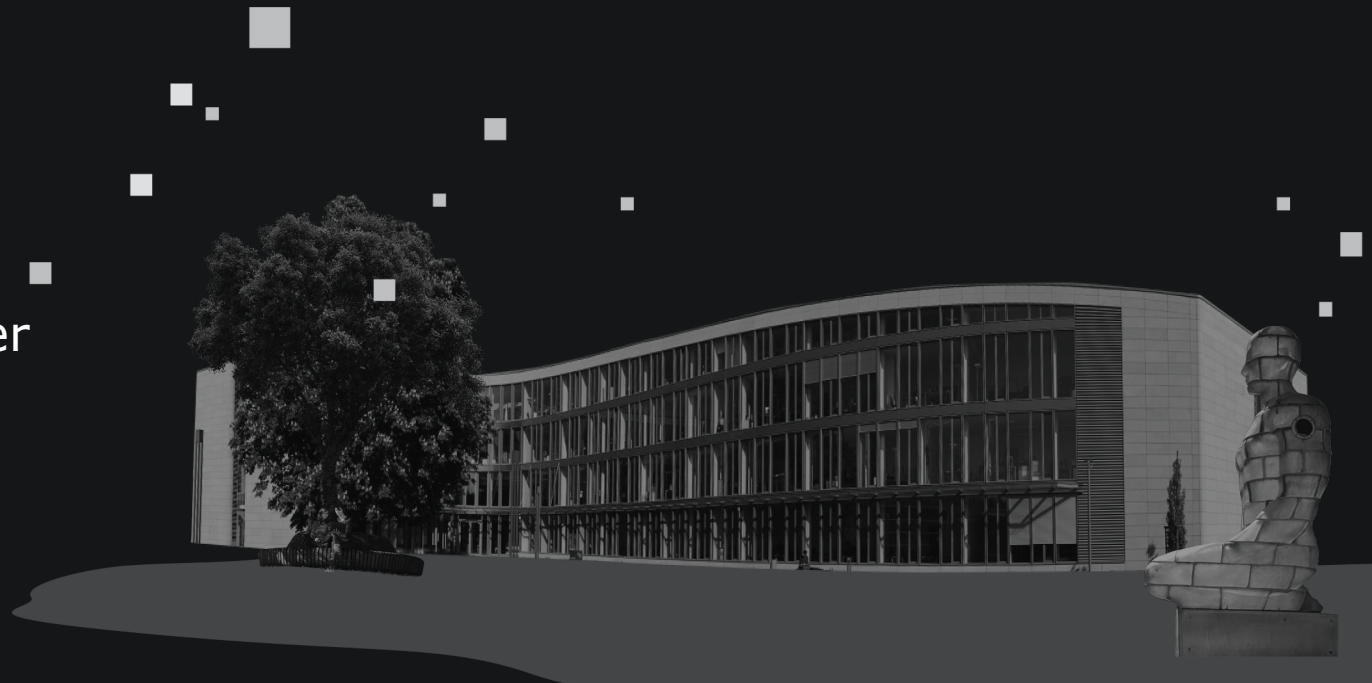
Christian Kaiser

Prof. Dr. Andreas Polze
Fachgebiet für Betriebssysteme und Middleware

Betreuung: Lukas Pirl und Dirk Friedenberger

Design IT.
Create Knowledge.

www.hpi.de



Agenda

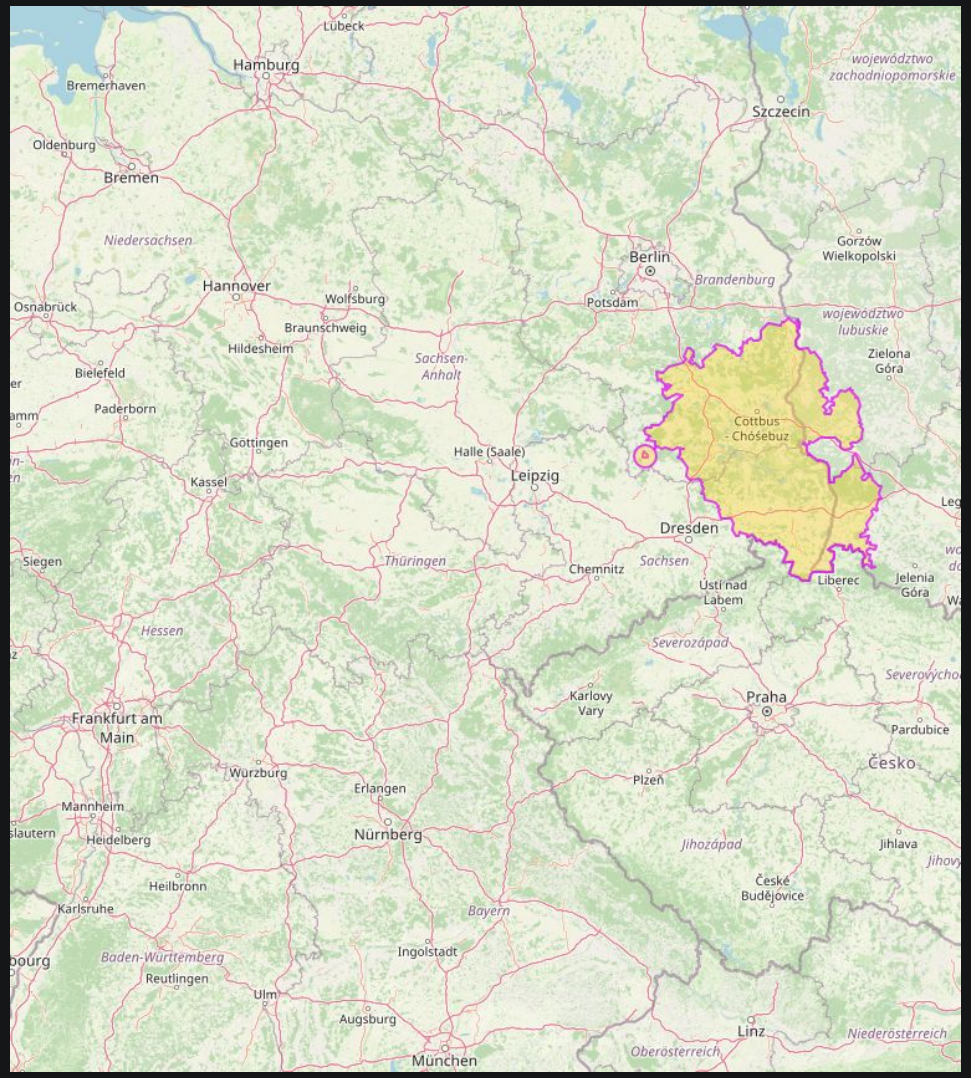
1. Projekthintergründe
2. Zielsetzungen der Arbeit
3. Vom Modell zum Dokument
4. Normativ geforderte Artefakte
5. Fazit und Ausblick

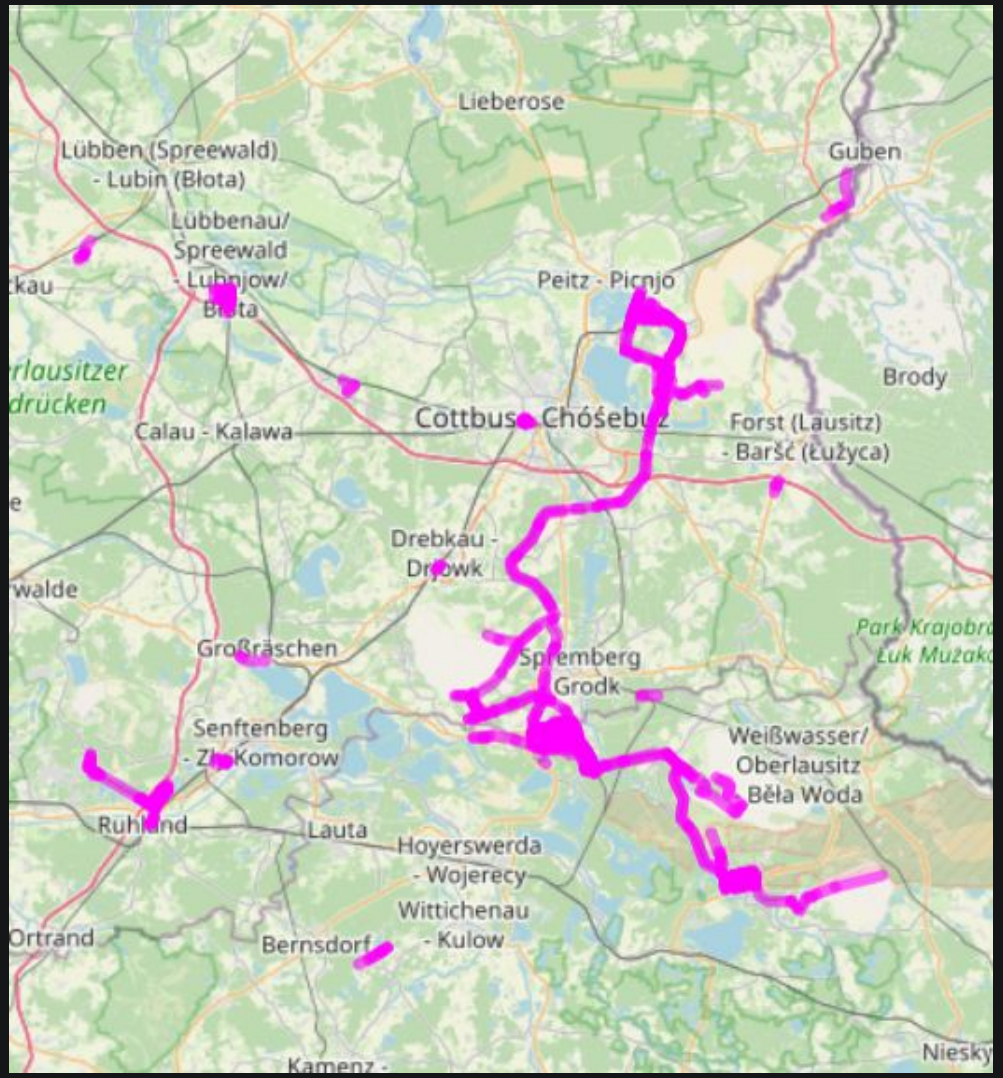
Agenda

1. Projekthintergründe
2. Zielsetzungen der Arbeit
3. Vom Modell zum Dokument
4. Normativ geforderte Artefakte
5. Fazit und Ausblick

Projekthintergründe

FlexiDug





Projekthintergründe
Zugleiter in der Cloud

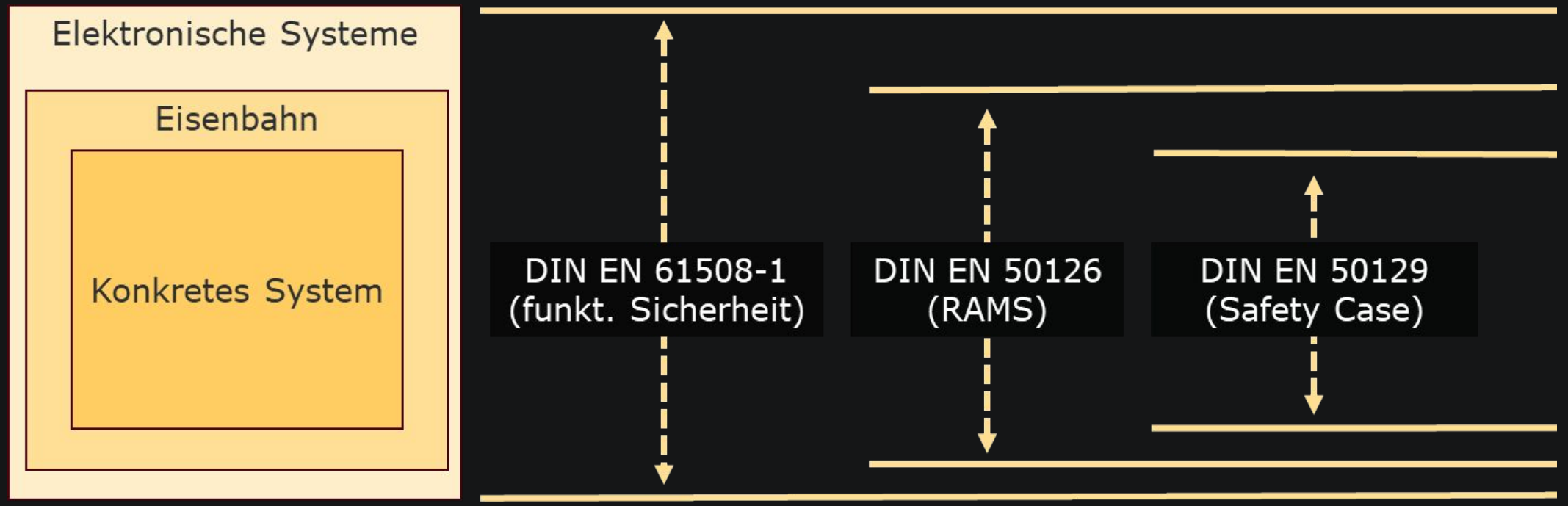
https://kleinbahnwiki.de/images/1/12/Belegblatt.Dornheim.2019.jpg

Projekthintergründe

Normen im Projektkontext

Relevante Normen: DIN EN 61508

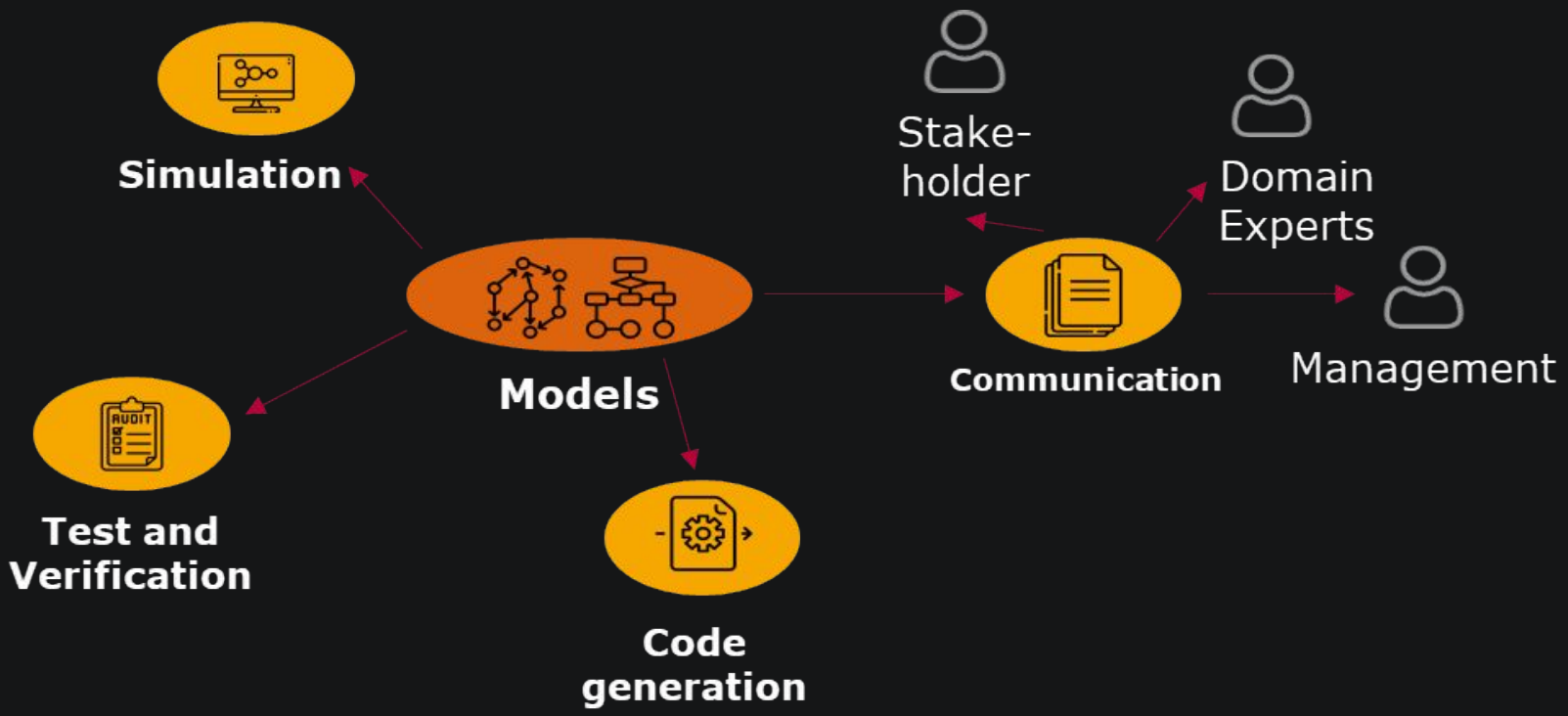
Sektorspezifisch: DIN EN 50126, 50129, 50716



RAMS: Reliability Availability Maintainability Safety

Projekthintergründe
Modellbasierte Softwareentwicklung

"An ontology is a formal explicit specification of a shared conceptualization"
Tom Gruber, Sep. 1992, Universität Stanford



Agenda

1. Projekthintergründe
2. Zielsetzungen der Arbeit
3. Vom Modell zum Dokument
4. Normativ geforderte Artefakte
5. Fazit und Ausblick

Zielsetzung der Arbeit

Forschungsfragen

1. **Forschungsfrage**

   In welchem Umfang können Inhalte eines Sicherheitsberichts nach DIN EN 50129 aus einem ontologiebasierten Ansatz abgeleitet und damit das geforderte Dokument automatisiert erzeugt werden?

2. **Forschungsfrage**

   Welche Implikationen ergeben sich daraus für zukünftige Projekte, insbesondere im Hinblick auf wiederverwendbare Leitlinien?

Agenda

1. Projekthintergründe
2. Zielsetzungen der Arbeit
3. Vom Modell zum Dokument
4. Normativ geforderte Artefakte
5. Fazit und Ausblick

Vom Modell zum Dokument

Modelldefinition

Ontologie-Modelle

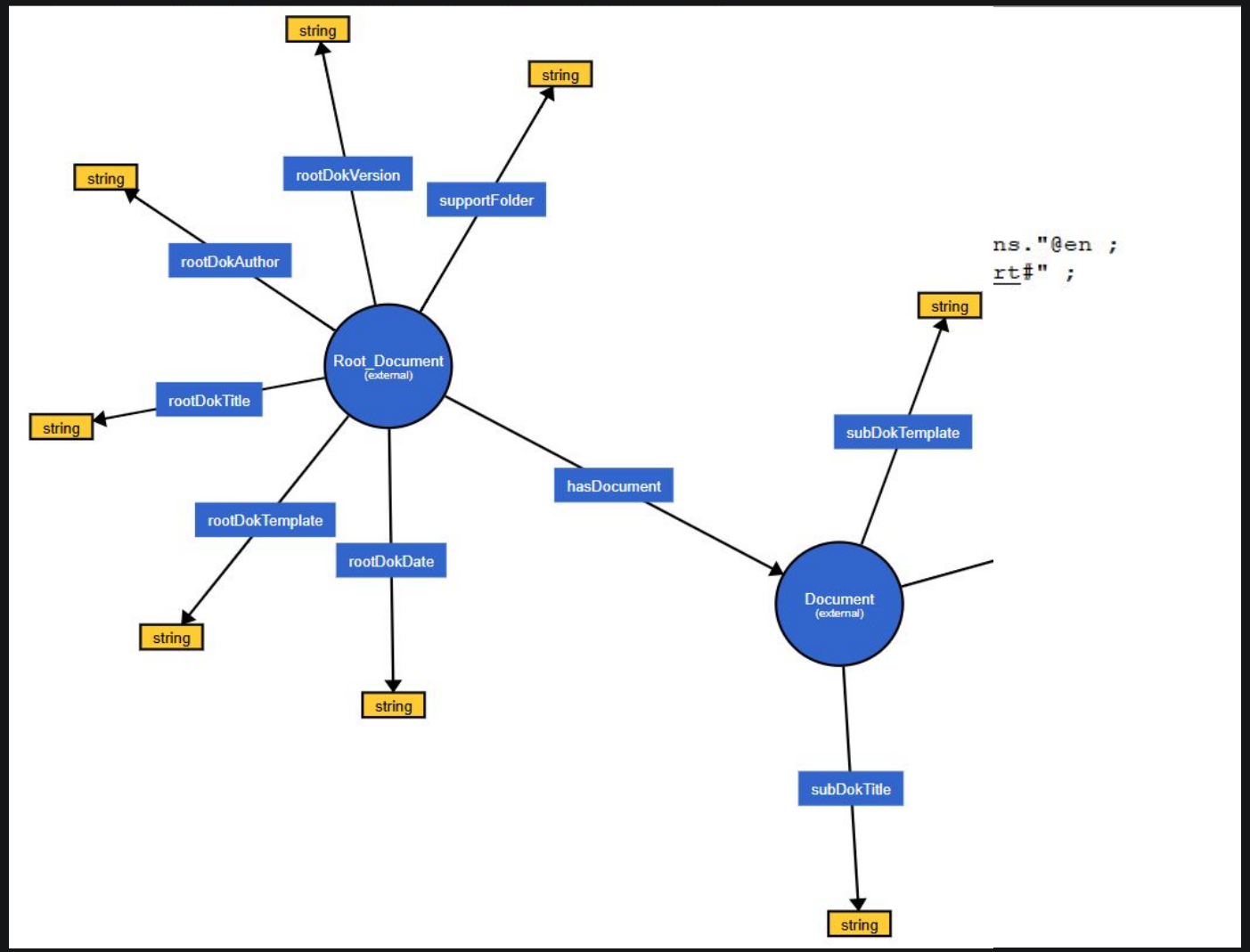
Key-Value Store

Dokumenten-gerüst

Abbildungen

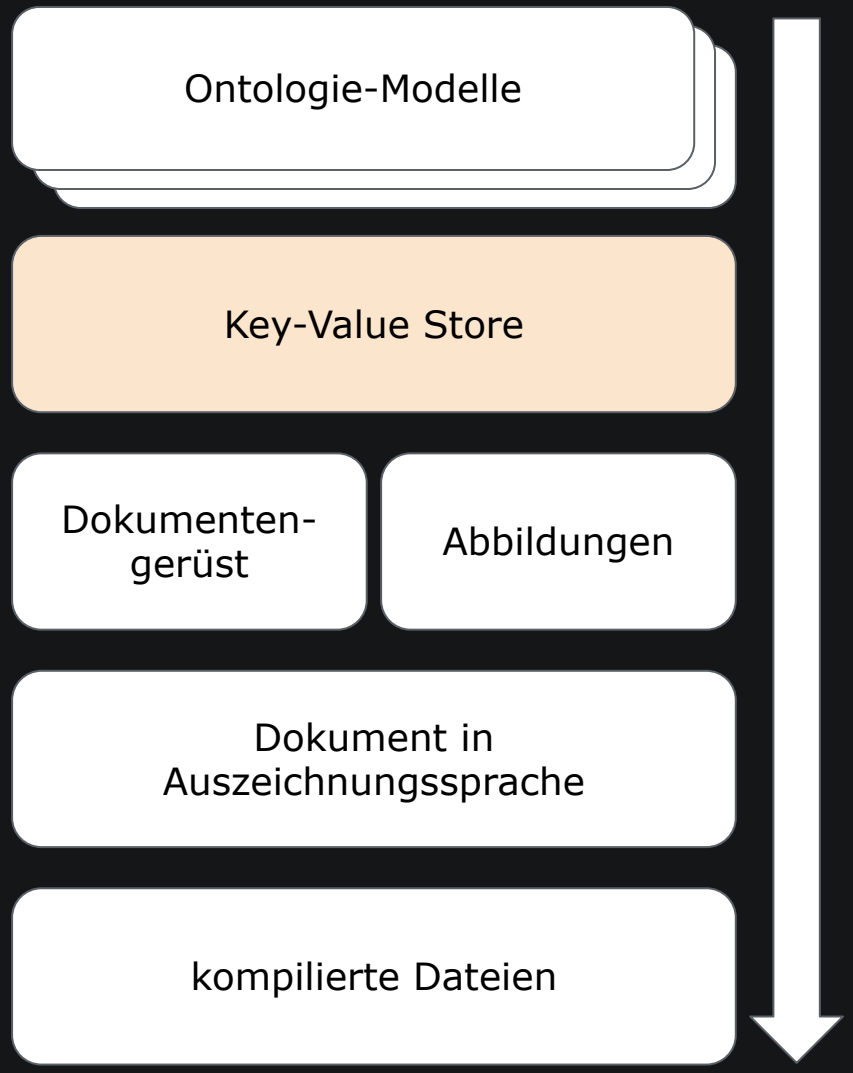
Dokument in Auszeichnungssprache

kompilierte Dateien



Vom Modell zum Dokument

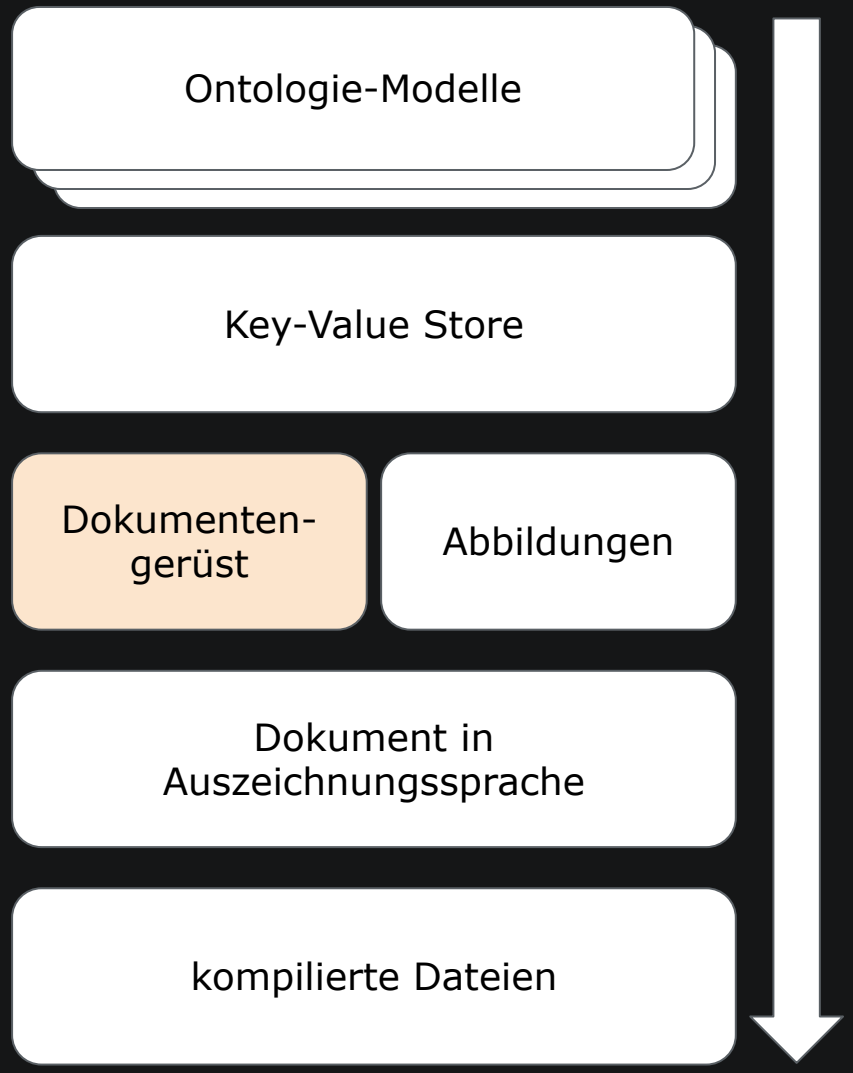
Instanziierung des Modells




```
<https://frittenburger.de/2022/11/EULYNX#Dictionary-Sicherheitsbericht> a asset:Dictionary ;
    rdfs:label "Dictionary"^^xsd:string ;
    asset:hasKeyValuePair [ a asset:KeyValuePair ;
            asset:key "partials" ;
            asset:value [ a asset:Dictionary ;
                    asset:hasKeyValuePair [ a asset:KeyValuePair ;
                            asset:key "Sicherheitsbericht" ;
                            asset:value "SafetyReport.adoc.mustache" ],
                        [ a asset:KeyValuePair ;
                            asset:key "Systemdefinition" ;
                            asset:value "Systemdefinition.adoc" ],
                        [ a asset:KeyValuePair ;
                            asset:key "Qualitätsmanagementbericht" ;
                            asset:value "Qualitymanagement.adoc" ],
                        [ a asset:KeyValuePair ;
                            asset:key "techn. Sicherheitsbericht" ;
                            asset:value "technicalSafety.adoc" ],
                        [ a asset:KeyValuePair ;
                            asset:key "Zusammenfassung" ;
                            asset:value "conclusion.adoc" ],
                        [ a asset:KeyValuePair ;
                            asset:key "Sicherheitsmanagementbericht" ;
                            asset:value "safetymanagement.adoc" ] ] ],
        [ a asset:KeyValuePair ;
            asset:key "data" ;
            asset:value [ a asset:Dictionary ;
                    asset:hasKeyValuePair [ a asset:KeyValuePair ;
                            asset:key "documents" ;
```

Vom Modell zum Dokument

Strukturen und Templates




```
= {{title}}
:doctype: book
:front-cover-image: image::logo.png[width=150, align=center]
:page-layout: title
:author: {{metadata.author}}
:email: {{metadata.author_email}}
:revnumber: {{metadata.version}}
:revdate: {{metadata.date}}

<<<

:toc:
:toclevels: 3
:sectnums:

:leveloffset: +1
{{#documents}}

{{#dynamic_section}}{{/dynamic_section}}

{{/documents}}
:leveloffset: -1
```

Vom Modell zum Dokument

Strukturen und Templates

Ontologie-Modelle

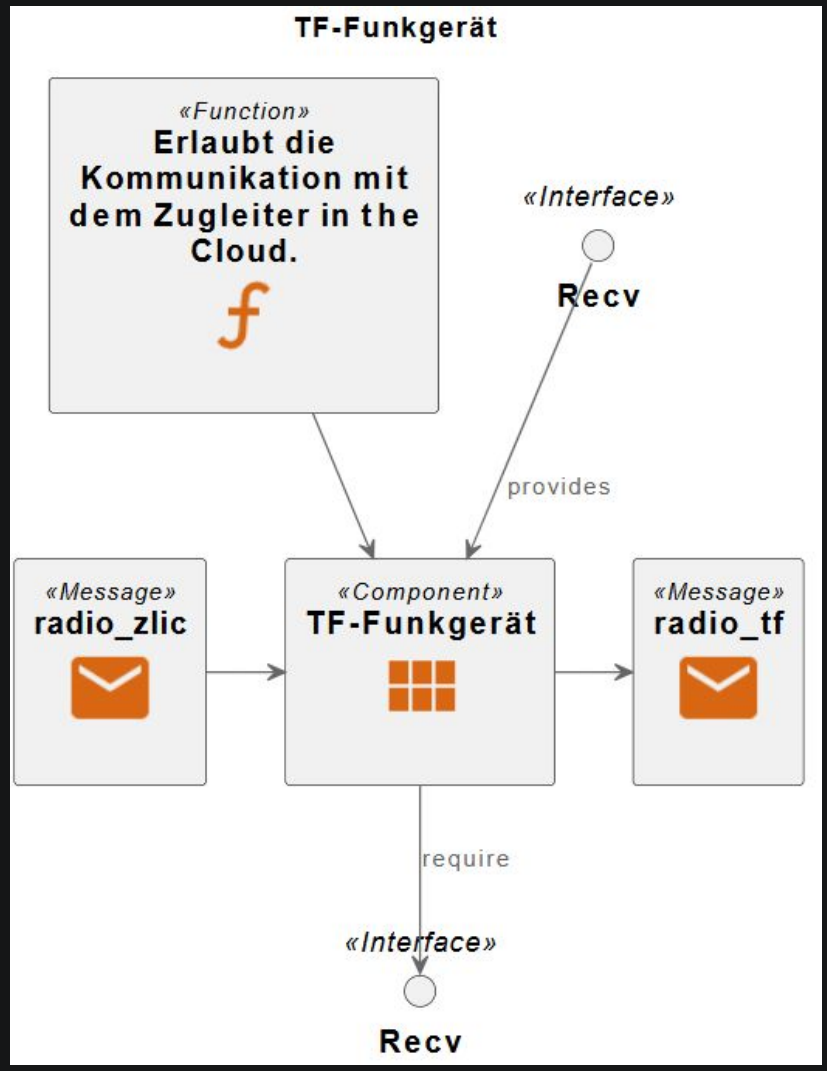
Key-Value Store

Dokumenten-gerüst

Abbildungen

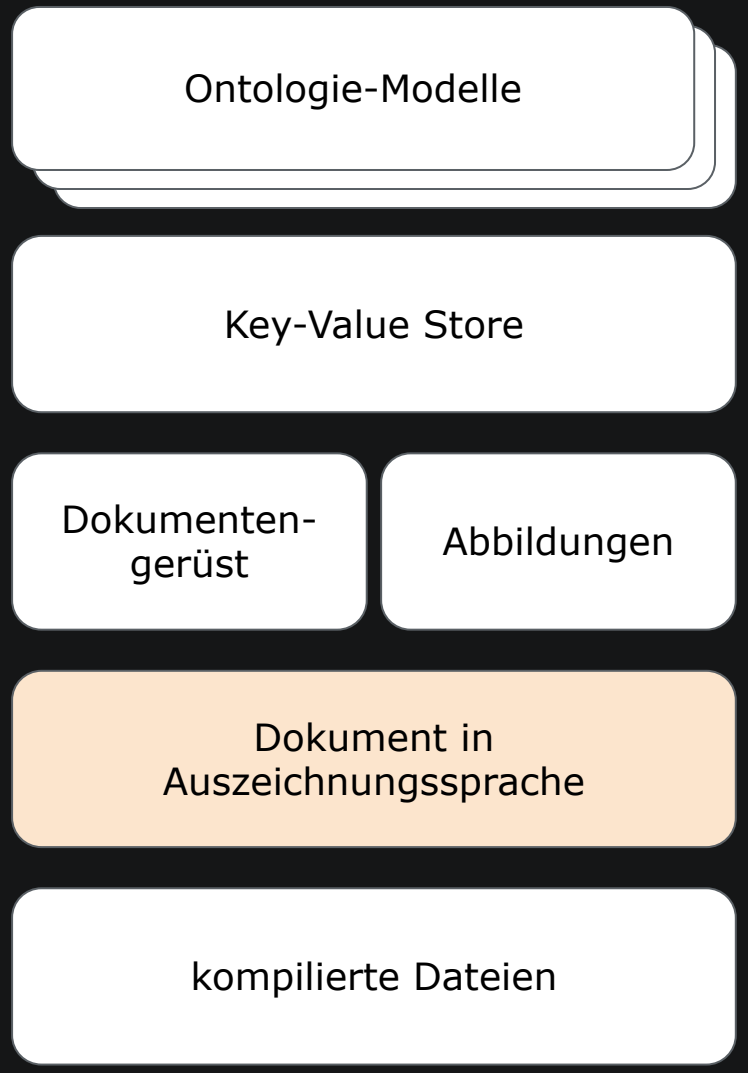
Dokument in Auszeichnungssprache

kompilierte Dateien



Vom Modell zum Dokument

Ergebnis der Integration




```
= Sicherheitsbericht
:doctype: book
:front-cover-image: image::logo.png[width=150, align=center]
:page-layout: title
:author: Christian Kaiser
:email: christian.kaiser@student.hpi.uni-potsdam.de
:revnumber: f8bd525275ebae5b4cb1032a04e114434db73c83
:revdate: 10.06.2025 10:58:58 Uhr

<<<

:toc:
:toclevels: 3
:sectnums:

:leveloffset: +1

= Systemdefinition

Der Zugleiter in der Cloud (im Folgenden abgekürzt als ZliC)
```

Vom Modell zum Dokument

Ergebnis der Integration

Ontologie-Modelle

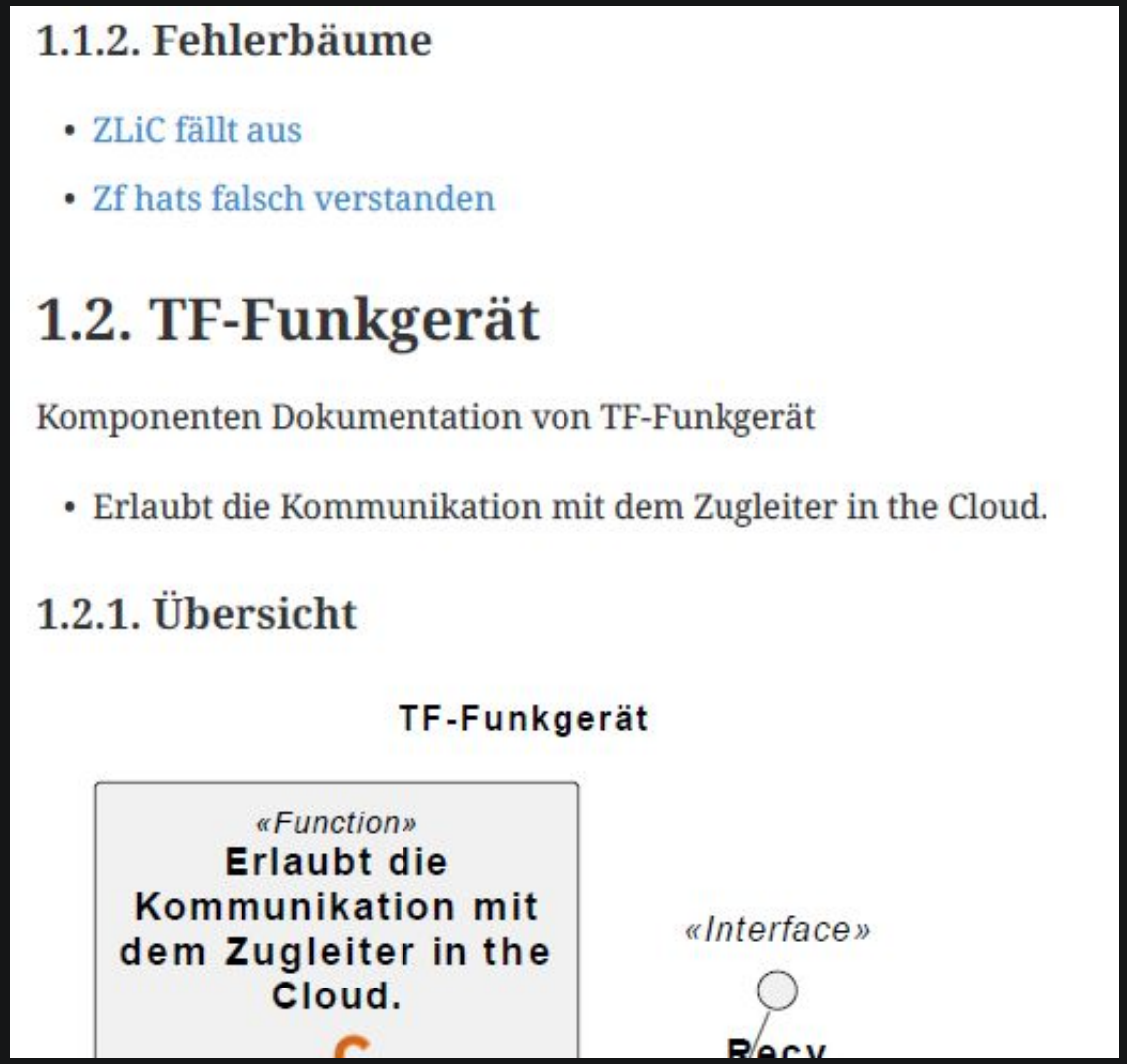
Key-Value Store

Dokumenten-gerüst

Abbildungen

Dokument in Auszeichnungssprache

kompilierte Dateien



1.1.2. Fehlerbäume

- ZLiC fällt aus
- Zf hats falsch verstanden

1.2. TF-Funkgerät

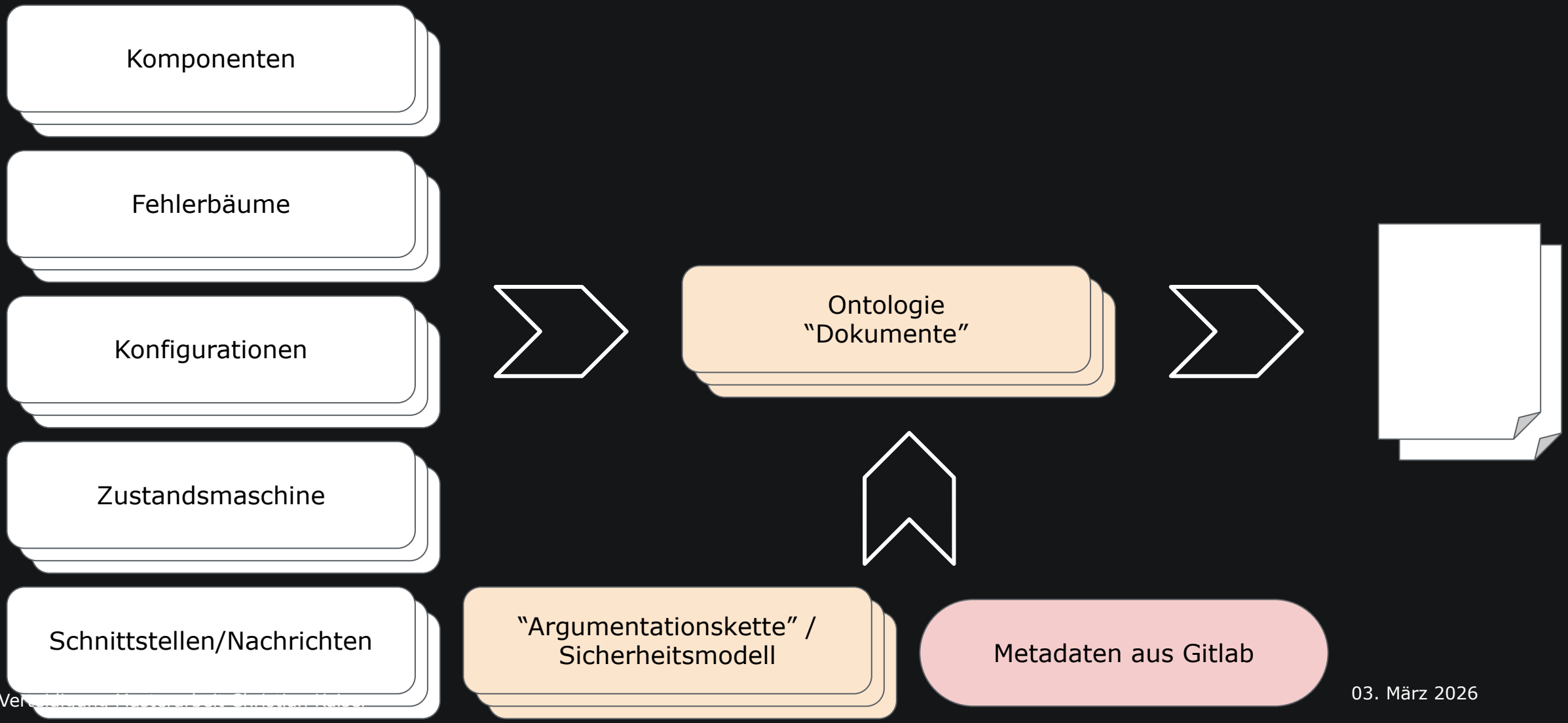
Komponenten Dokumentation von TF-Funkgerät

- Erlaubt die Kommunikation mit dem Zugleiter in the Cloud.

1.2.1. Übersicht

Vom Modell zum Dokument

Strukturierte Erfassung der Inhalte



Vom Modell zum Dokument

Sicherheitsargumentation

1 — 2 — 3 — 4 — 5

Gefährdungen

Erfassen der (sicherheitsrelevanten) Gefährdungen

Eigenschaften: Risikowert, primäres Schutzziel, primäres Asset

Anforderungen

Erfassen der resultierenden Anforderungen

Eigenschaften: SIL, Maßnahme gg. Risiko

Funktion

Welche Funktion implementiert die Anforderung

Eigenschaften: SIL

Komponente

Verknüpfung zum Modell der Komponenten

Nachweis

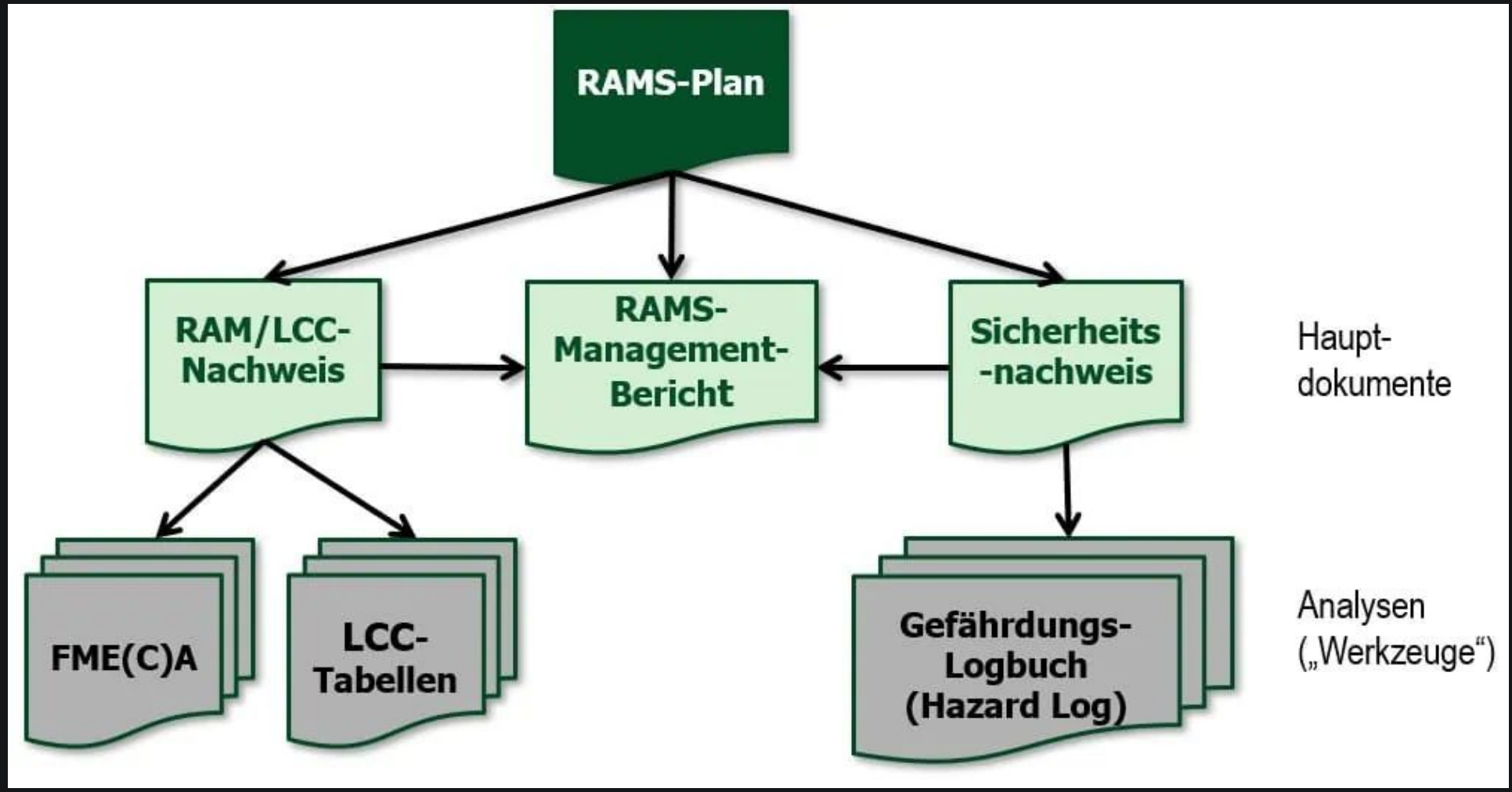
Nachweis zum korrekten Verhalten der Funktion und zur Erfüllung der Anforderung

Agenda

1. Projekthintergründe
2. Zielsetzungen der Arbeit
3. Vom Modell zum Dokument
4. Normativ geforderte Artefakte
5. Fazit und Ausblick

Normativ geforderte Inhalte

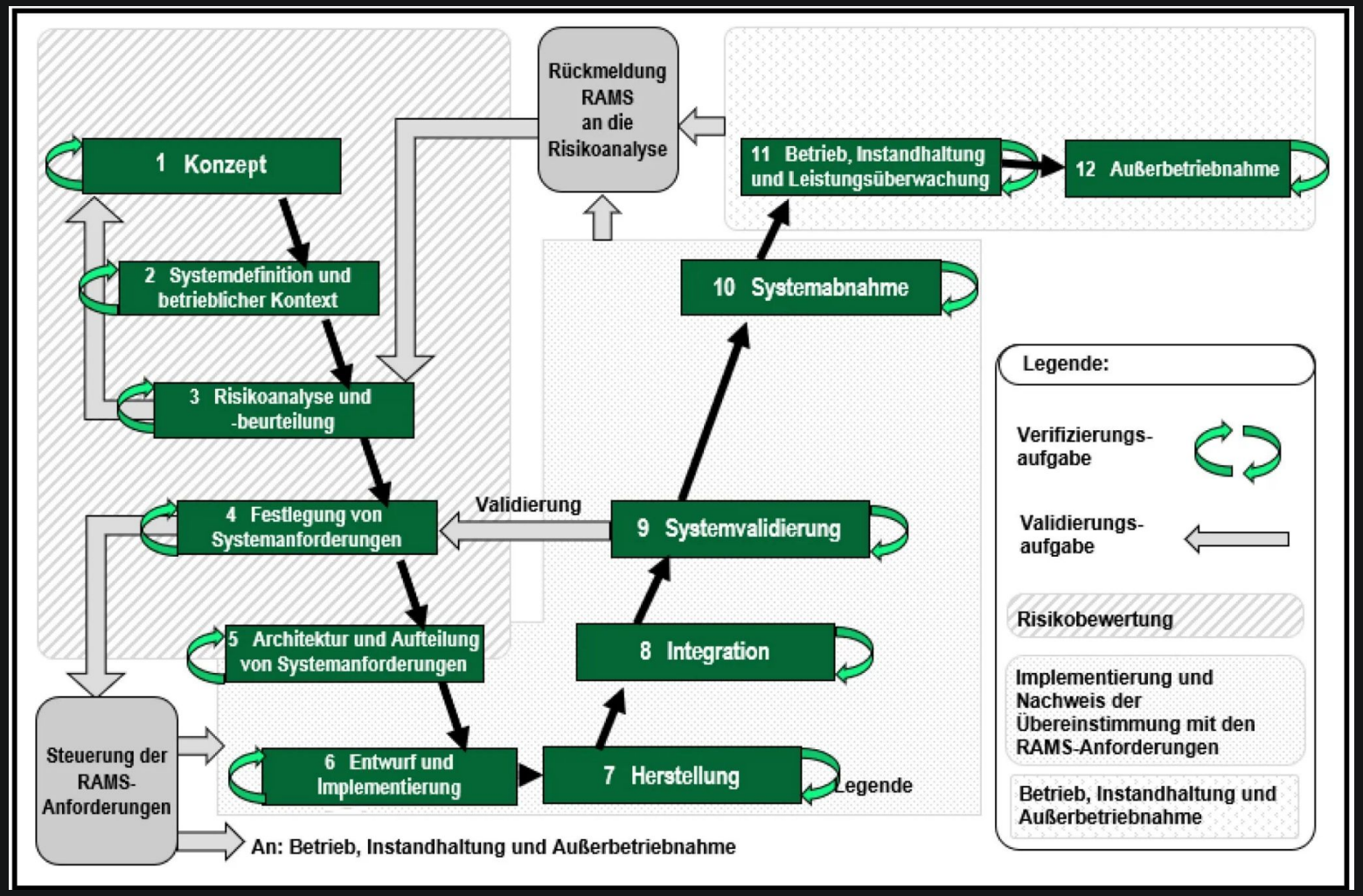
Konzept nach DIN EN 50126



Quelle: IZP Dresden mbH

Normativ geforderte Inhalte

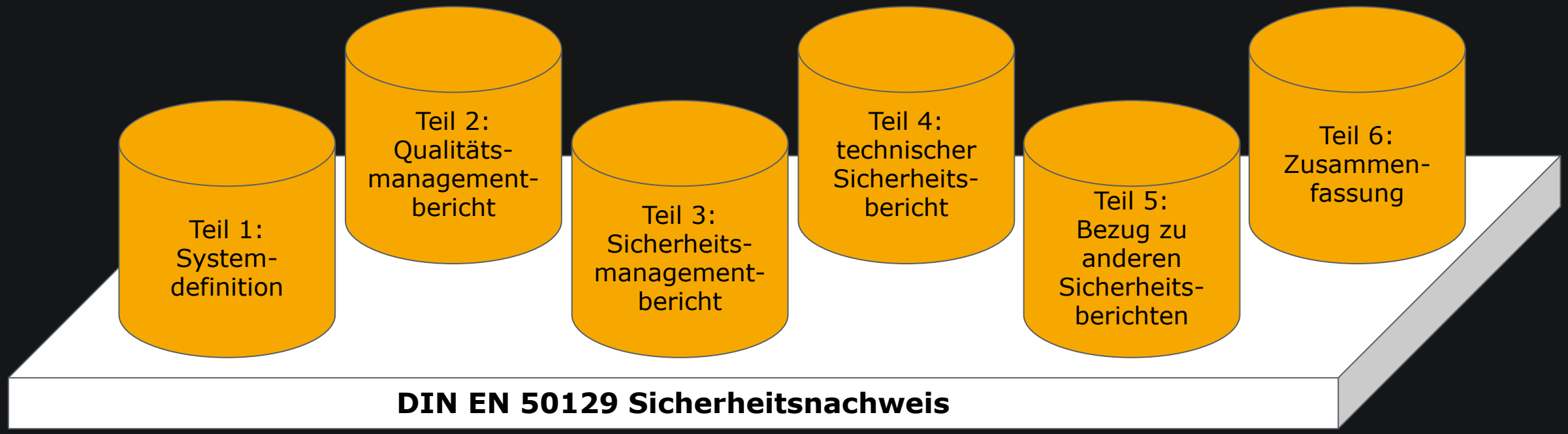
Konzept nach DIN EN 50126



Quelle: IZP Dresden mbH

Normativ geforderte Inhalte

Inhalte des Sicherheitsberichts



Normativ geforderte Inhalte
Systemdefinition

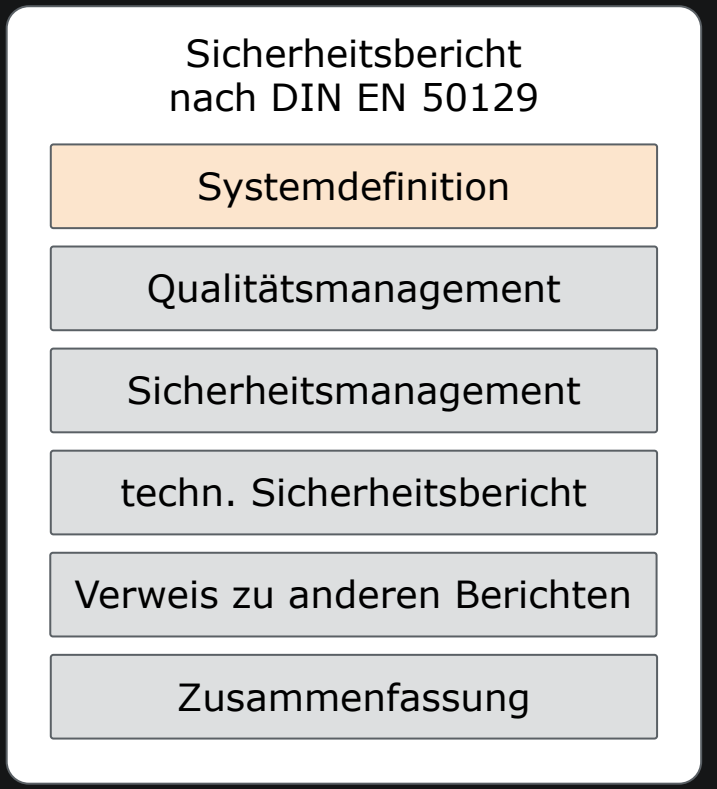
Identifikation und Konfiguration

Kontext und Grenzen

Funktionale Beschreibung und Sicherheitsfunktionen

Systemstruktur und Schnittstellen

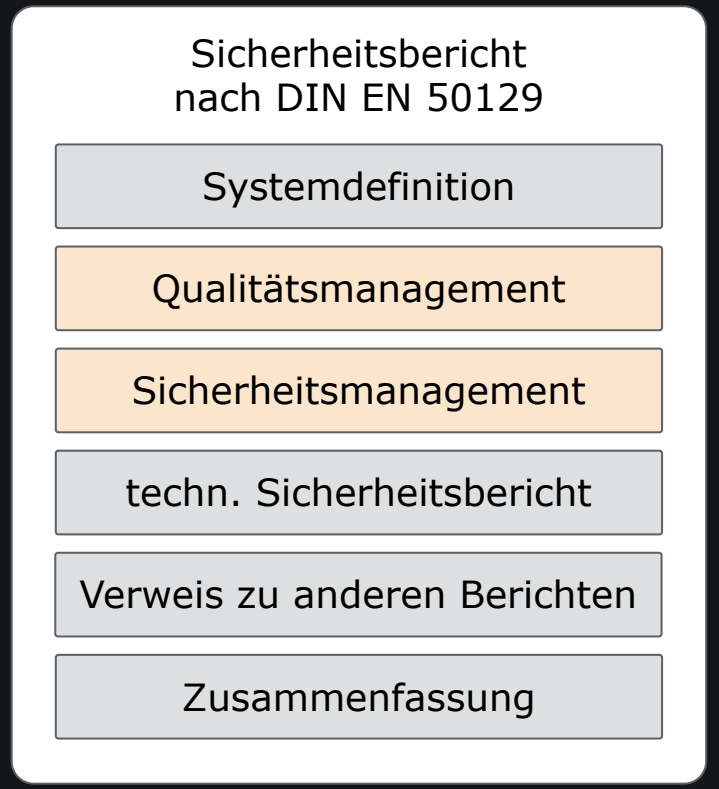
Betriebs- Wartungs- und Umgebungsbedingungen



Normativ geforderte Inhalte
Managementberichte

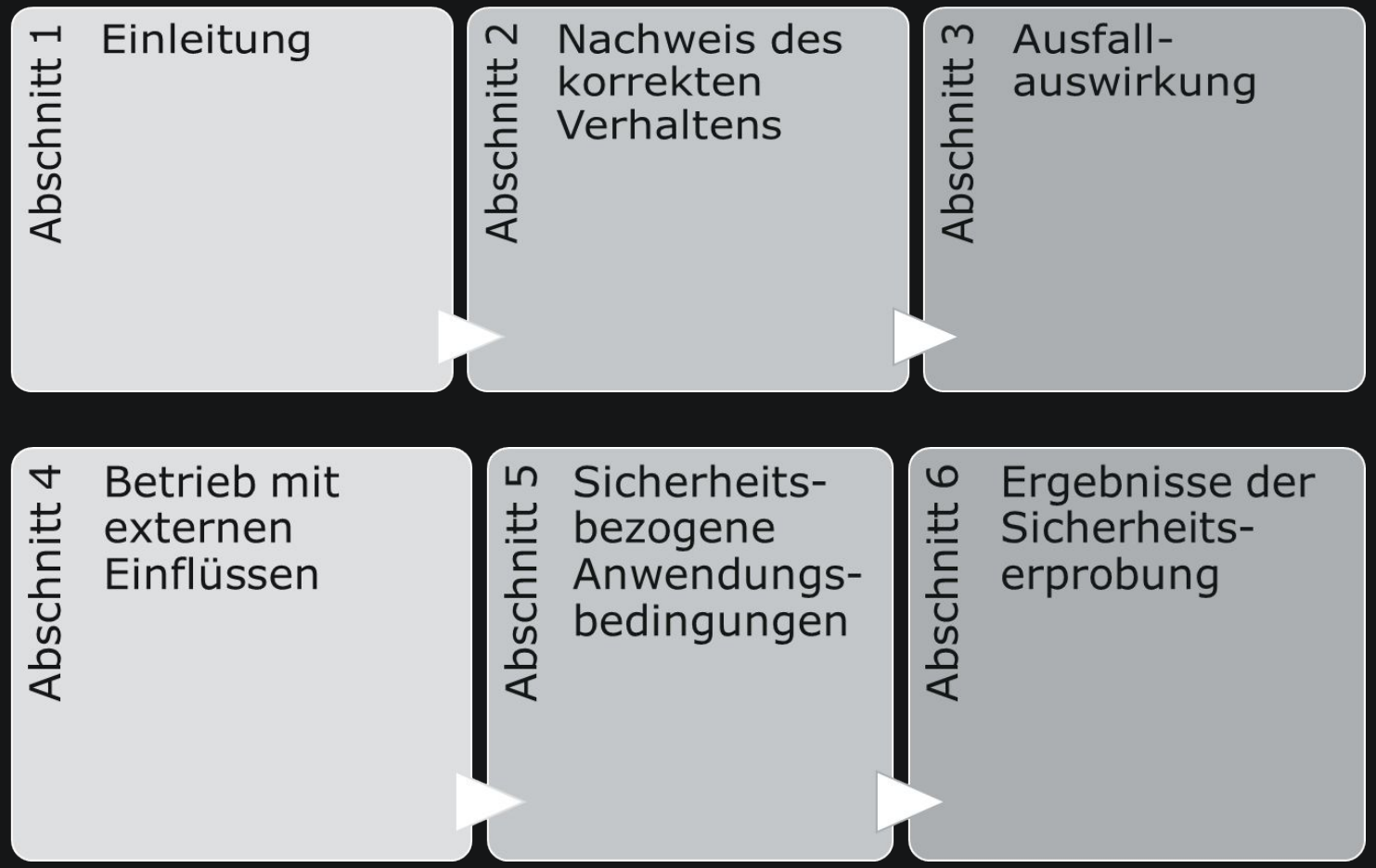
- Begleitung des gesamten Softwarelebenszyklus durch Qualitätsmanagement (gemäß ISO 9001)
- Ziel: Betrachtung, Überwachung und Reduktion von Fehlern
- Verbesserung der Wirksamkeit einzelner Prozesse

- Nachweis über gelebte Informationssicherheit im Projekt- und Entwicklungskontext (gemäß ISO 27001)
- Ziel: Implementierung eines Umfelds, in dem Sicherheit Teil der Kultur ist



Normativ geforderte Inhalte

Technischer Sicherheitsbericht



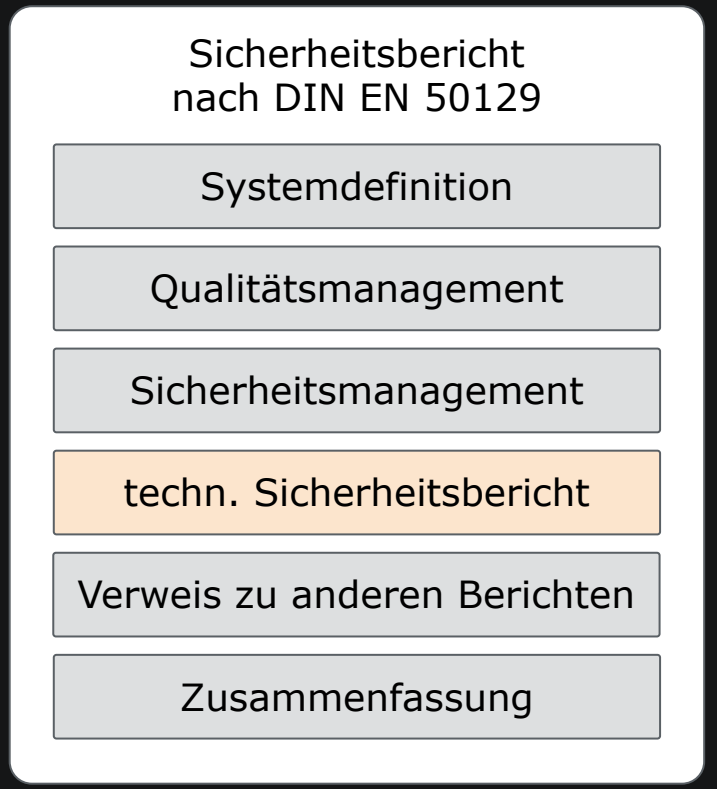
Sicherheitsbericht
nach DIN EN 50129

- Systemdefinition
- Qualitätsmanagement
- Sicherheitsmanagement
- techn. Sicherheitsbericht
- Verweis zu anderen Berichten
- Zusammenfassung

Normativ geforderte Inhalte

Technischer Sicherheitsbericht

- **Einleitung**: Systemüberblick und relevante Normen
- **korrektes funkt. Verhalten**: Nachweis der Sicherheit im normalen Betrieb, Schnittstellen, Hardware und Software
- **Ausfallauswirkung**: Einzelausfälle, Fehlererkennung, Fehlerbehandlung, Mehrfachausfälle
- **Externe Einflüsse**: externe Fehlerquellen, Umwelt, andere Systeme, Kommunikation
- **SRAC**: Randbedingungen, organisatorische Maßnahmen, Konfigurationen, Wartung
- **Ergebnisse**: Begründung über Sicherheit im Normalbetrieb, Restrisiken, Randbedingungen und Grenzen

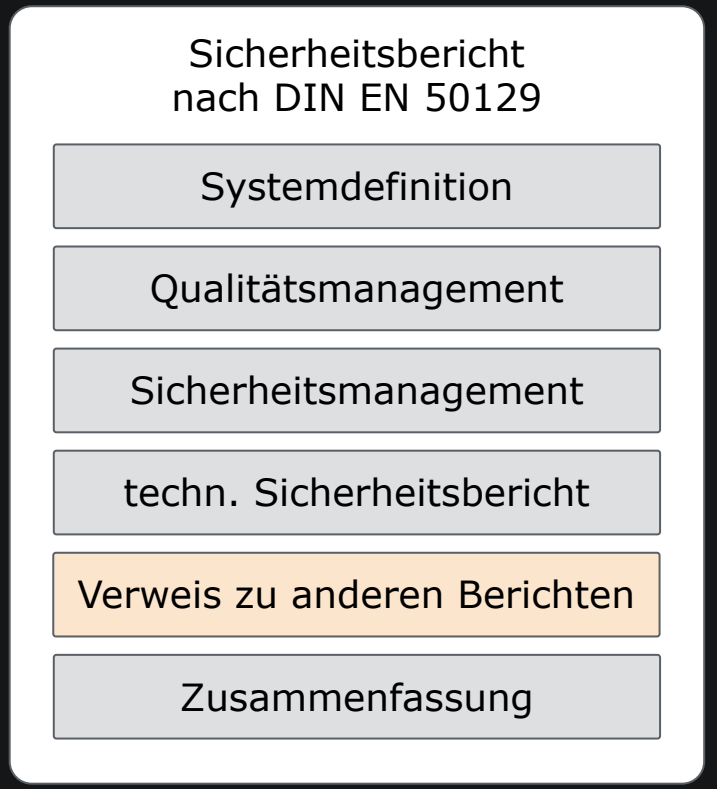


Normativ geforderte Inhalte
Beziehung zu anderen Sicherheitsberichten

Identifikation relevanter Fremdsysteme

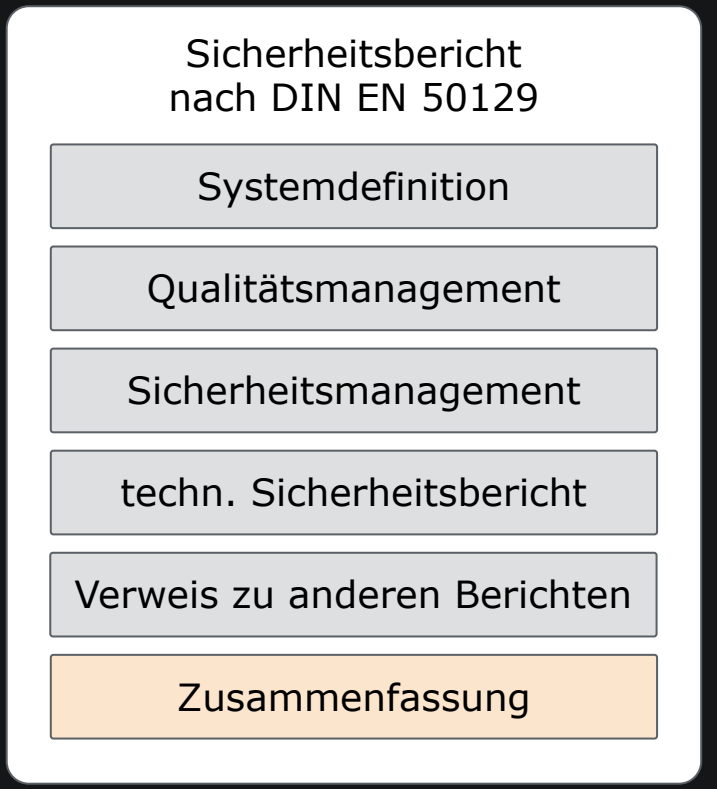
Beziehung und Abgrenzung zwischen den Systemen

SRAC des Fremdsystems



Normativ geforderte Inhalte
Schlussfolgerung

- Bewertung über tatsächliche Sicherheit des Systems
- **Ergebnisse** der vorherigen Kapitel
- **Vollständigkeit** der erbrachten Nachweise
- **Randbedingungen und Grenzen** in denen das System als sicher eingestuft werden kann
- **Folgeaktivitäten** und offene Punkte, die im weiteren Verlauf angegangen werden sollen



Fazit und Ausblick

Modellierbare Inhalte

Systemdefinition:

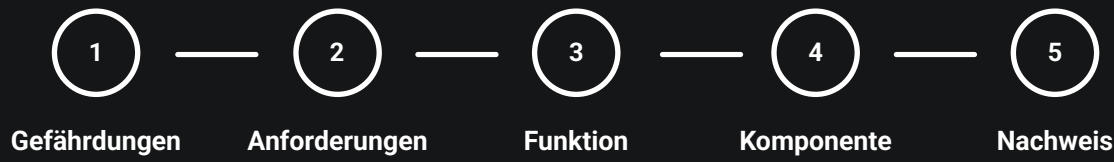
- Zustandsmaschine und Zustandsübergänge
- Komponentenübersicht und Schnittstellen
- Konfigurationen

technischer Sicherheitsbericht:

- Nachweis des korrekten Systembetriebs
- Ausfallverhalten
- sicherheitsrelevante Anforderungen und Schnittstellen

Metadaten:

- aus Gitlab heraus können Rollen abgeleitet werden: AutorIn, FreigeberIn, PrüferInnen
- Dazu Versionsnummern und Änderungshistorien



Sicherheitsbericht
nach DIN EN 50129

- Systemdefinition
- Qualitätsmanagement
- Sicherheitsmanagement
- techn. Sicherheitsbericht
- Verweis zu anderen Berichten
- Zusammenfassung

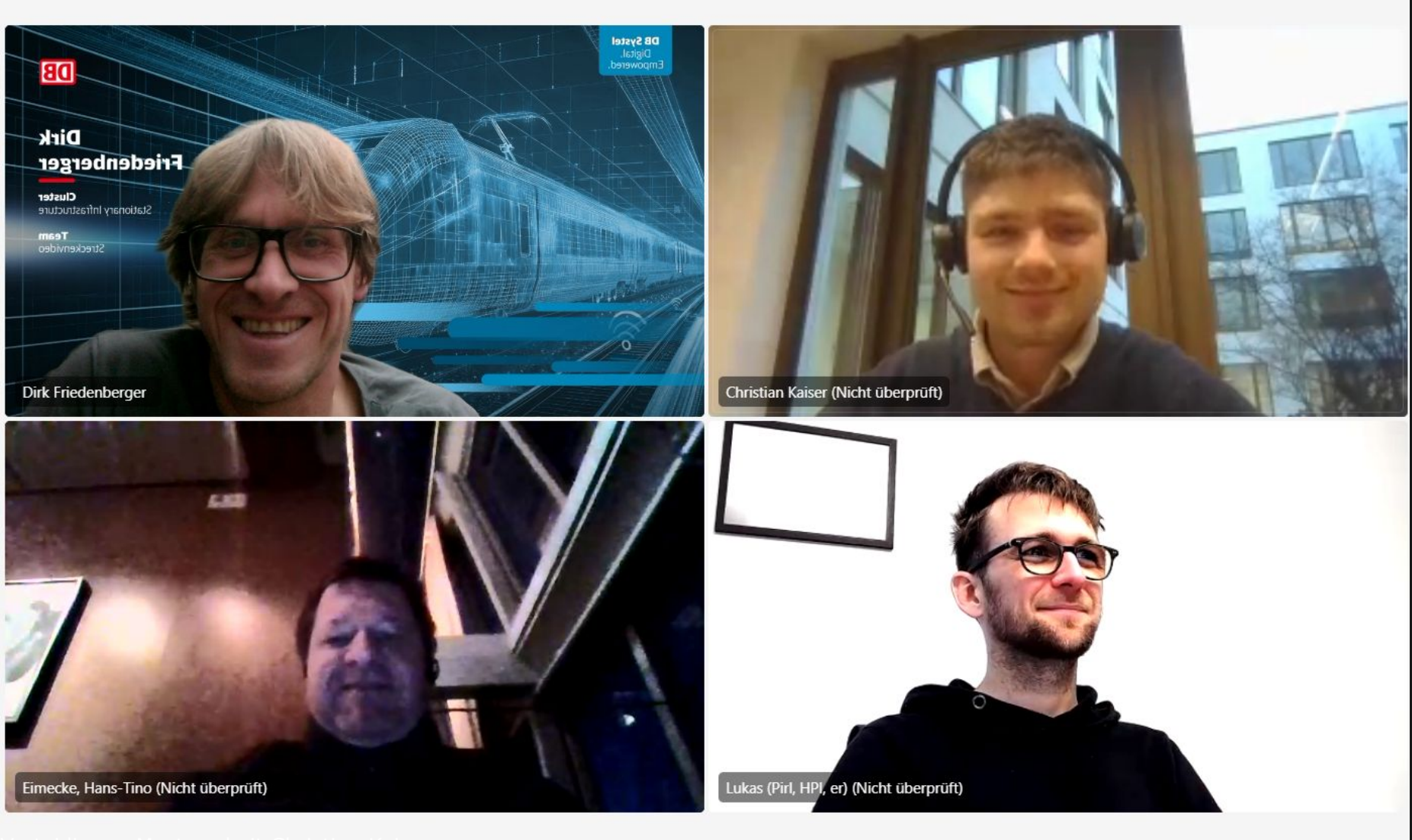
Fazit und Ausblick

Leitlinien für zukünftige Projekte

- Der Sicherheitsbericht ist kein nachgelagertes Dokumentationsprojekt
- Anforderungsanalyse muss modellhaft gepflegt werden
- Strukturierte Versionierung und Rollenmanagement

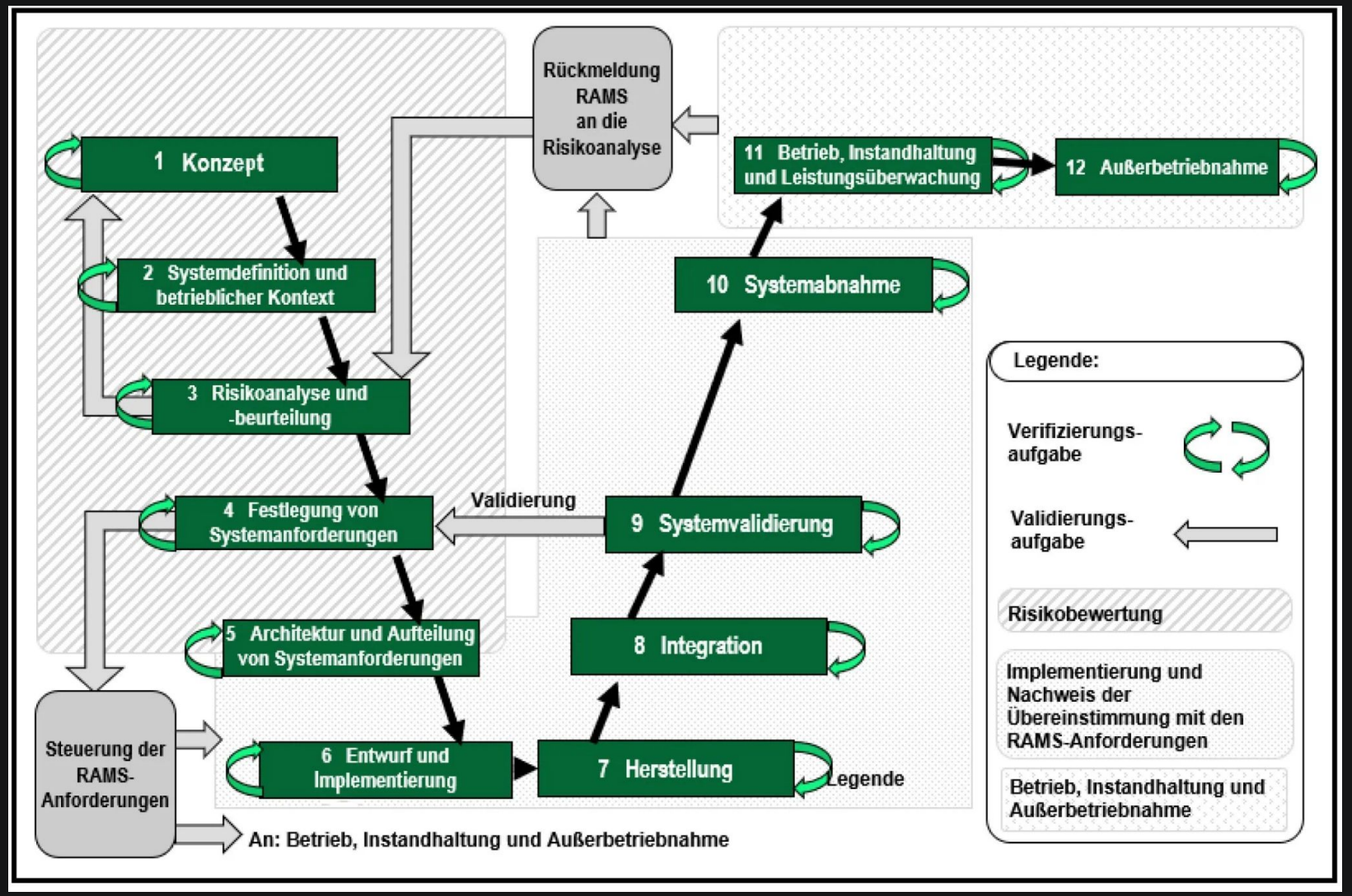
Fazit und Ausblick

Evaluation des Ansatzes



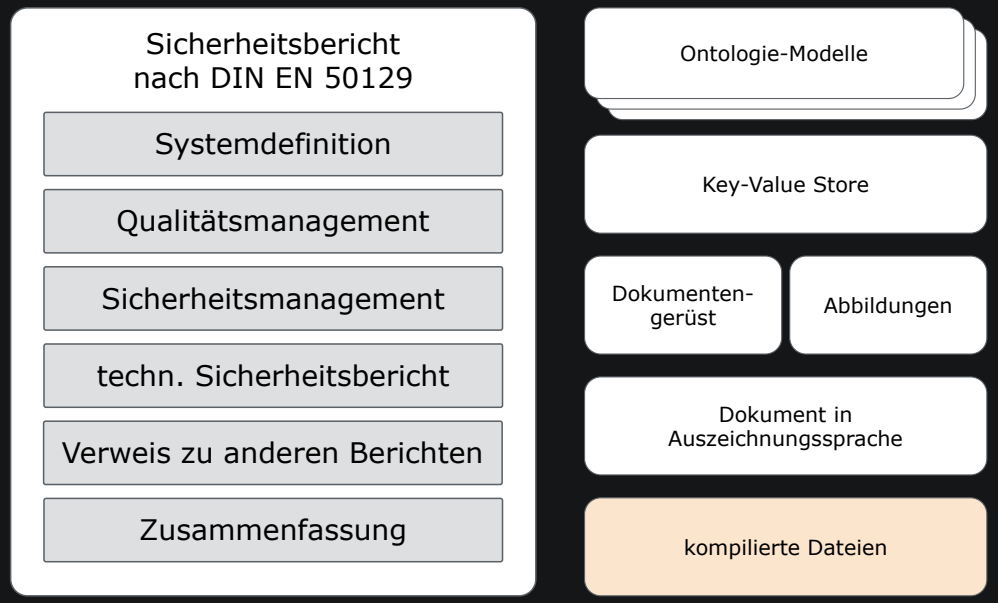
Fazit und Ausblick

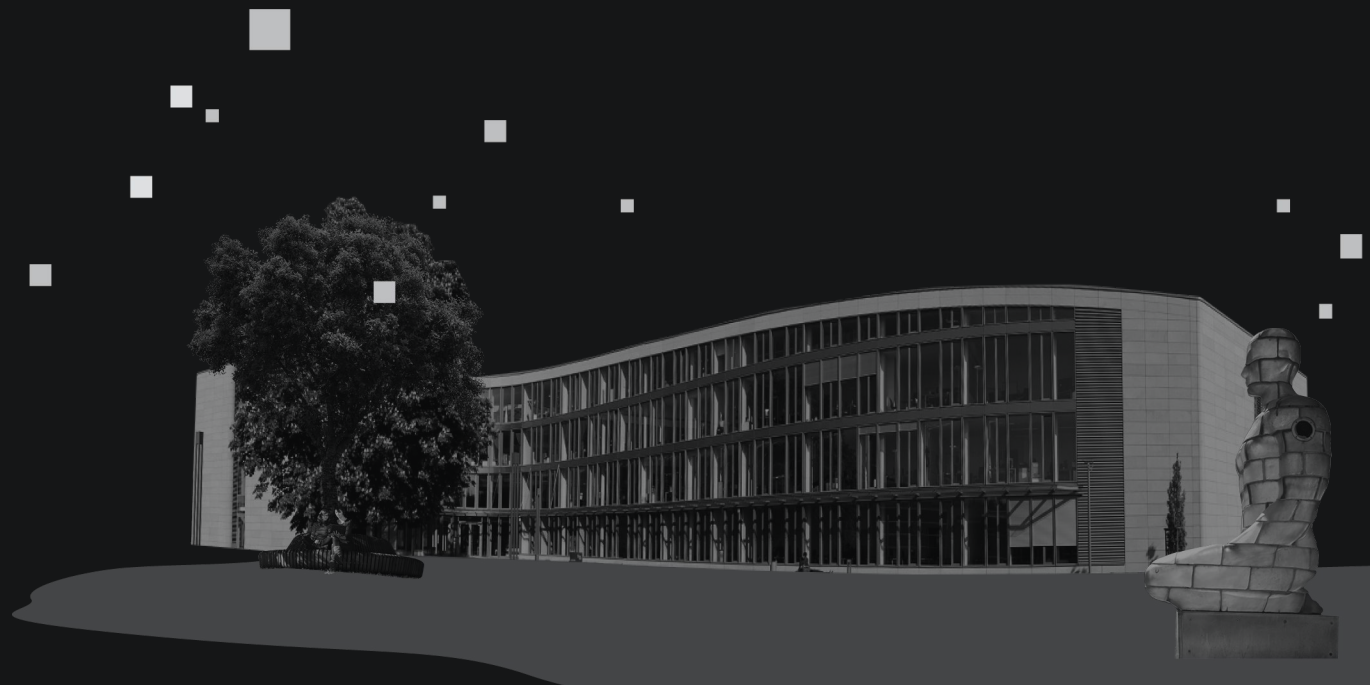
Evaluation des Ansatzes



Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Unterstützung des Zulassungsverfahrens von Bahnsystemen durch ontologiebasierte Systemmodelle





Sicherheitsbericht
nach DIN EN 50129

- Systemdefinition
- Qualitätsmanagement
- Sicherheitsmanagement
- techn. Sicherheitsbericht
- Verweis zu anderen Berichten
- Zusammenfassung

Ontologie-Modelle

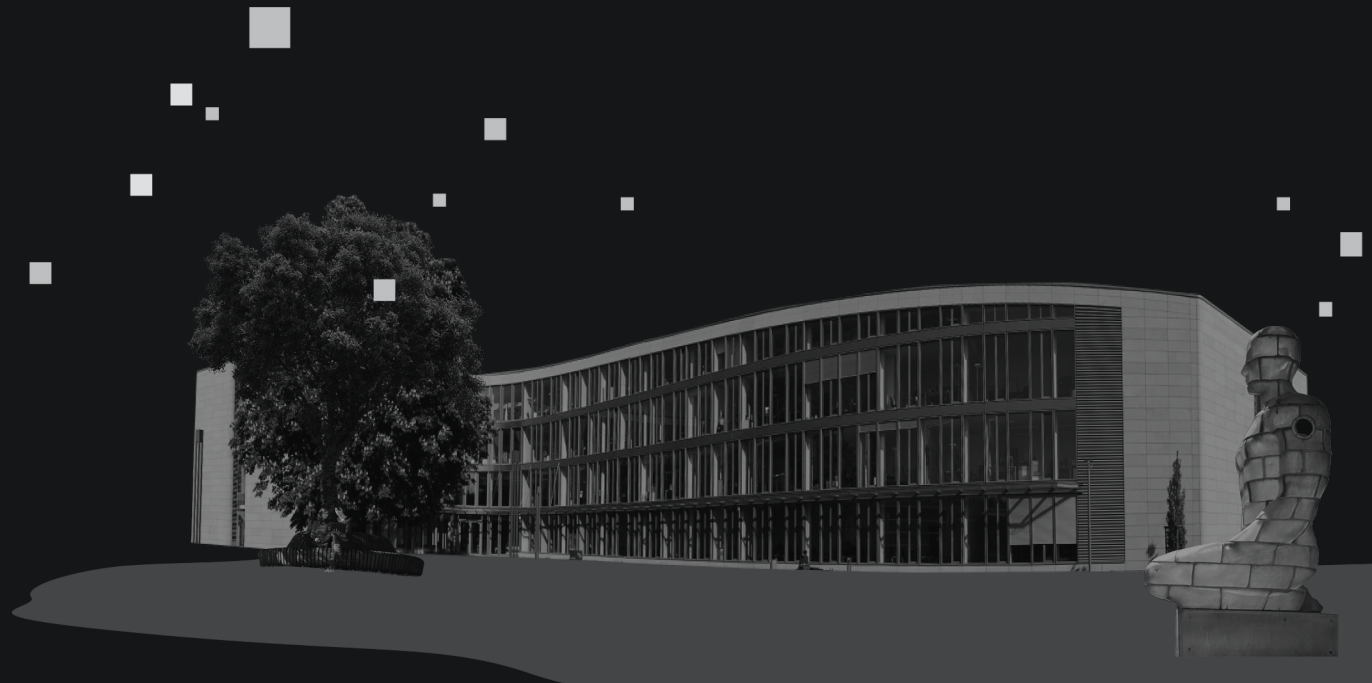
Key-Value Store

Dokumenten-gerüst

Abbildungen

Dokument in Auszeichnungssprache

kompilierte Dateien



Design IT.
Create Knowledge.

www.hpi.de

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam