

# Modell-basierter Barentango mit dem System Architecture Framework

Alexander Haarer<sup>1</sup>, Markus Andres<sup>2</sup>,

M. Leute<sup>3</sup>, S. Ackva<sup>4</sup>, C. Lalitsch-Schneider<sup>5</sup>,

S. Husung<sup>6</sup>, P. Malecki<sup>7</sup>

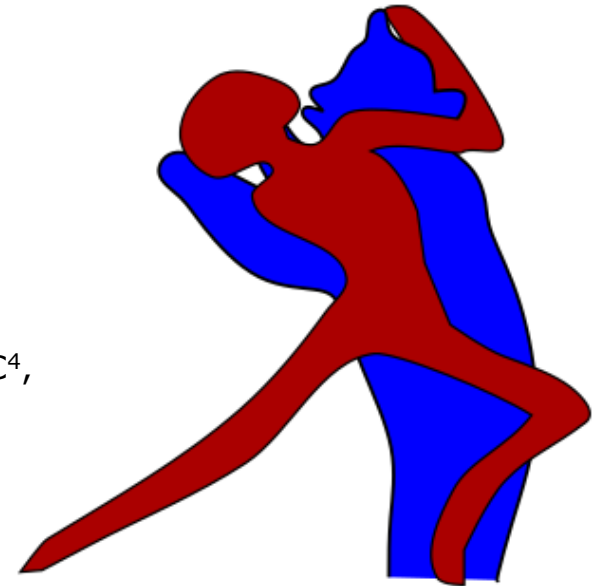
GfSE Arbeitsgruppe SAF

Atlas Elektronik<sup>1</sup>, HENSOLDT Sensors GmbH<sup>2</sup>, AIRBUS<sup>3</sup>, Continental A.D.C<sup>4</sup>,

ZF Friedrichshafen AG<sup>5</sup>, Technische Universität Ilmenau<sup>6</sup>,

thyssenkrupp Marine Systems<sup>7</sup>

**TdSE 2021**



- Das übergeordnete Ziel in der Frühphase eines Projekts ist «das Richtige» zu bauen, nicht nur «es richtig zu bauen».
- Hier spielt der «Bärentango» eine maßgebliche Rolle.
- Der Bärentango steht stellvertretend für das ausgewogene Zusammenspiel zwischen
  - Auftraggeber, der ein Lastenheft vorlegt, und
  - Auftragnehmer, der daraus ein belastbares Pflichtenheft generieren will.
- Wir wollen an einem Beispiel (Forest Fire Detection System) konkret aufzeigen, wie man den «Bärentango» mit Hilfe des SAF erfolgreich choreografieren kann.



[Bärentango] Tom DeMarco, Timothy Lister, Bärentango Mit Risikomanagement Projekte zum Erfolg führen, erschienen im Carl Hanser Verlag

## → SAF

- Architecture Framework für modellbasierte Entwicklung technischer Systeme
- Von Mitgliedern der **SAF Arbeitsgruppe** der **GfSE** getragen und entwickelt
- Standards: **SysML, ISO42010, ISO15288**

## → SAF Ziele

- **Standardisierung** von Modellelementen und Viewpoints
- **Unterstützung** bei der Erstellung, Analyse und Kommunikation der für Systems Engineering relevanten Inhalte
- **Beschränkung des Modellierungsaufwandes** auf das Notwendige
- **Modellierung planbar und skalierbar** machen
- **Automatisierung** und **Datenaustausch**

→ SAF ist eine **Toolbox**:

- SAF stellt Viewpoints für den Bedarf des SE bereit.
- SAF deckt die technischen SE Prozesse der ISO15288 ab.
- SAF ist neutral gegenüber **Prozessen** oder **Methoden**.

→ SAF ist **offen**:

- SAF wird weiterentwickelt, neue Domänen, Aspekte und Viewpoints.
- Eigene Viewpoints können erstellt werden.

→ SAF ist **Toolübergreifend**

- Implementiert für verschiedene SysML Tools

→ SAF ist eine **Fortsetzung** von Enterprise Frameworks:

- kompatibel zu Enterprise Frameworks UAF, NAF, MoDAF, ADMBw.
- SAF beginnt, wo Enterprise Frameworks aufhören.

## → Der Kunde (AG) hat Bedarf an einem System zur Lösung seines Problems:

- Es gibt ein Lastenheft mit Anforderungen.
- Eine Beschreibung des beabsichtigten Nutzens (z.B. ConOps) liegt nur unvollständig vor.
- Technische Lösung ist grob umrissen.
- System soll beschafft werden.



## → Der Auftragnehmer (AN) will ein System entsprechend des Lastenhefts anbieten:

- Lastenheft enthält wahrscheinlich nicht alle Nachbarelemente des zukünftigen System.
- Die Hintergründe für Anforderungen im Lastenheft sind unklar.
- Es ist erforderlich, den Kontext des Systems besser zu verstehen.
- Das angebotene System soll mit einem Pflichtenheft definiert werden.



## → Problemfelder und Risiken identifizieren

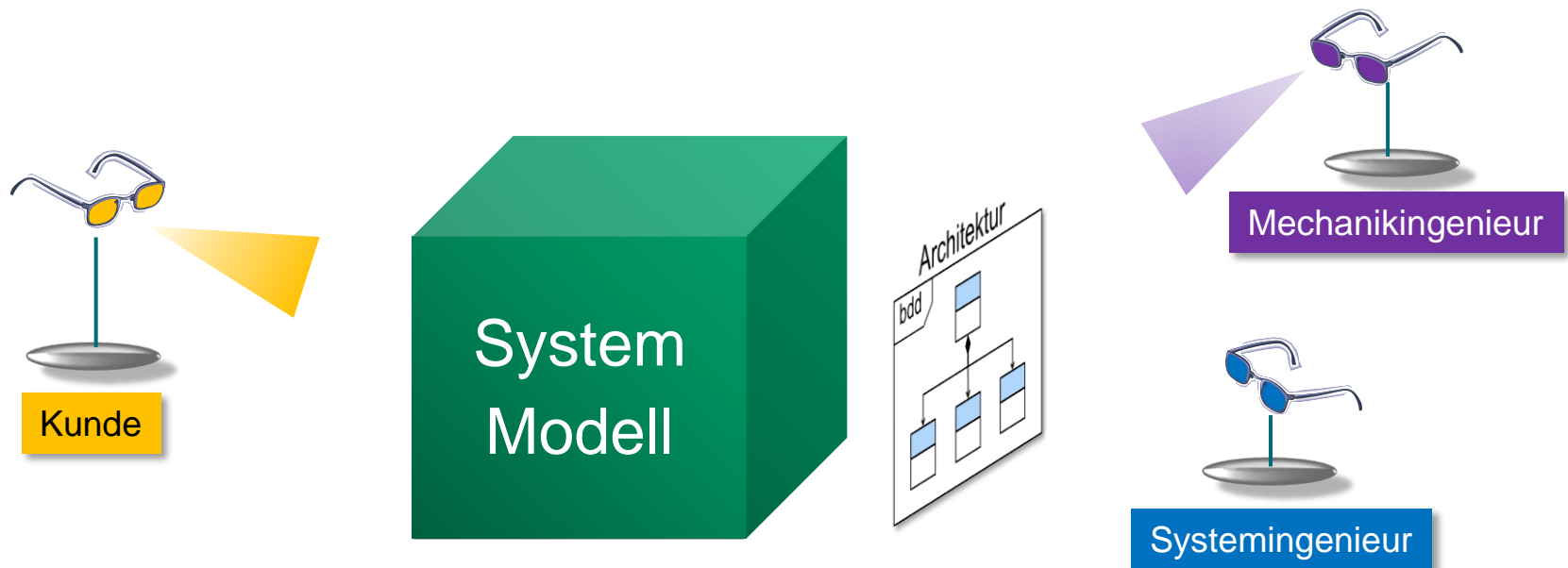
- Kontext der Nutzung nicht gut genug verstanden
  - Ggfs. unbekannte Nachbarelemente
- Operationeller Betrieb (Ausgangssituation und Zielbild) nicht gut genug verstanden

## → Viewpoints entsprechend auswählen

- Concerns der Viewpoints geben Hinweise
- Nur die nötigen Viewpoints auswählen
- Auswahl ggfs. nach fachbezogenem Risiko schneiden

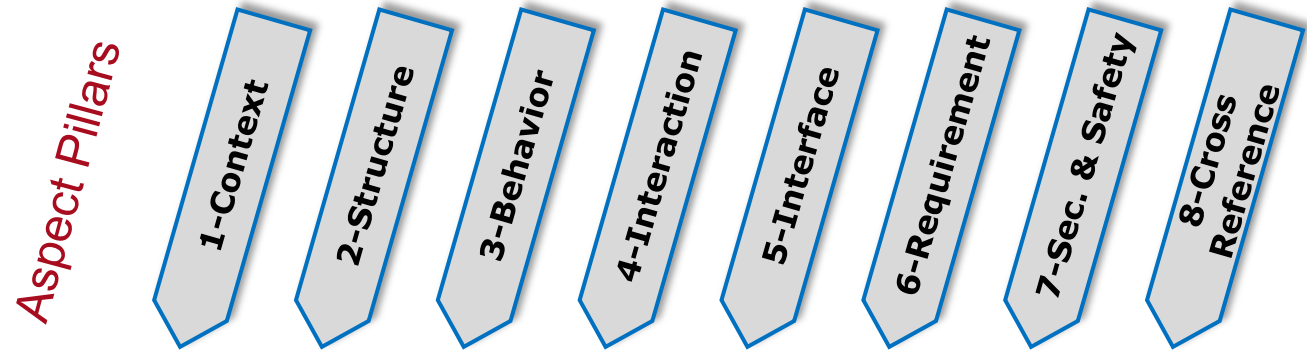
## → Workflow durch SAF Viewpoints definieren

# Was sind Viewpoints ?



- ➔ Modelle sind umfangreich
- ➔ Nicht jeder benötigt an Information alles
- ➔ Ein **Viewpoint** spezifiziert eine Zusammenstellung bestimmter Modellelemente für einen bestimmten Zweck.

# ... die Viewpoint Auswahl



## Domain Layers

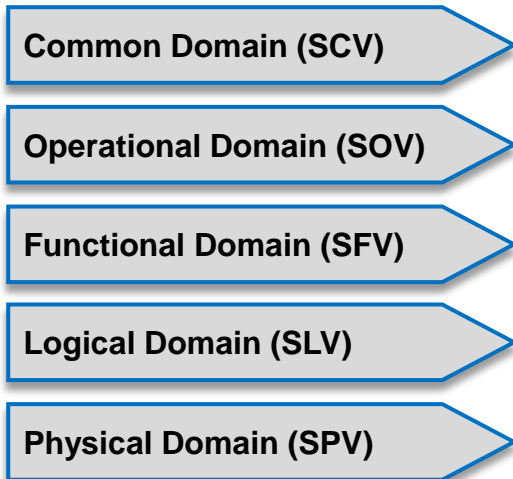
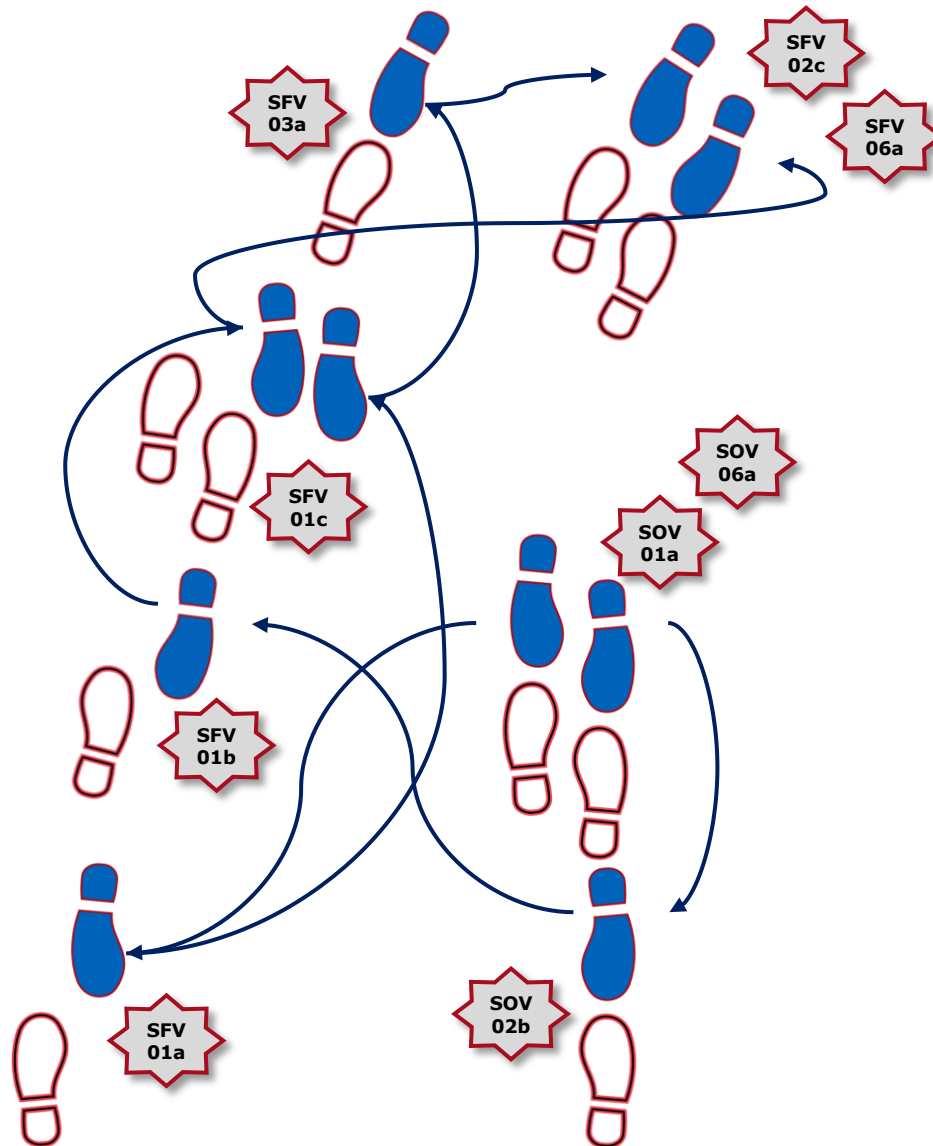
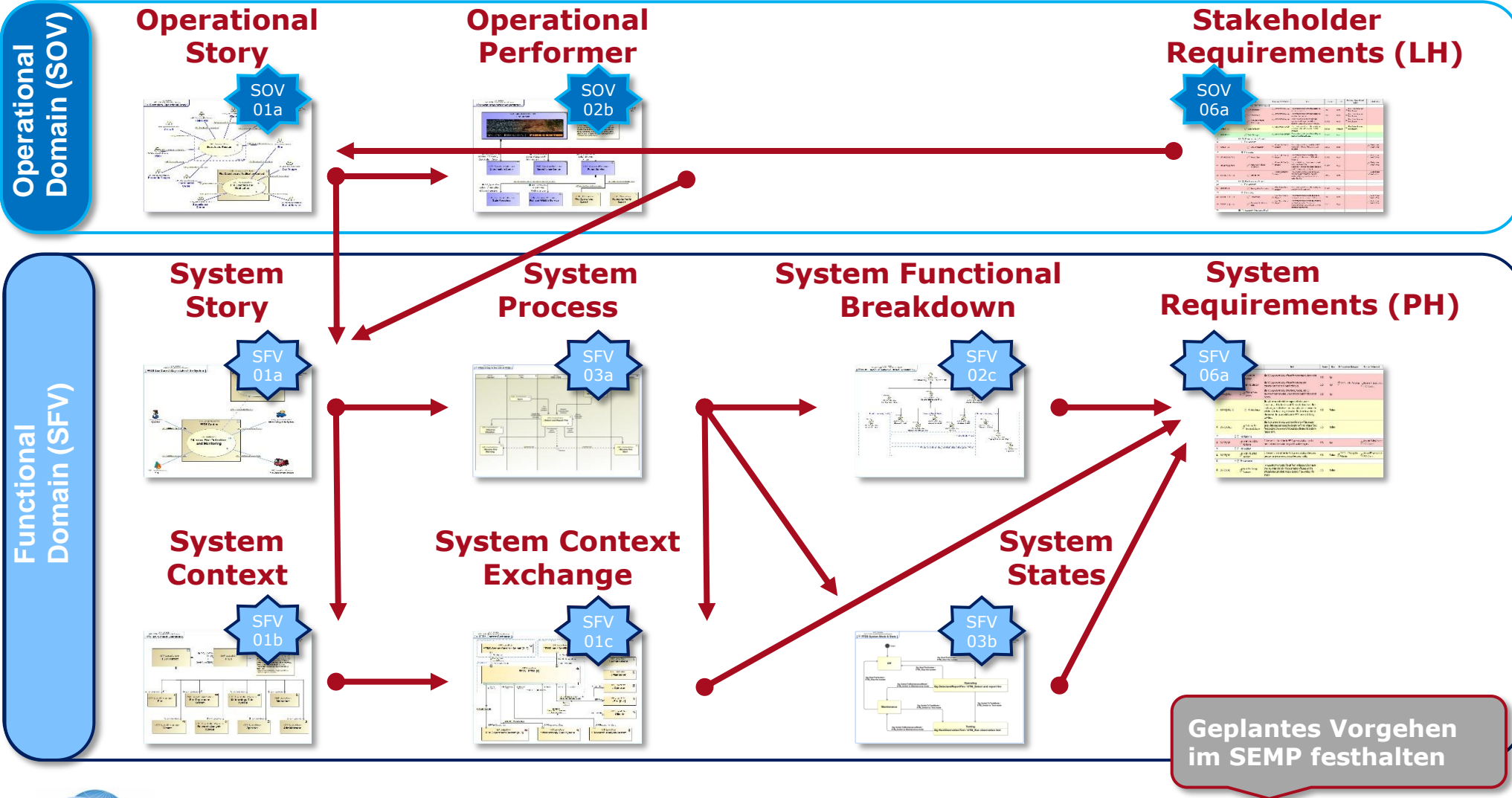


Diagram Description SAF Viewpoint grid	1-STORY CONTEXT & EXCHANGE	2-STRUCTURE	3-PROCESS & BEHAVIOR	4-INTERACTION & COLLABORATION	5-INTERFACE	6-REQUIREMENT	7-SAFETY & SECURITY	8-MAPPING & CROSS REFERENCE
COMMON DOMAIN SCV								
OPERATIONAL DOMAIN SOV	Operational Story Context & Exchange Operational Story Profile Operational Context Definition Profile Operational Context Exchange Profile	Operational Structure Operational Domain Item Kind Profile Operational Domain Performance Profile Operational Capability Profile Identification Profile	Operational Process Operational Process Profile	Operational Interaction Operational Interaction Profile		Stakeholder Requirement Stakeholder Requirement Profile		Mapping Operational Capability Traceability Profile Operational Process Traceability Profile
FUNCTIONAL DOMAIN SFV	Functional Story Context & Exchange System Story Profile System Context Definition Profile System Context Exchange Profile	Functional Structure System Domain Item Kind Profile System Functional Capability Profile System Functional Breakdown Profile	Functional Process System Process Profile System State Profile	Functional Interaction System Context Interaction Profile		System Requirement System Requirement Profile	Functional Hazard	Mapping System Requirement Traceability Profile System Function Block Risk Allocation Profile
LOGICAL DOMAIN SLV	Logical Context & Exchange	Logical Structure Logical Structure Profile	Logical Behavior	Logical Interaction Logical Interaction Profile Logical Internal Exchange Profile				Mapping
PHYSICAL DOMAIN SPV	Physical Context & Exchange Physical Context Definition Profile Physical Context Exchange Profile	Physical Structure Physical Structure Profile	Physical Behavior					



# ... die Schrittfolge





# Schritt 0: Ausgangsposition: Lastenheft erfassen

## SOV06a Stakeholder Requirements



- ➔ Wir (AN) haben ein Lastenheft bekommen
- ➔ ... ins Modell aufnehmen
- ➔ Anforderungen weiterer Stakeholder miterfassen

SOV 06a elements				
ID	Name	Specification	Source	Risk
CPBLTY-11	FireDetection	The system shall have the ability to detect fire areas.	StkRS	High
CPBLTY-12	FireMonitoring	The system shall have the ability to monitor fire areas.	StkRS	High
CPBLTY-12.1	AreaOfInterestMonitoring	In the event of a forest fire the system shall have the ability to monitor a specific area of interest.	StkRS	High
CPBLTY-14	DataCollection	The system shall have the ability to provide collected data for further analysis.	StkRS	Medium
CPBLTY-15	DataStorage	The system shall have the ability to store the collected data.	StkRS	Low
CPBLTY-16	Availability_24_7	The system shall be available 24/7. Rational: A forest fire could occur anytime.	StkRS	High
CPBLTY-17	PropagationEstimation	The system shall have the ability to predict the fire spread.	StkRS	High
CPBLTY-18	ForestFireDetectingAndMonitoringCapability	The system shall have the ability to detect and monitor forest fires.	StkRS	High
CPBLTY-19	ForestFirePatternResearchCapability	The system shall have the ability to research forest fire pattern(s) in order to trace the origin and development of a fire.	StkRS	High
CPBLTY-20	BurntForestAreaDamageAssesmentCapability	The system shall have the ability to assess damage in burnt areas in order to base post-fire assessment and management decisions on this information. Rational: Plant mortality, regeneration and reproduction are closely tied to how hot and how long a wildfire burns and will determine the make-up of post-fire plant communities. Burn severity also effects wildlife habitat, changes in the soil, erosion potential and many components of aquatic environments.	StkRS	High
STK-REQ-QLT-...	ForestSize	The system shall be scalable for forest up to the size of 500 million hectare.	StkRS	High
STK-REQ-QLT-...	FalseAlarm_falseNegative)	The probability of false alarms must be lower than 5 %. Rational: A forest fire alarm triggers a lot of expensive actions.	StkRS	High
STK-REQ-QLT-...	SizeOfFire	The system shall be able to detect fire areas of at least 50 square meter initiating reactive actions to cope the fire.	StkRS	High
STK-REQ-QLT-...	Geolocation	The system shall be able to locate fires with an accuracy of 100 meter.	StkRS	High
STK-REQ-QLT-...	FireAlertNotificationTime	The system shall be able to report a verified fire within 5 seconds. Rational: Every second counts when fighting a forest fire.	StkRS	High

# Schritt 1: Nutzung verstehen

## SOV01a Operational Story

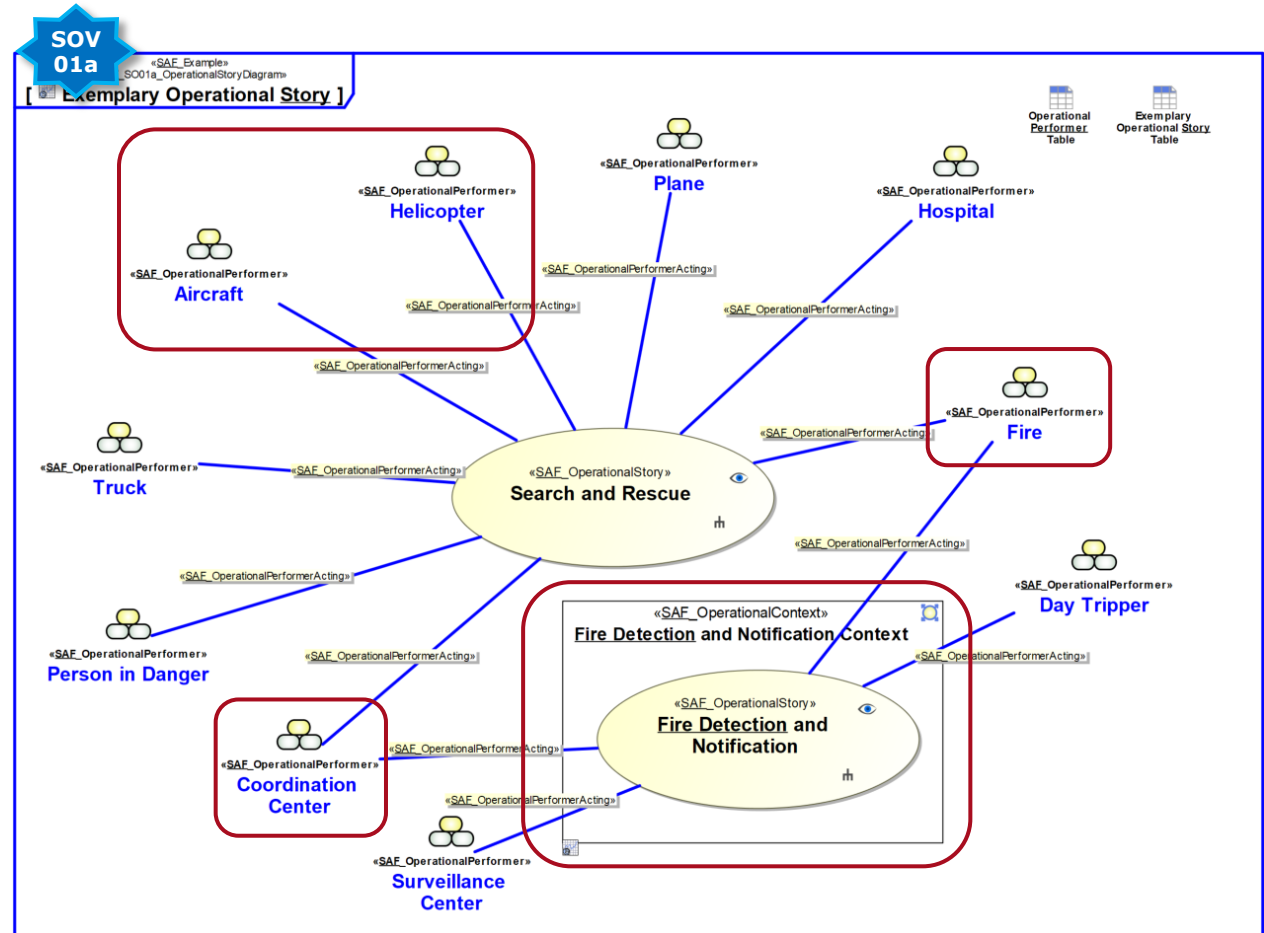
**SOV 06a**

Stakeholder	Requirement	Priority	Status	Version	Created By	Last Modified By
Stakeholder 1	Requirement 1.1	High	Open	1.0	John Doe	2023-11-10 10:00
Stakeholder 2	Requirement 2.1	Medium	Open	1.0	Jane Smith	2023-11-10 11:00
Stakeholder 3	Requirement 3.1	Low	Open	1.0	John Doe	2023-11-10 12:00
Stakeholder 4	Requirement 4.1	High	Open	1.0	Jane Smith	2023-11-10 13:00
Stakeholder 5	Requirement 5.1	Medium	Open	1.0	John Doe	2023-11-10 14:00
Stakeholder 6	Requirement 6.1	Low	Open	1.0	Jane Smith	2023-11-10 15:00
Stakeholder 7	Requirement 7.1	High	Open	1.0	John Doe	2023-11-10 16:00
Stakeholder 8	Requirement 8.1	Medium	Open	1.0	Jane Smith	2023-11-10 17:00
Stakeholder 9	Requirement 9.1	Low	Open	1.0	John Doe	2023-11-10 18:00
Stakeholder 10	Requirement 10.1	High	Open	1.0	Jane Smith	2023-11-10 19:00

Stakeholder Requirements

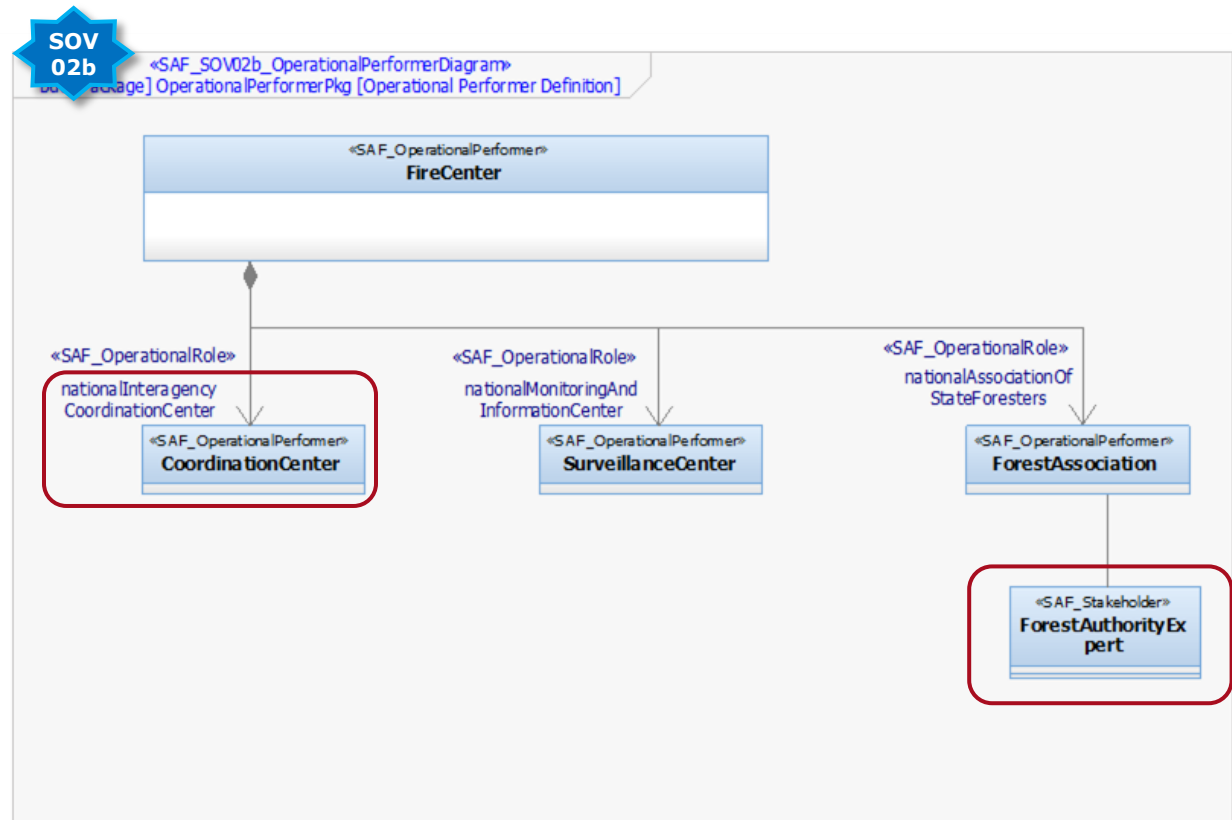
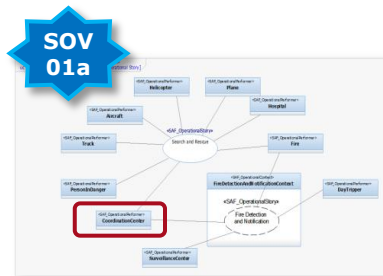


- "Operational Story" erzählen, Nutzer mitnehmen
- "Operational Performer" identifizieren
- Mit Auftraggeber "Operational Stories" validieren



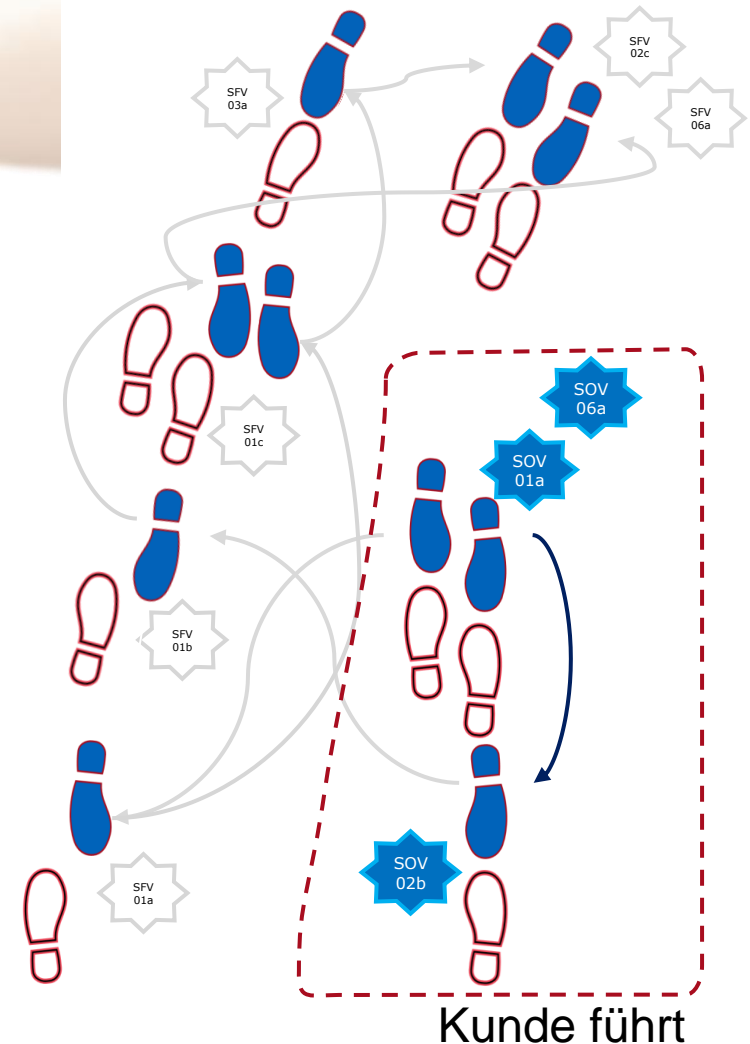
# Schritt 2: Umfeld verstehen

## SOV02b Operational Performer

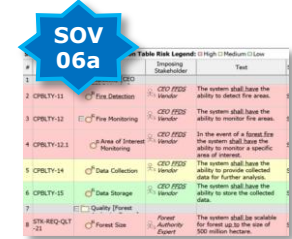
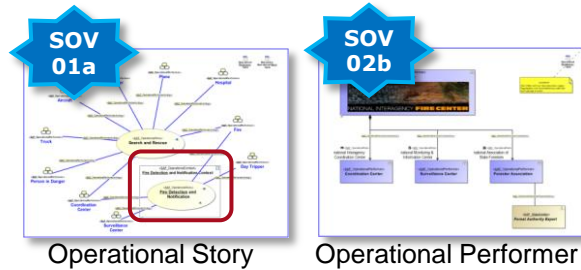


- ➔ Potenzielle Nachbarsysteme identifizieren
- ➔ Stakeholder identifizieren

- Kontext der Nutzung besser verstanden
  - Interaktionen mit Nachbarsystemen umfassender identifiziert
  - Weitere Stakeholder benannt
  - Operationeller Einsatz und Bedarf besser verstanden
  - Nachvollziehbarkeit hergestellt
- 
- **Mit Auftraggeber (AG) abgestimmt**
  - **Risiken verringert**

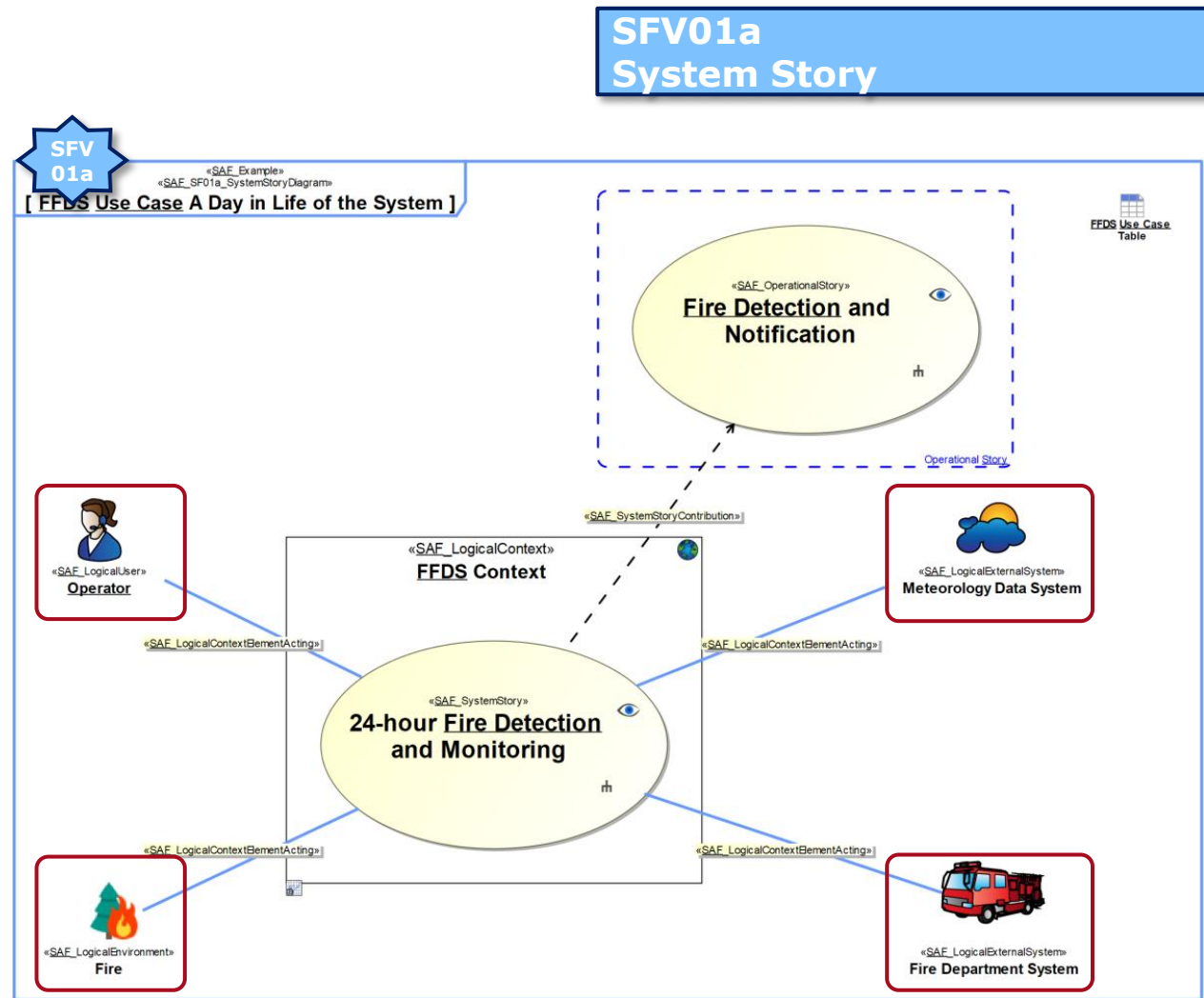






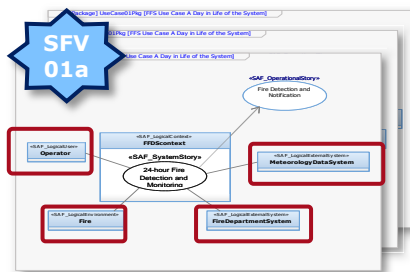
## Stakeholder Requirements

- ➔ System Stories aus Operational Domain ableiten
- ➔ Externe Entitäten identifizieren
- ➔ System Stories mit AG abstimmen
- ➔ **Geplante Verwendung**

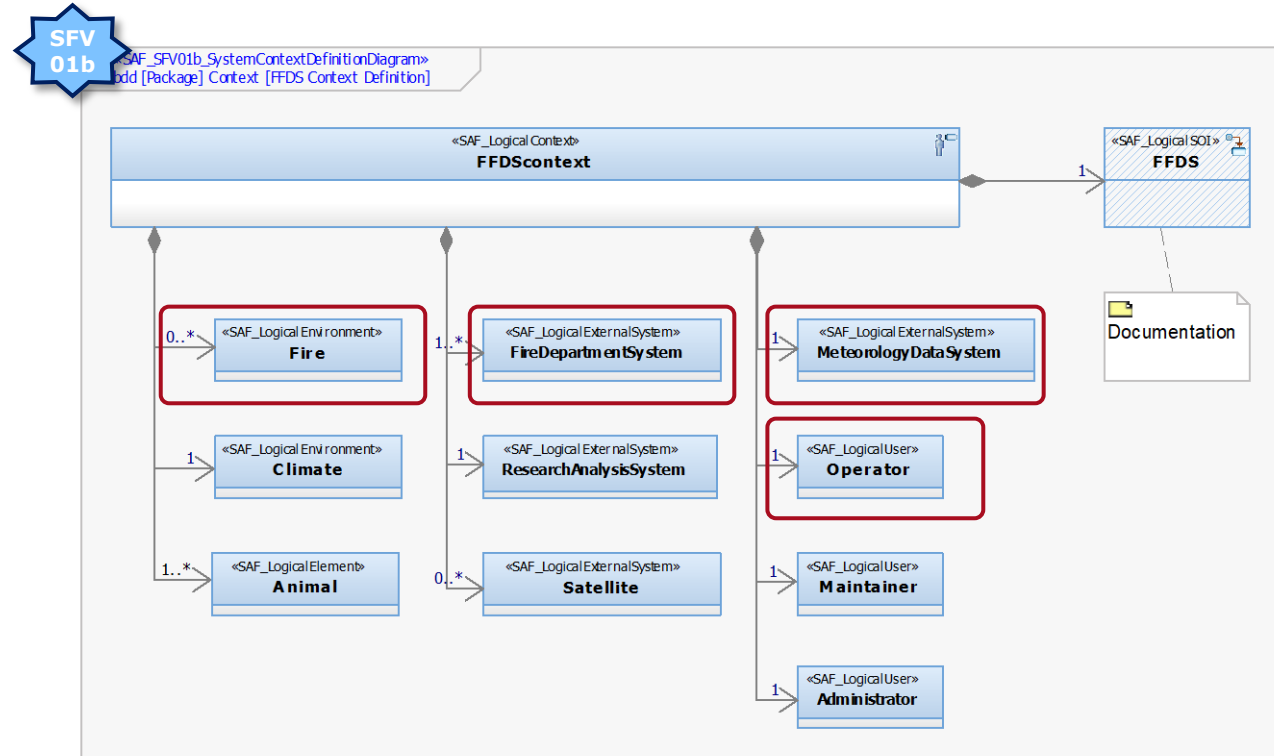


# Schritt 4: System Kontext definieren

## SFV01b System Context Definition



System Story

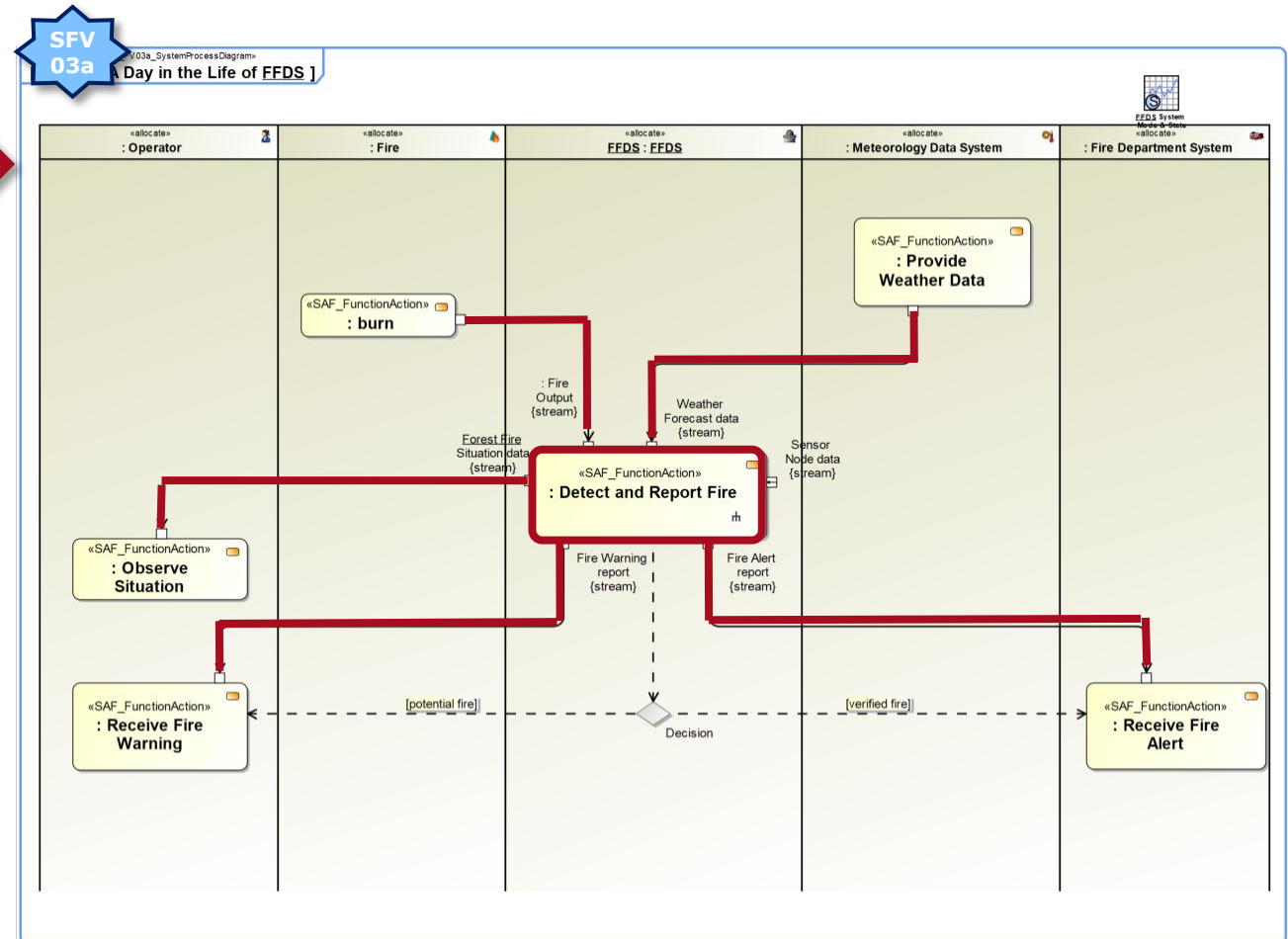
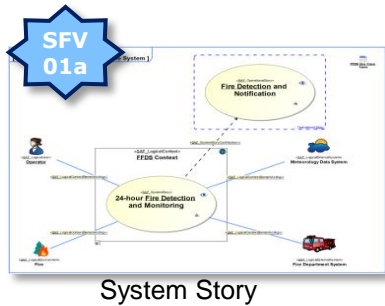


- Systemkontext aus "System Stories" ableiten
- Summe der Elemente aus n "System Stories"
- Für unterschiedliche Kontexte
- **Definition der Systemgrenze**



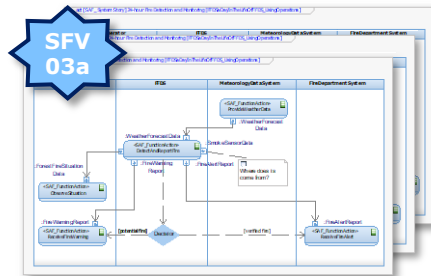
# Schritt 5: System Stories ausarbeiten

## SFV03a System Process

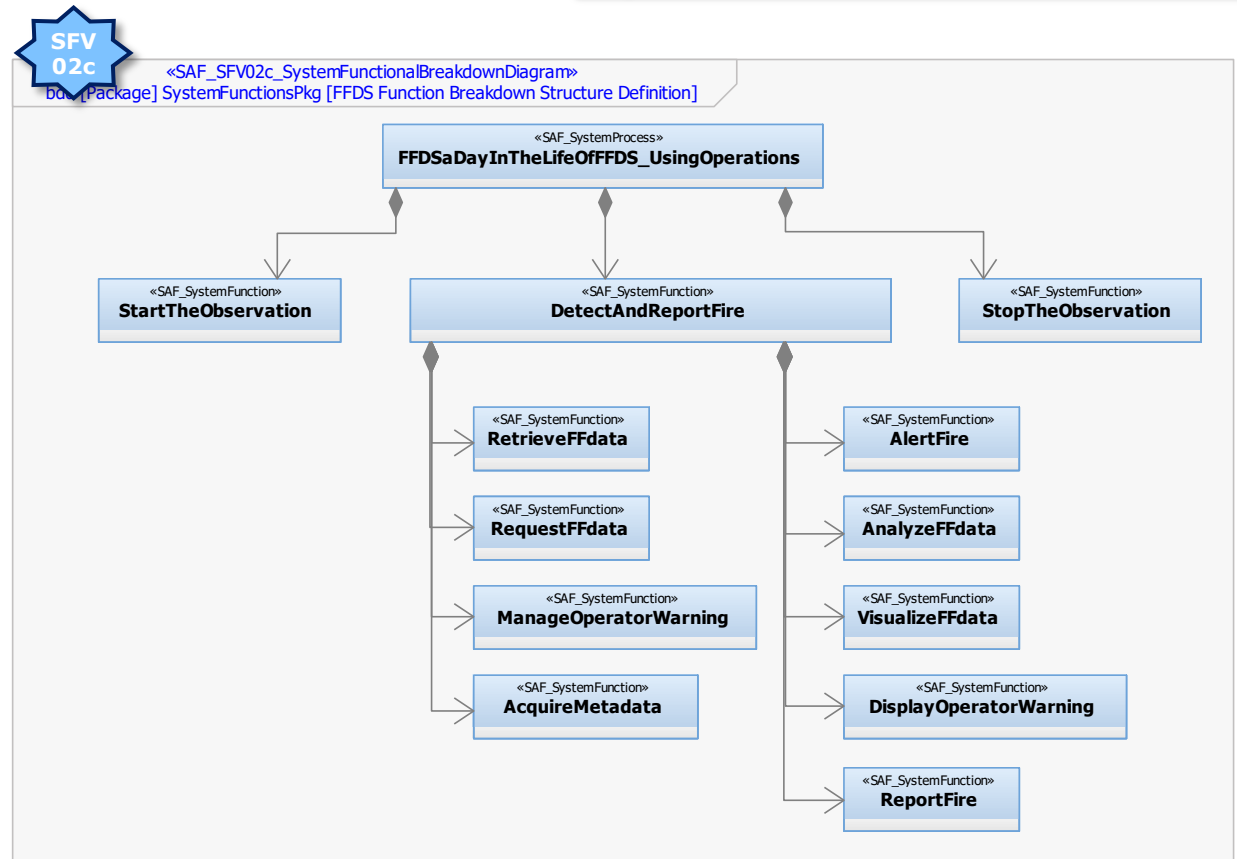


- System Stories mit System Prozessen verfeinern
- Systemfunktionen identifizieren
- **Funktionalen Austausch identifizieren**

# Schritt 6: Funktionale Struktur erstellen



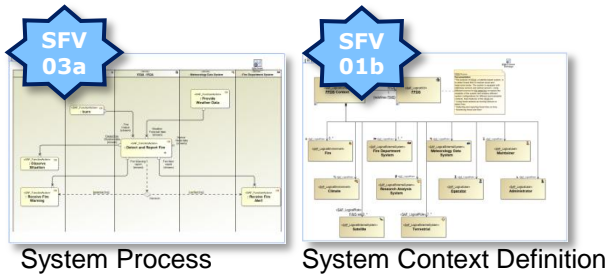
System Process



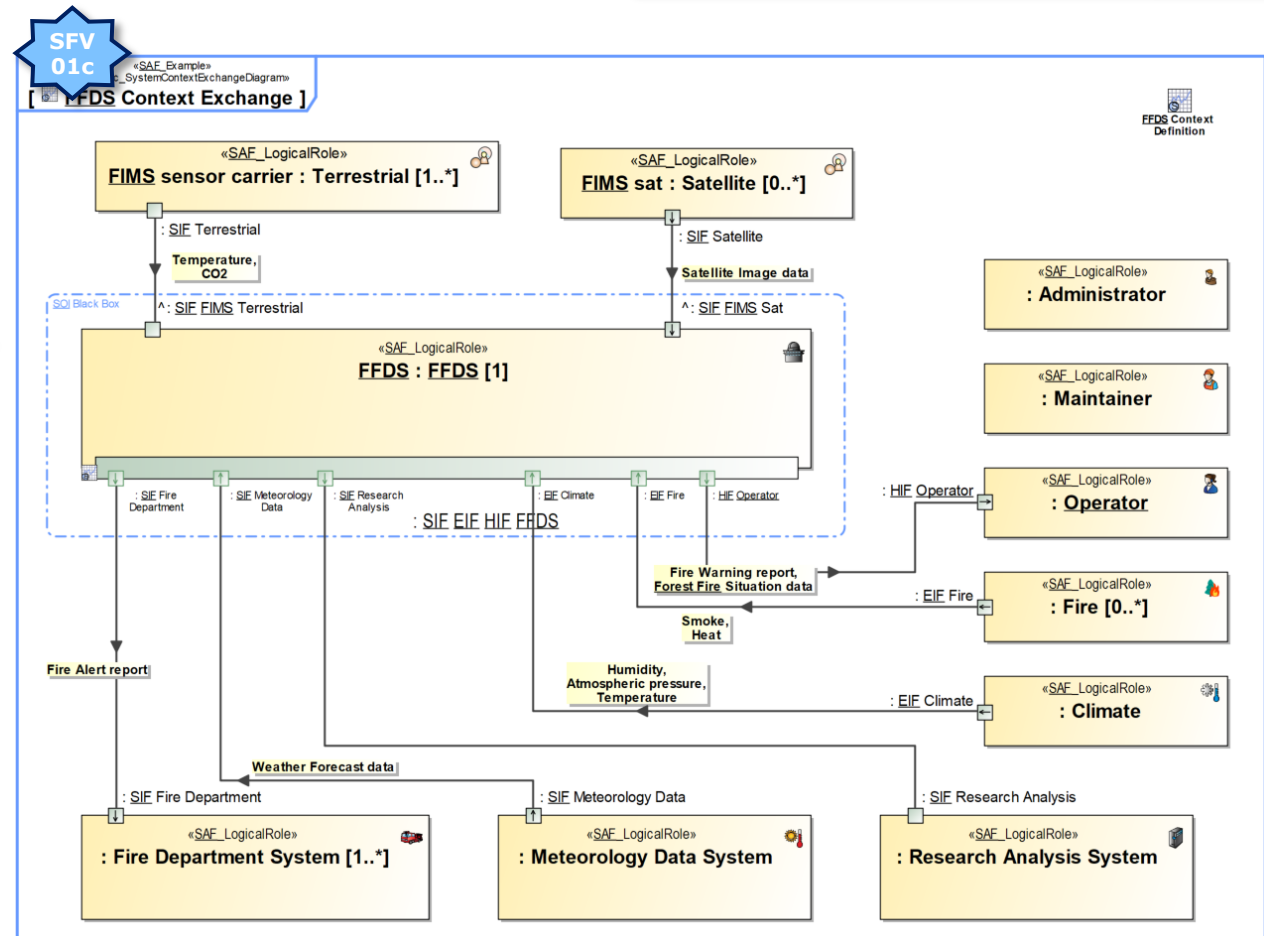
- ➔ Funktionsbaum aus mehreren System Stories konsolidieren
- ➔ Übersicht über Systemfunktionen gewinnen
- ➔ **Quelle für Anforderungen**

# Schritt 7: Austauschbedarfe ableiten

## SFV01c System Context Exchange

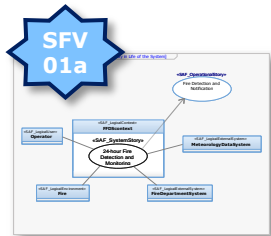


- Grundlage für Schnittstellen Absprachen
- Austauschbedarf identifizieren
- aus funktionalem Austausch ableiten
- **Quelle für Anforderungen**

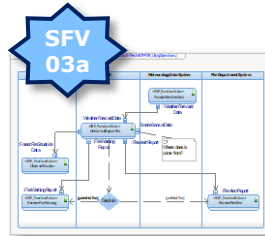


# Schritt 8: System Zustände definieren

## SFV03b System States



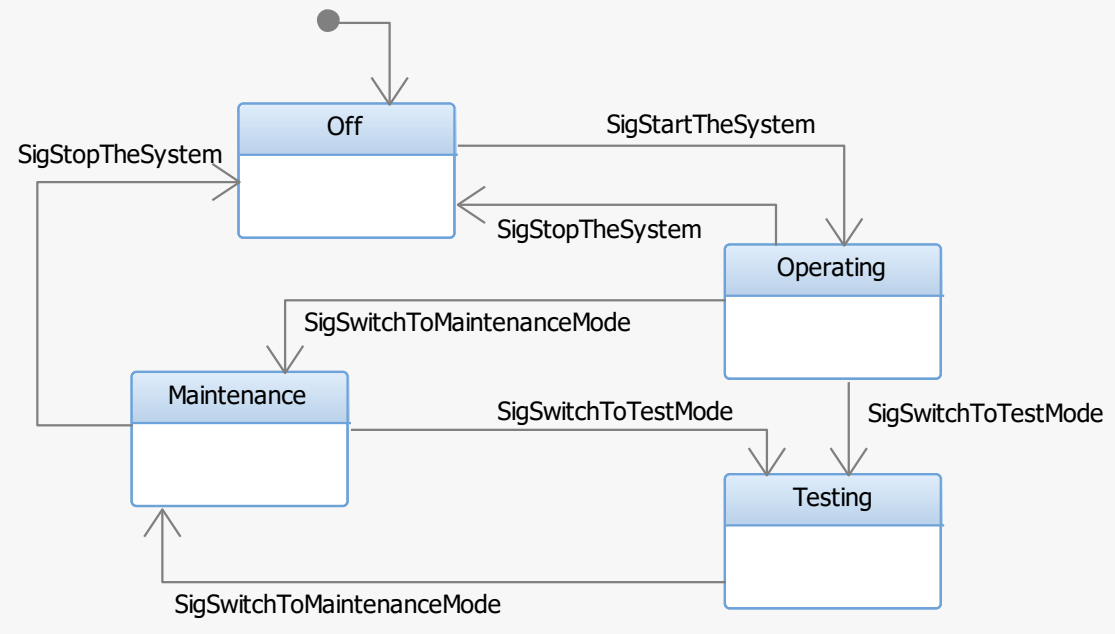
System Story



System Process



«SAF\_SFV03b\_SystemStateMachineDiagram»  
stm [SAF\_Logical SOI] FFDS [FFDS System ModeAndState]



## → System Process

→ Guards

## → System Stories:

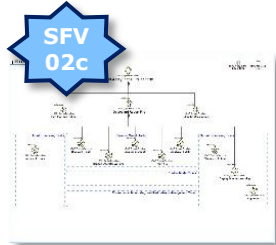
→ Preconditions

→ Postconditions

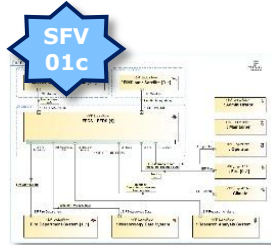
→ Trigger

## → Quelle für Anforderungen

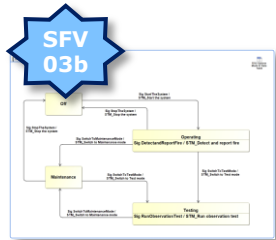
# Schritt 9: System Anforderungen ableiten



System Function Breakdown



System Context Exchange



System States



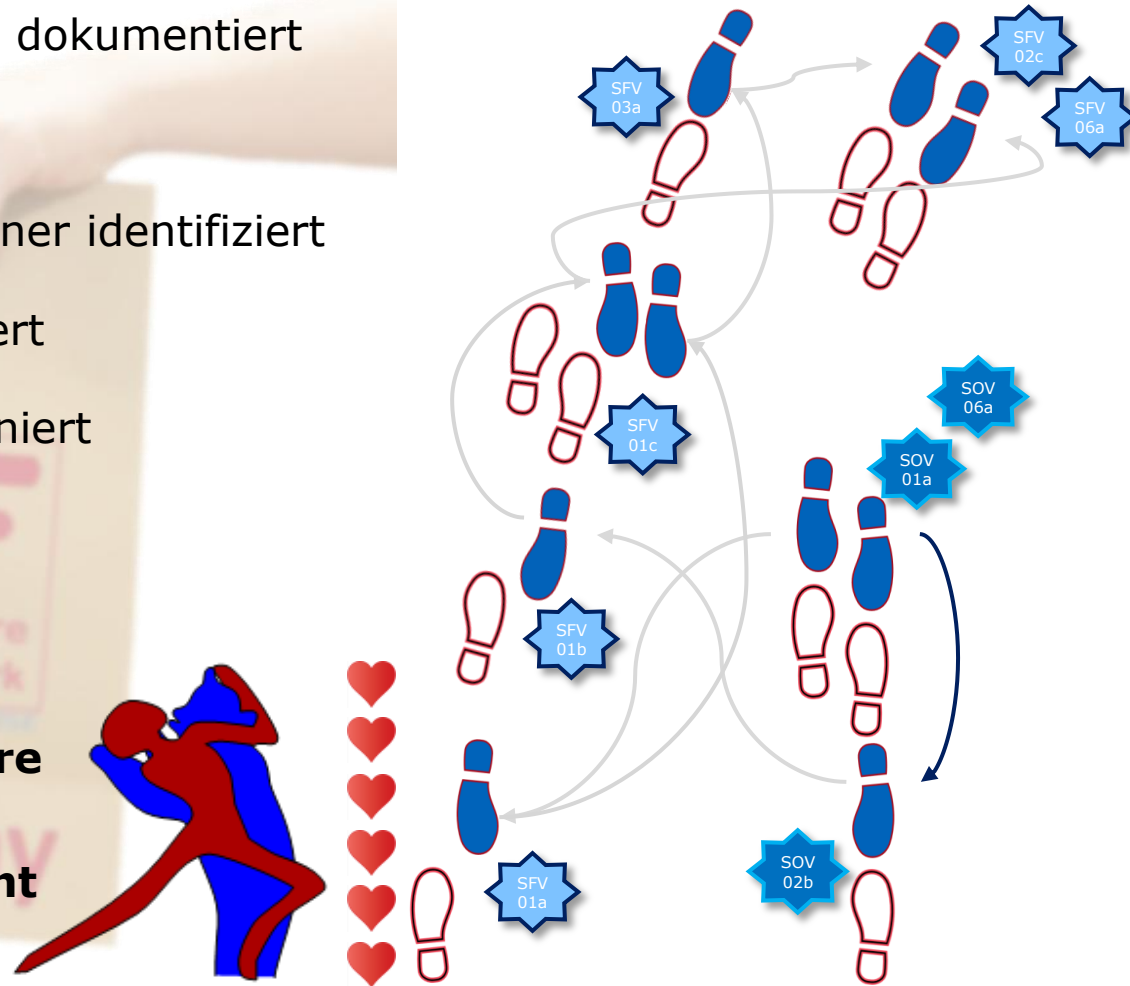
	Name	Text	Source	Risk	Derived from Stk Requirement	Refining System Function
1	Fire Detection					
2	SYS-REQ-001	24/7 Forest Fire Recognition	SDS	High		
3	SYS-REQ-002	Forest Fire Detection	SDS	High	CPBLTY-11 Fire Detection	Retrieve FF data(context FFDS Context)
4	SYS-REQ-002.1	Wireless Sensor Network	SDS	High		
5	SYS-REQ-002.1.1	Wireless Sensor	SDS	Medium		
6	SYS-REQ-002.2	Smoke and Fire Detection Software	SDS	Medium		
7	Fire Monitoring					
8	SYS-REQ-003	Forest Fire Evolution Monitoring	SDS	High	CPBLTY-12 Fire Monitoring	Request FF data(context FFDS Context)
9	Fire Prediction					
10	SYS-REQ-004	Forest Fire Spread Prediction	SDS	Medium	CPBLTY-17 Propagation Estimation	Analyze FF data(context FFDS Context)
11	Fire Assessment					
12	SYS-REQ-005	Forest Fire Damage Assessment	SDS	Medium		

## SFV06a System Requirements

- Systemfunktionen
- Austausch im Systemkontext
- Zustände / Betriebsmodi
- Stakeholder Anforderungen

## Systemanforderungen ableiten und tracen

- Verwendung des Systems umfassend dokumentiert
- Systemgrenze definiert
- Austauschbedarfe und Austauschpartner identifiziert
- Austausch über Systemgrenze definiert
- Systemfunktionen und Zustände definiert
- Begründete Systemanforderungen
- **Übersetzung der Stakeholder Anforderungen in nachvollziehbare Systemanforderungen**
- **Mit Auftraggeber (AG) abgestimmt**
- **Entwicklungsrisiken verringert**

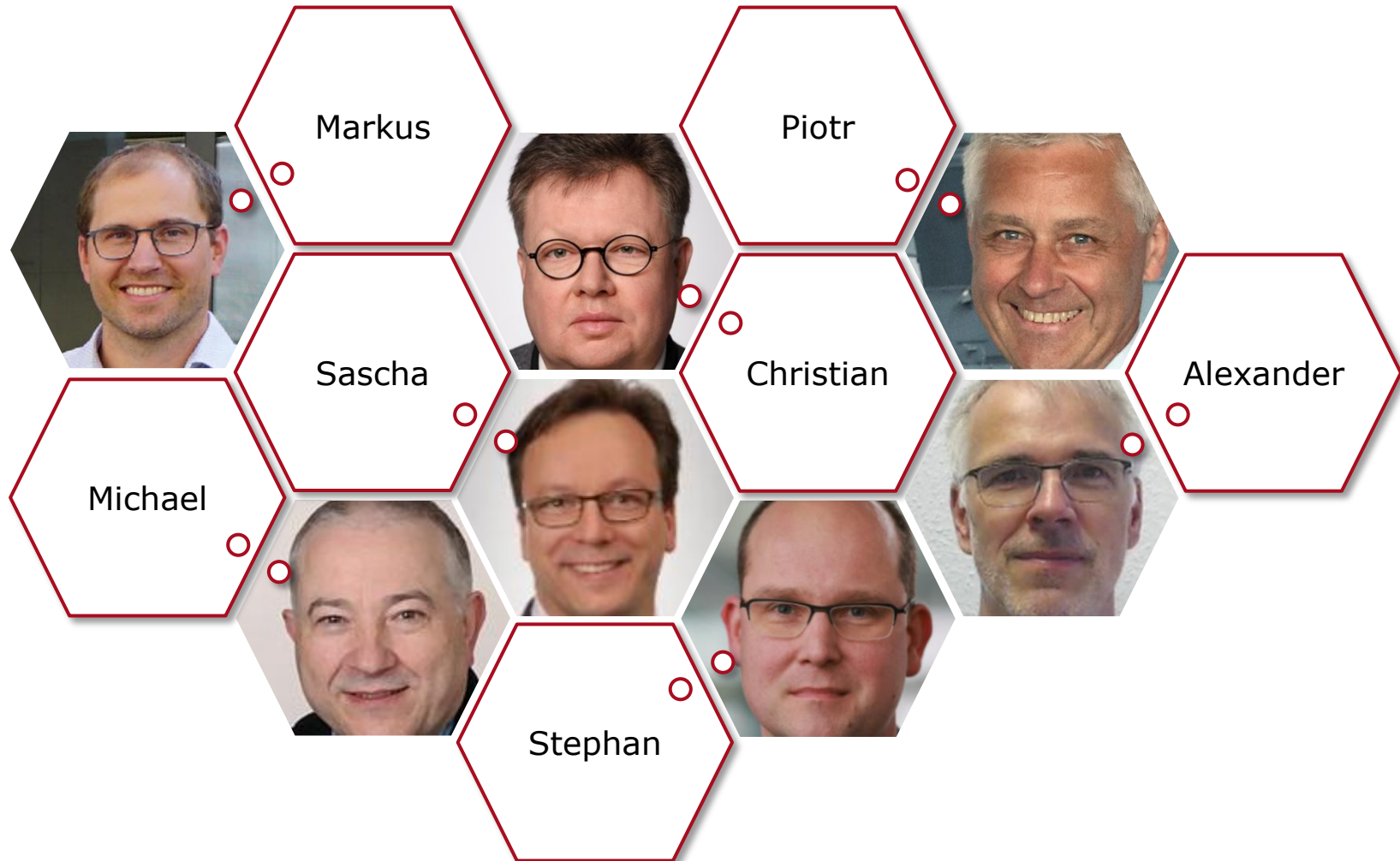


- ➔ Der Vortrag hat einen Weg aufgezeigt, den Barentango mit Hilfe des SAF zu tanzen, um eine vollständige und abgestimmte Systemdefinition zu erhalten.
  
- ➔ **Folgende SAF Eigenschaften erweisen sich als hilfreich:**
  - ➔ **schneller effektiv durch vorgegebene Viewpoints**
  - ➔ **dem Problem angepasster Aufwand**
  - ➔ **nur notwendige Informationen werden erfasst**
  - ➔ **flexibles und kontrolliertes Tailoring**
  - ➔ **vereinfachte Erstellung eines SEMP**





# Team der Präsentation





# Wir bedanken uns für Ihre Aufmerksamkeit

<https://github.com/GfSE/SAF>

**GfSE Arbeitsgruppe SAF**  
**Gesellschaft für Systems Engineering e.V.**