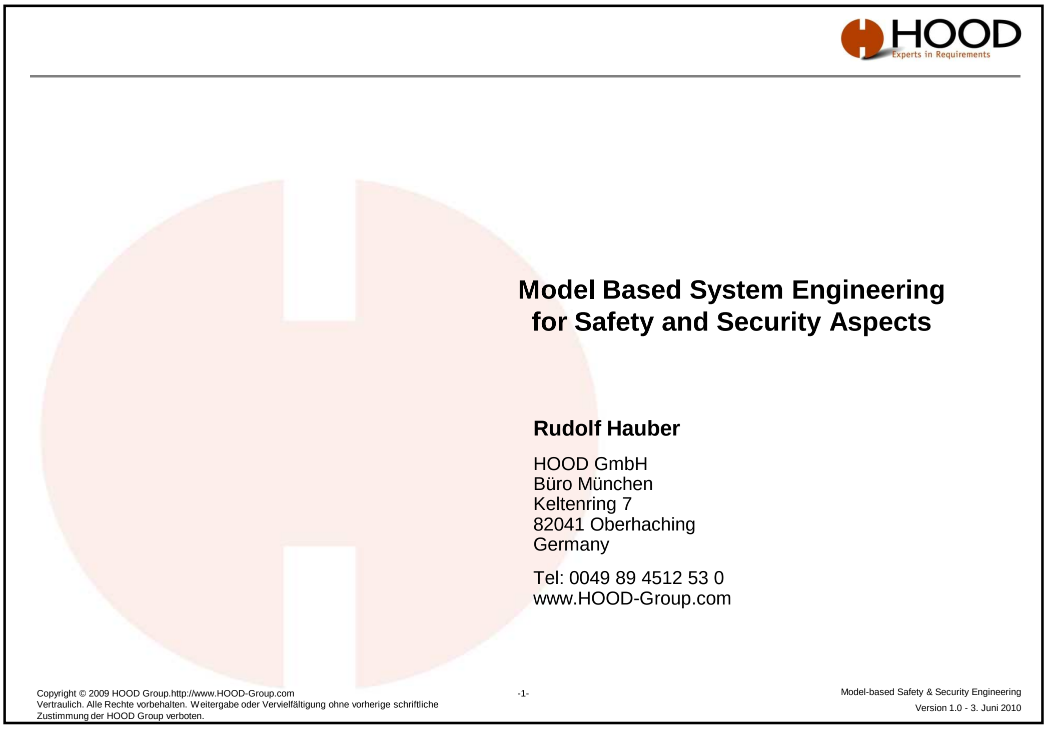
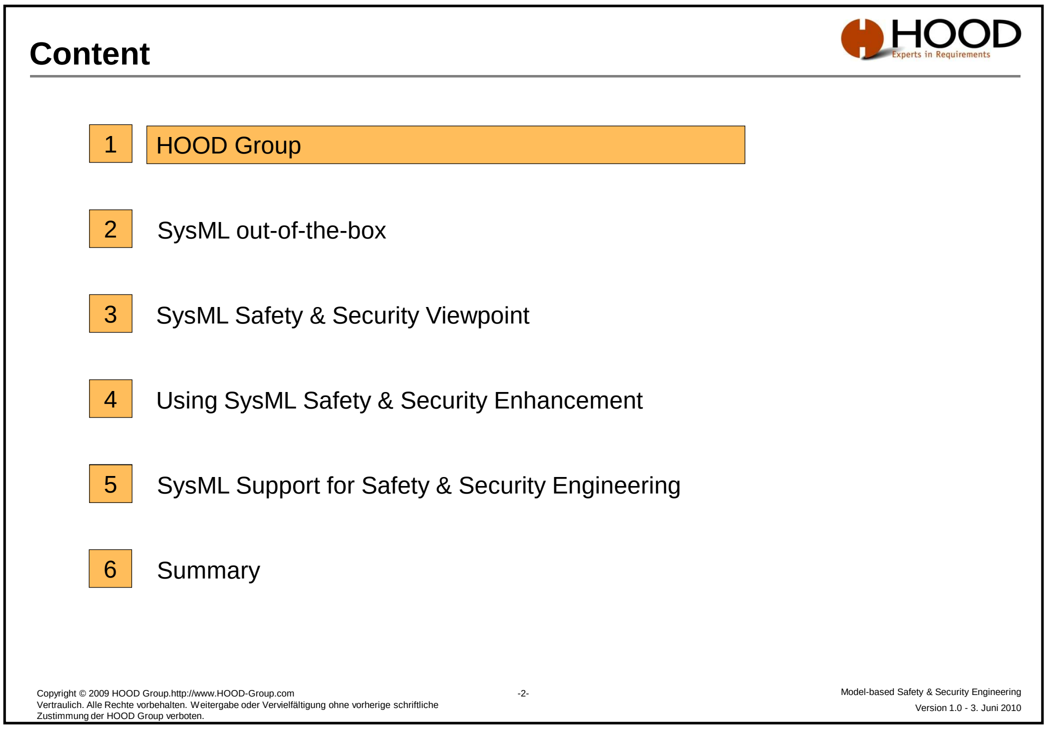


Model Based System Engineering for Safety and Security Aspects

Rudolf Hauber

HOOD GmbH
Büro München
Keltenring 7
82041 Oberhaching
Germany

Tel: 0049 89 4512 53 0
www.HOOD-Group.com



Content

1 HOOD Group

2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

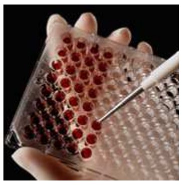
4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

6 Summary

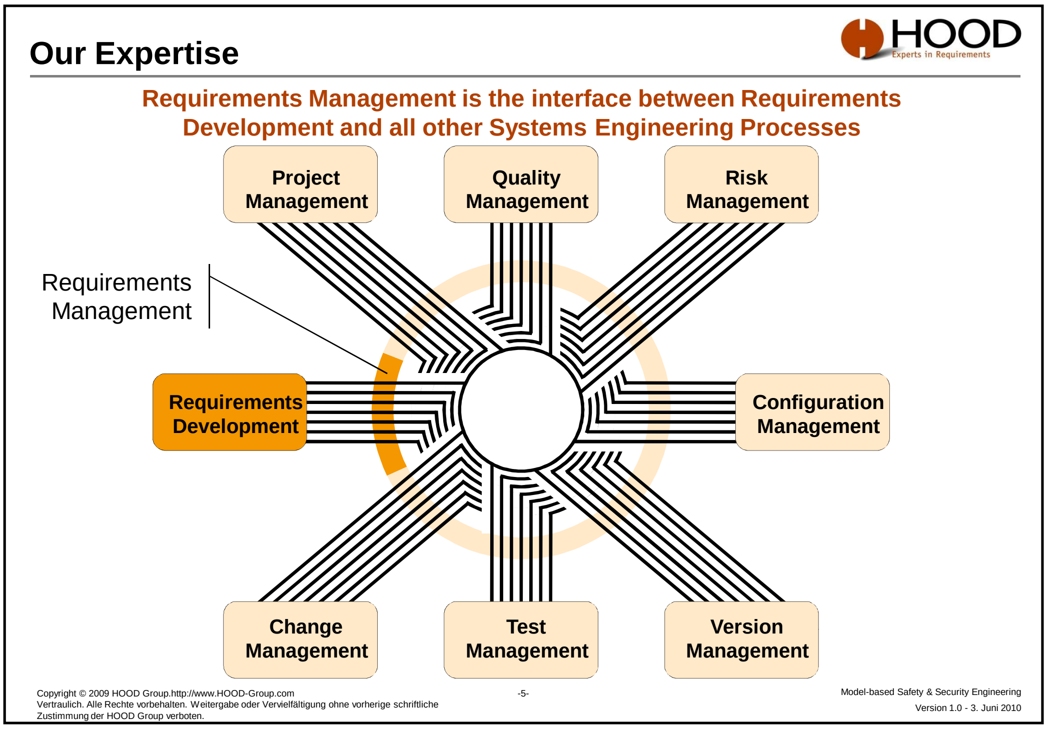
Our Business

The usage of **Requirements Management & Engineering (RM&E)** and continuous process improvement initiatives like CMMI or SPICE are an essential part for big and world wide organisations to develop complex products, services and systems.



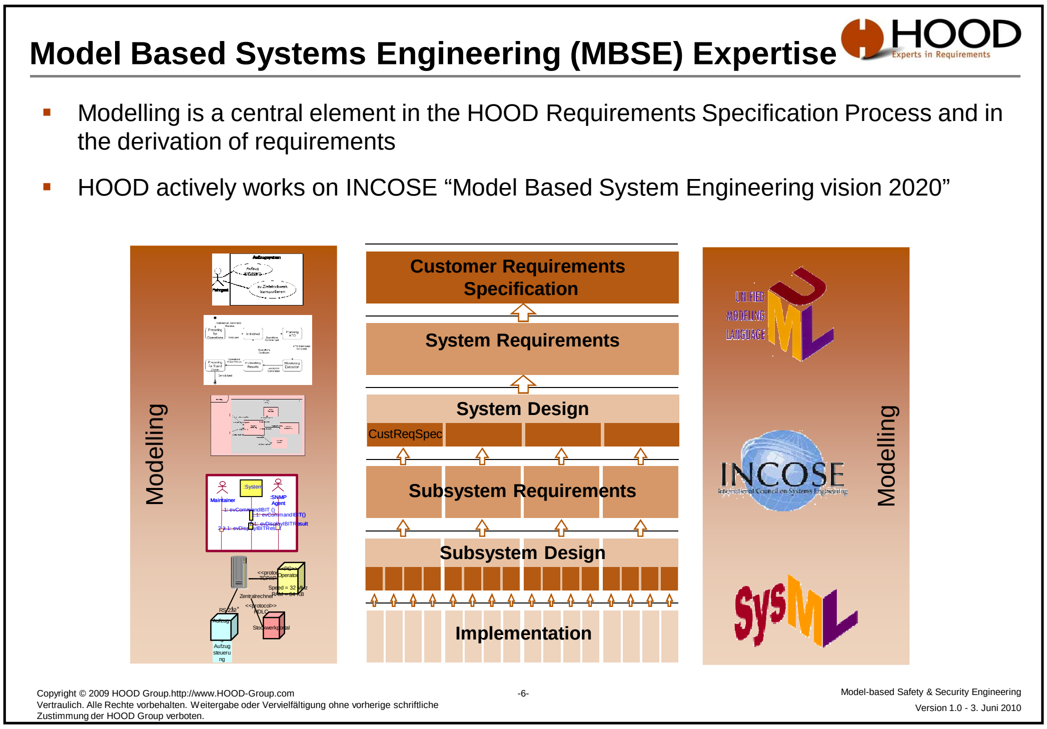
Our Customers

- **Automotive Manufacturer**
  - Adam Opel GmbH
  - Audi AG
  - BMW AG
  - Daimler AG
  - Volkswagen AG
- **Automotive Supplier**
  - Hella KGaA Hueck& Co
  - Robert Bosch GmbH
  - TRW
- **Logistic**
  - Deutsche Bahn AG
  - Schenker Logistics
  - Siemens Mobility
- **Aerospace Industry**
  - EADS
- **Medical Industry**
  - Drägerwerk AG & Co. KGaA
  - Siemens Healthcare
- **Telecommunication**
  - Alcatel-Lucent
  - NetCologne Gesellschaft für Telekommunikation mbH
  - O2 Germany GmbH & Co. OHG
  - Vodafone
- **Banking and Insurance**
  - AXA Konzern AG
  - BMW Bank GmbH
  - Interpolis



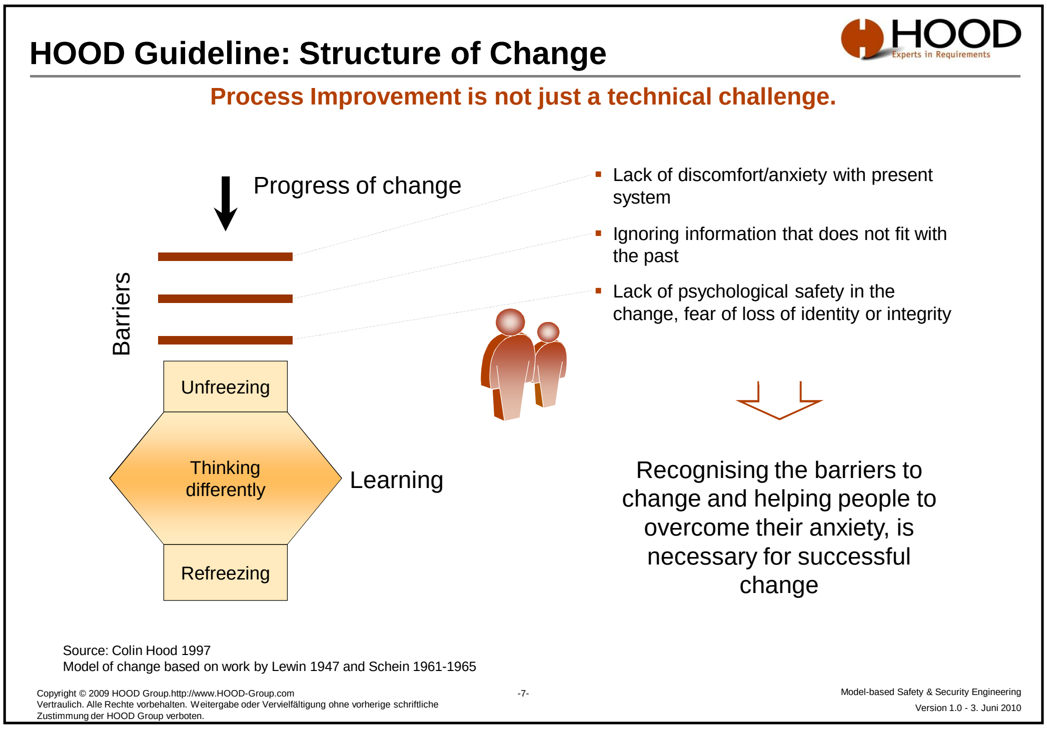
Our Expertise

Requirements Management is the interface between Requirements Development and all other Systems Engineering Processes



Model Based Systems Engineering (MBSE) Expertise

- Modelling is a central element in the HOOD Requirements Specification Process and in the derivation of requirements
- HOOD actively works on INCOSE “Model Based System Engineering vision 2020”



HOOD Guideline: Structure of Change

Process Improvement is not just a technical challenge.

Progress of change

Barriers

Unfreezing

Thinking differently

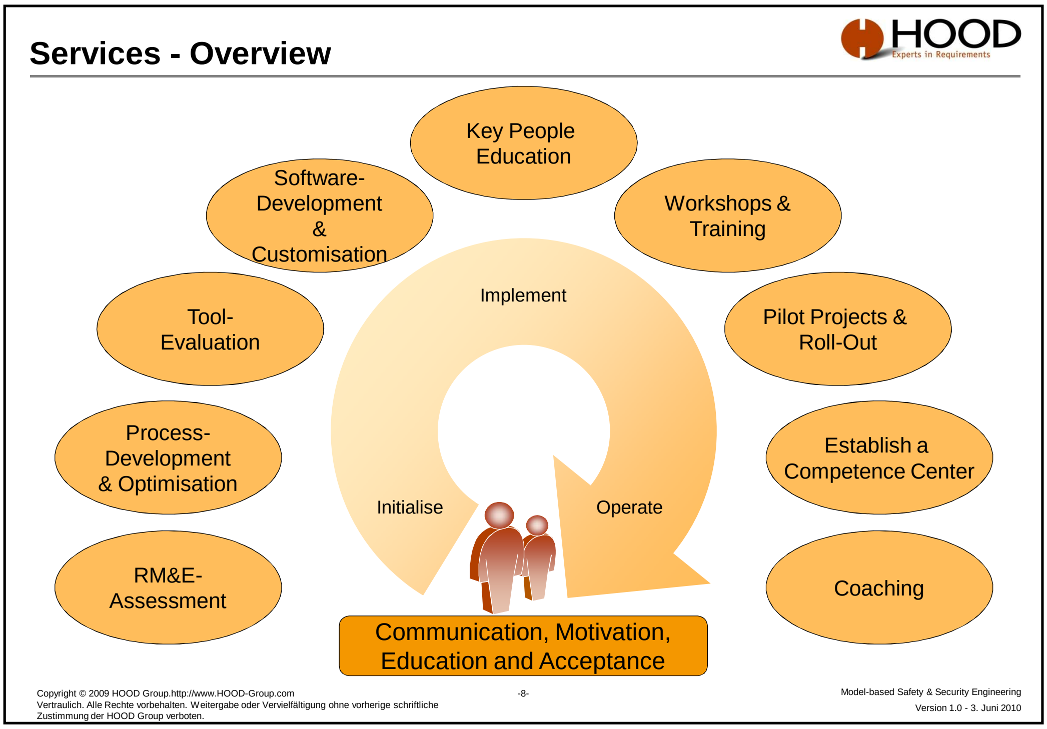
Learning

Refreezing

- Lack of discomfort/anxiety with present system
- Ignoring information that does not fit with the past
- Lack of psychological safety in the change, fear of loss of identity or integrity

Recognising the barriers to change and helping people to overcome their anxiety, is necessary for successful change

Source: Colin Hood 1997
Model of change based on work by Lewin 1947 and Schein 1961-1965



Services - Overview

Key People Education

Workshops & Training

Pilot Projects & Roll-Out

Establish a Competence Center

Coaching

Software-Development & Customisation

Tool-Evaluation

Process-Development & Optimisation

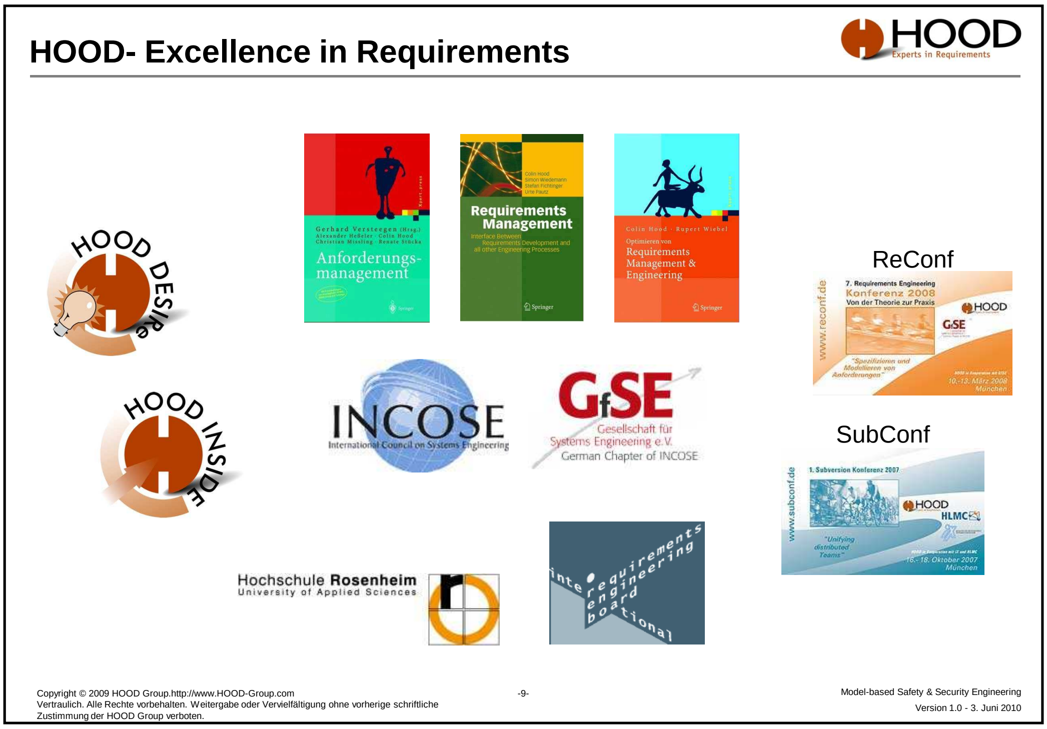
RM&E-Assessment

Implement

Initialise

Operate

Communication, Motivation, Education and Acceptance

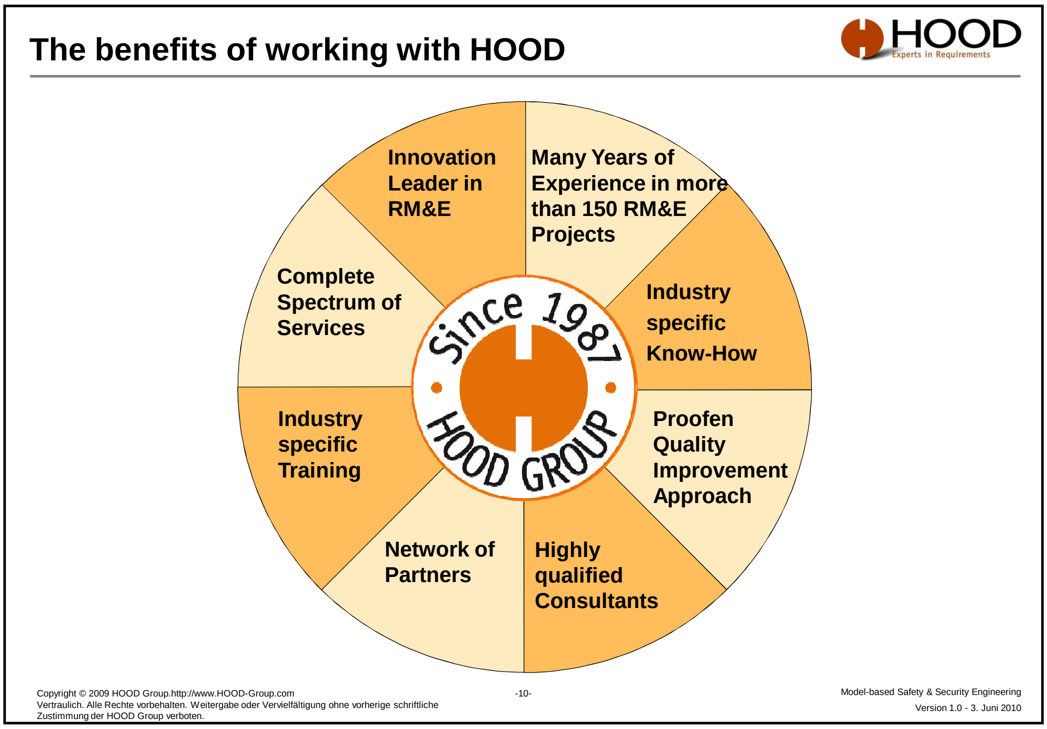


HOOD- Excellence in Requirements

HOOD DESIRe
HOOD INSIDE
Anforderungs-management
Requirements Management
Optimieren von Requirements Management & Engineering
INCOSE
International Council on Systems Engineering
GfSE
Gesellschaft für Systems Engineering e.V.
German Chapter of INCOSE
Hochschule Rosenheim
University of Applied Sciences
international requirements engineering board
www.reconf.de
7. Requirements Engineering Konferenz 2008
Von der Theorie zur Praxis
www.subconf.de
1. Subversion Konferenz 2007

ReConf

SubConf



The benefits of working with HOOD

Innovation Leader in RM&E

Many Years of Experience in more than 150 RM&E Projects

Industry specific Know-How

Proofen Quality Improvement Approach

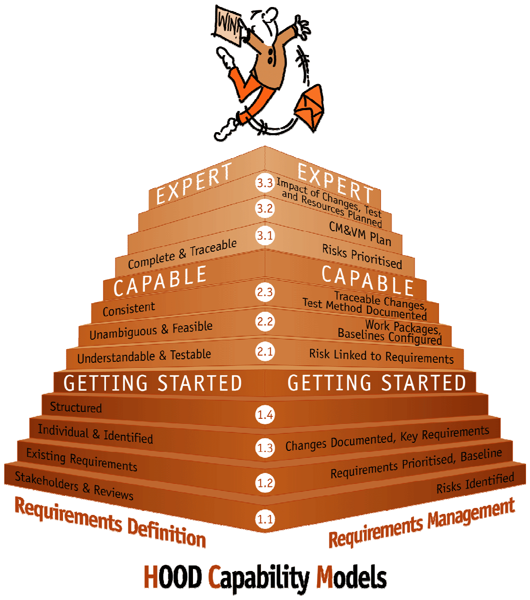
Highly qualified Consultants

Network of Partners

Industry specific Training

Complete Spectrum of Services

HCMs – Requirements Management & Definition



Content

1 HOOD Group

2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

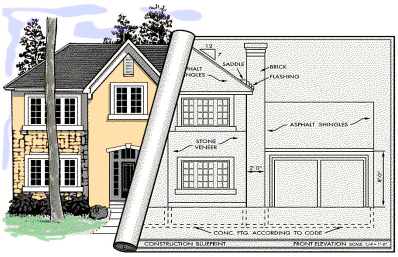
6 Summary

Motivation

System- and Software-Development is not easy!

- Using models for problem area and solution area
  - reduces complexity
  - facilitates communication
  - eases re-use

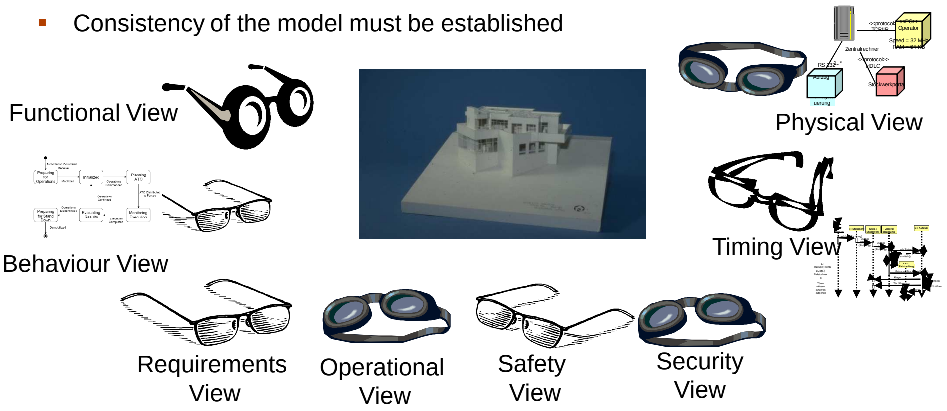
- Modeling is well-established engineering technique
- Benefits for different stakeholders
  - Customer
  - Project management
  - Development
  - Quality assurance
  - Other stakeholders

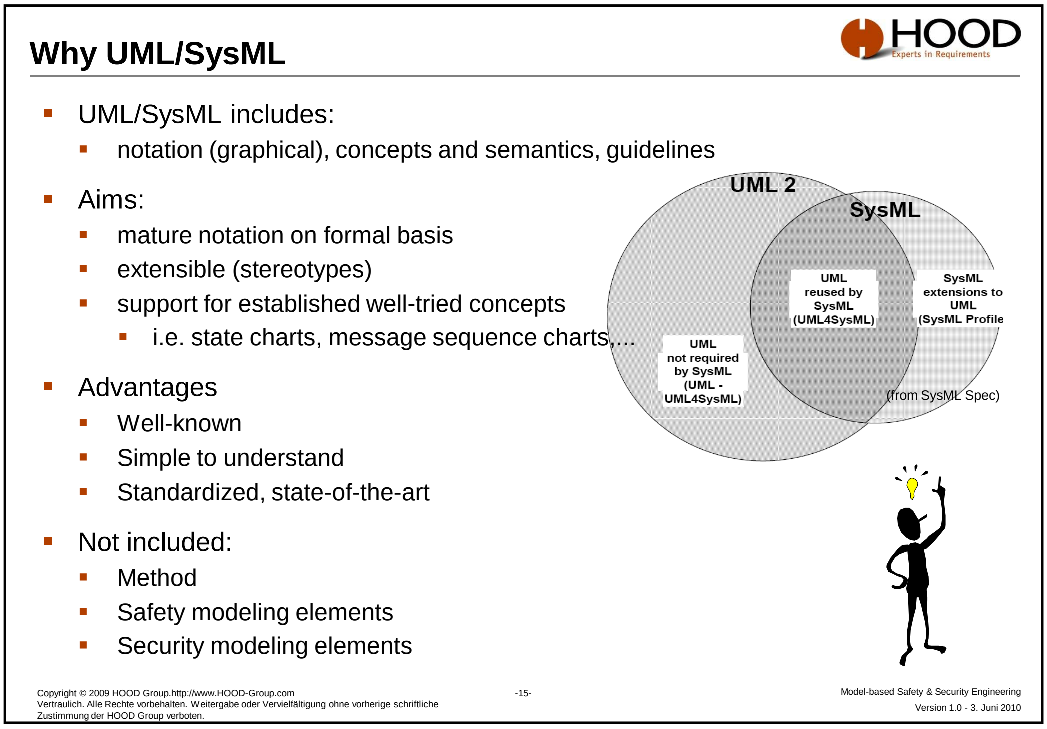


(Von Rational Websources)

Views, models and diagrams

- Different types of diagrams show different aspects of the system
- Aspects complement and overlap one another
- Architecture frameworks guide the creation of models
- Consistency of the model must be established

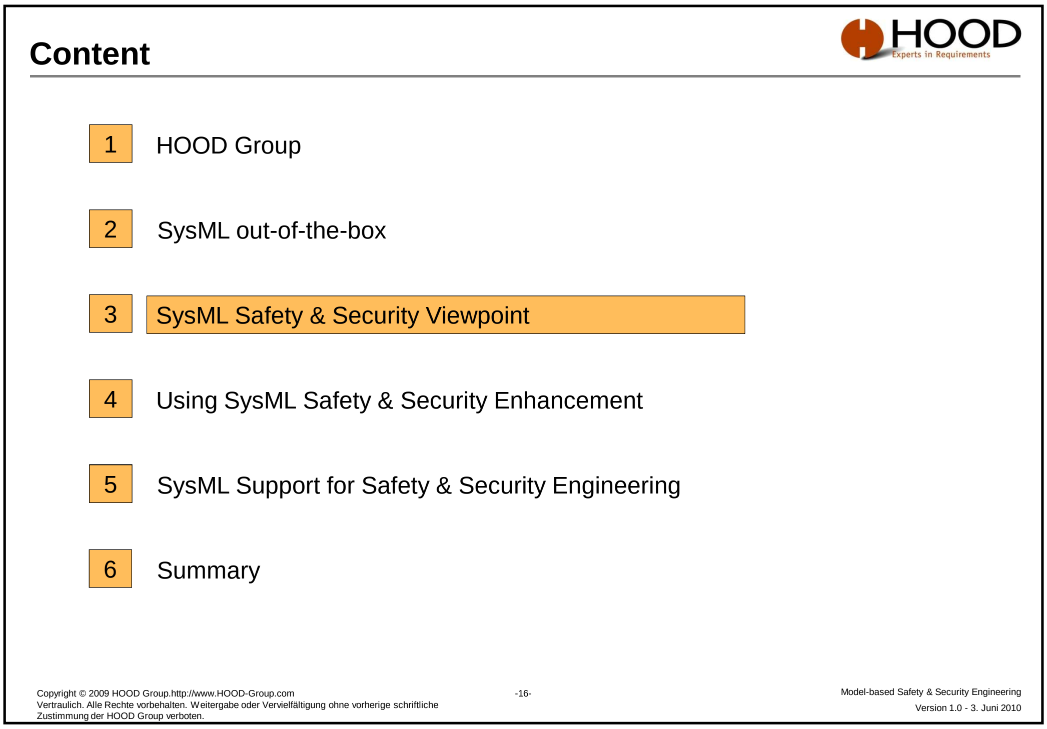




Why UML/SysML

- UML/SysML includes:
  - notation (graphical), concepts and semantics, guidelines
- Aims:
  - mature notation on formal basis
  - extensible (stereotypes)
  - support for established well-tried concepts
    - i.e. state charts, message sequence charts,...
- Advantages
  - Well-known
  - Simple to understand
  - Standardized, state-of-the-art
- Not included:
  - Method
  - Safety modeling elements
  - Security modeling elements

UML 2
SysML
UML not required by SysML (UML - UML4SysML)
UML reused by SysML (UML4SysML)
SysML extensions to UML (SysML Profile
(from SysML Spec)



Content

1 HOOD Group

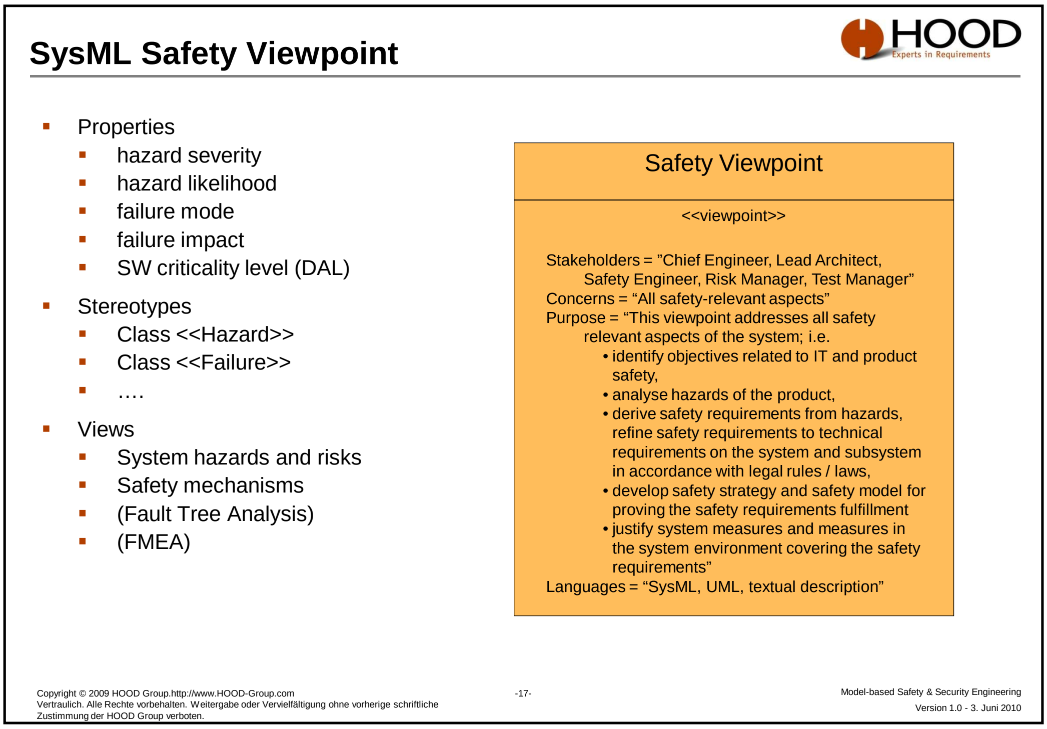
2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

6 Summary



SysML Safety Viewpoint

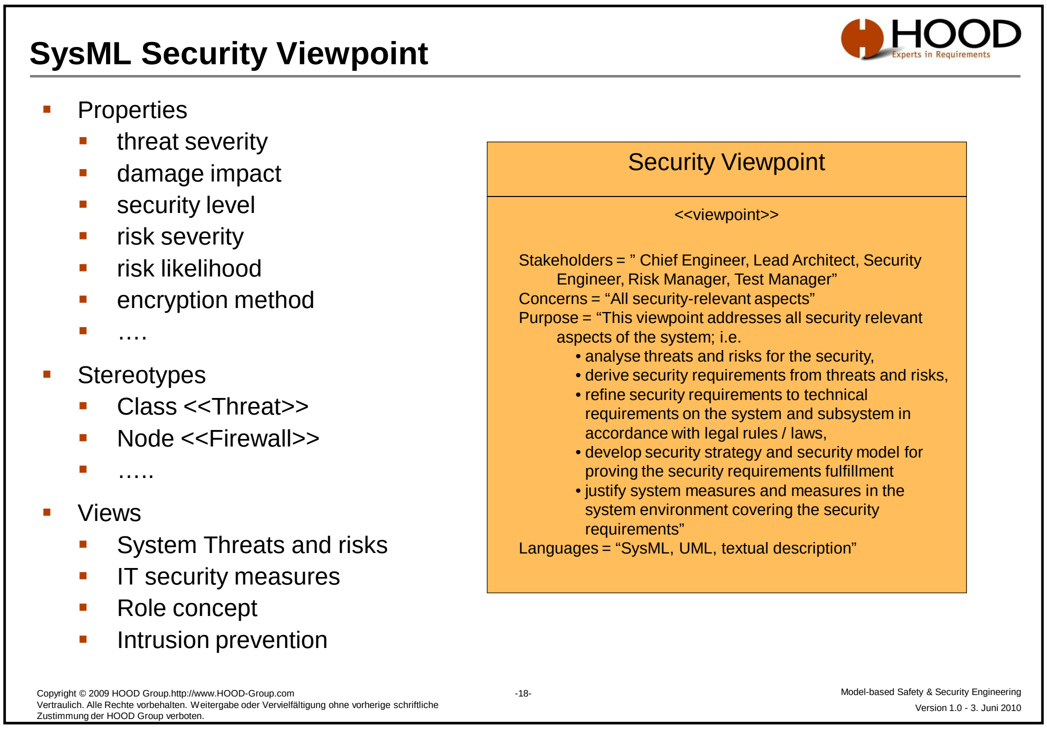
- Properties
  - hazard severity
  - hazard likelihood
  - failure mode
  - failure impact
  - SW criticality level (DAL)
- Stereotypes
  - Class <<Hazard>>
  - Class <<Failure>>
  - ….
- Views
  - System hazards and risks
  - Safety mechanisms
  - (Fault Tree Analysis)
  - (FMEA)

Safety Viewpoint

<<viewpoint>>

Stakeholders = "Chief Engineer, Lead Architect, Safety Engineer, Risk Manager, Test Manager"
Concerns = "All safety-relevant aspects"
Purpose = "This viewpoint addresses all safety relevant aspects of the system; i.e.
- identify objectives related to IT and product safety,
- analyse hazards of the product,
- derive safety requirements from hazards, refine safety requirements to technical requirements on the system and subsystem in accordance with legal rules / laws,
- develop safety strategy and safety model for proving the safety requirements fulfillment
- justify system measures and measures in the system environment covering the safety requirements"

Languages = "SysML, UML, textual description"



SysML Security Viewpoint

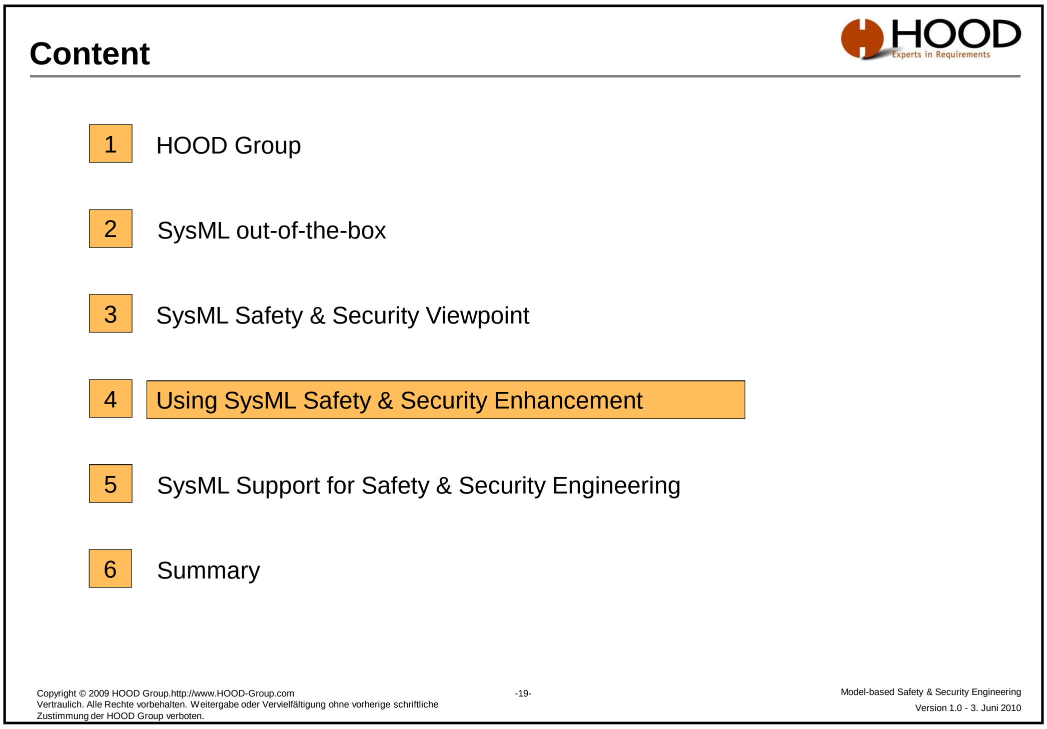
- Properties
  - threat severity
  - damage impact
  - security level
  - risk severity
  - risk likelihood
  - encryption method
  - ….
- Stereotypes
  - Class <<Threat>>
  - Node <<Firewall>>
  - …..
- Views
  - System Threats and risks
  - IT security measures
  - Role concept
  - Intrusion prevention

Security Viewpoint

<<viewpoint>>

Stakeholders = " Chief Engineer, Lead Architect, Security Engineer, Risk Manager, Test Manager"
Concerns = "All security-relevant aspects"
Purpose = "This viewpoint addresses all security relevant aspects of the system; i.e.
- analyse threats and risks for the security,
- derive security requirements from threats and risks,
- refine security requirements to technical requirements on the system and subsystem in accordance with legal rules / laws,
- develop security strategy and security model for proving the security requirements fulfillment
- justify system measures and measures in the system environment covering the security requirements"

Languages = "SysML, UML, textual description"



Content

HOOD Experts in Requirements

1 HOOD Group

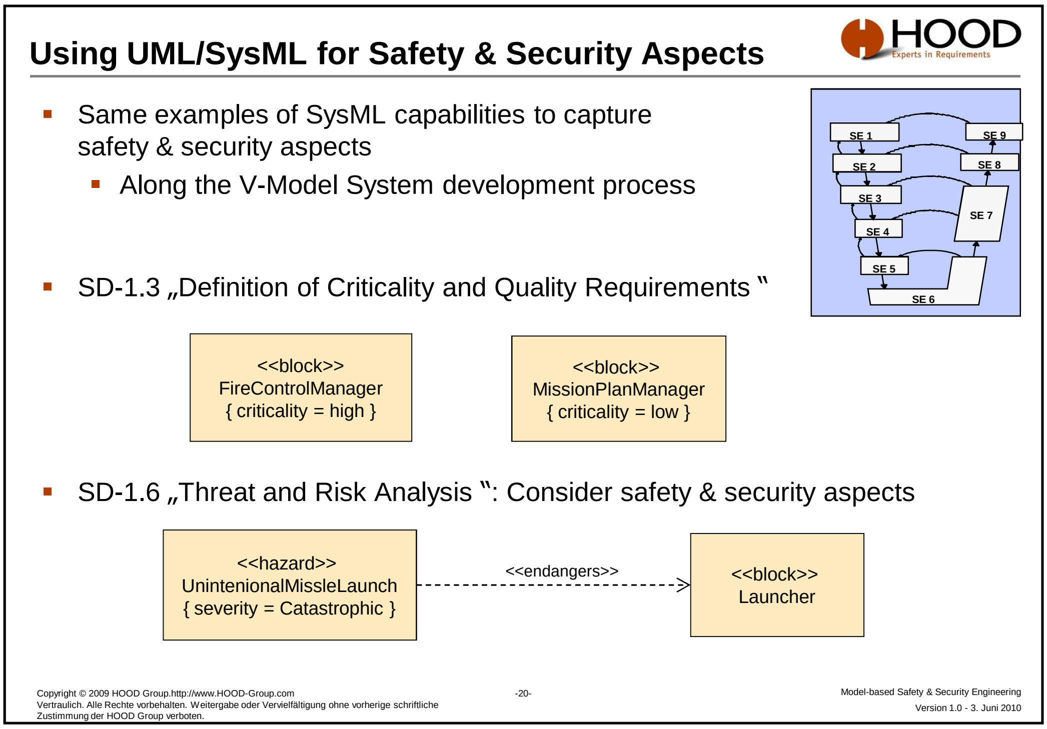
2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

6 Summary



Using UML/SysML for Safety & Security Aspects

HOOD Experts in Requirements

- Same examples of SysML capabilities to capture safety & security aspects
  - Along the V-Model System development process
- SD-1.3 „Definition of Criticality and Quality Requirements ‟

<<block>>
FireControlManager
{ criticality = high }

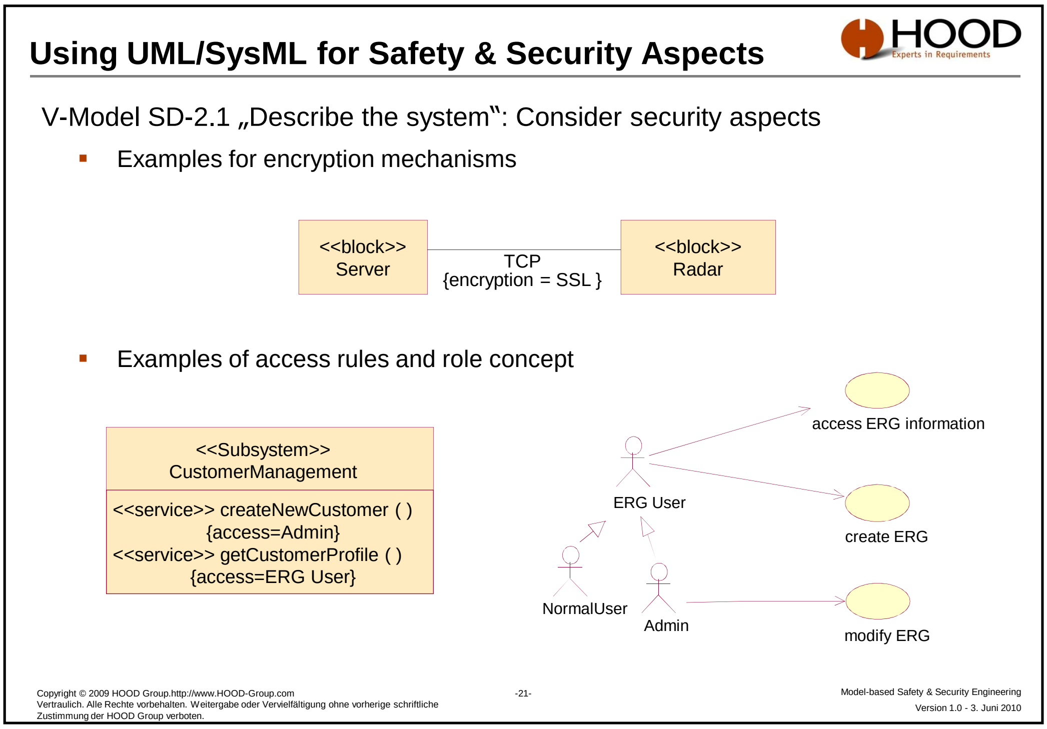
<<block>>
MissionPlanManager
{ criticality = low }

- SD-1.6 „Threat and Risk Analysis ‟: Consider safety & security aspects

<<hazard>>
UnintenionalMissleLaunch
{ severity = Catastrophic }

<<endangers>>

<<block>>
Launcher



Using UML/SysML for Safety & Security Aspects

V-Model SD-2.1 „Describe the system": Consider security aspects

- Examples for encryption mechanisms

<<block>> Server

TCP {encryption = SSL }

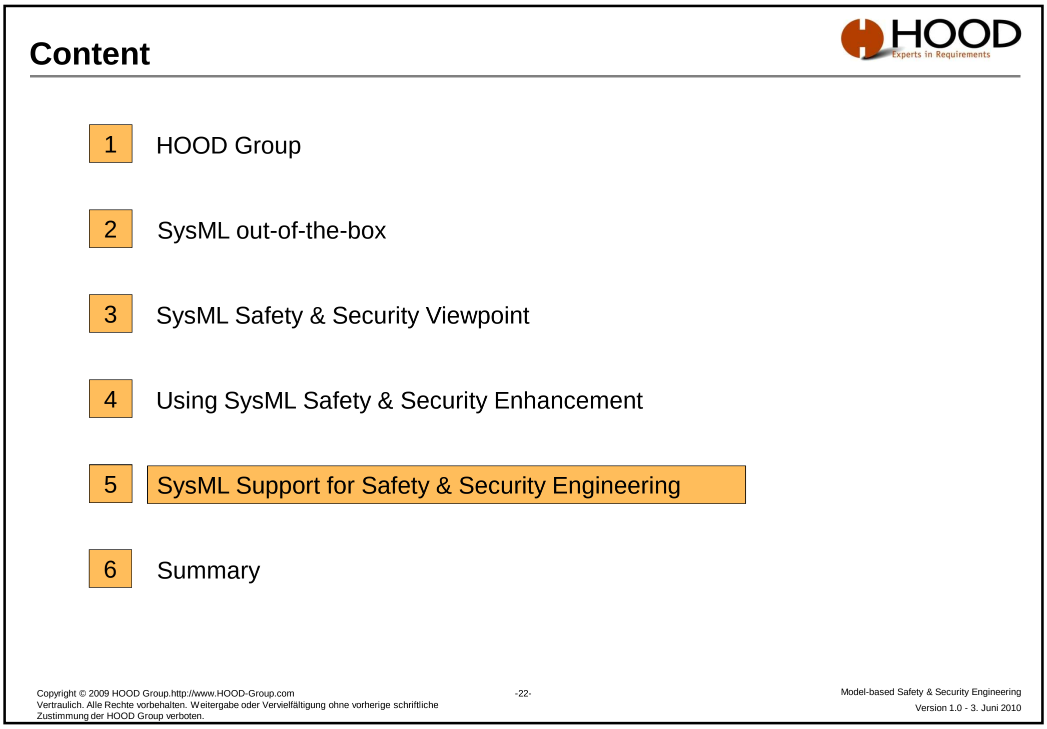
<<block>> Radar

- Examples of access rules and role concept

<<Subsystem>> CustomerManagement

<<service>> createNewCustomer ( ) {access=Admin}

<<service>> getCustomerProfile ( ) {access=ERG User}



Content

1 HOOD Group

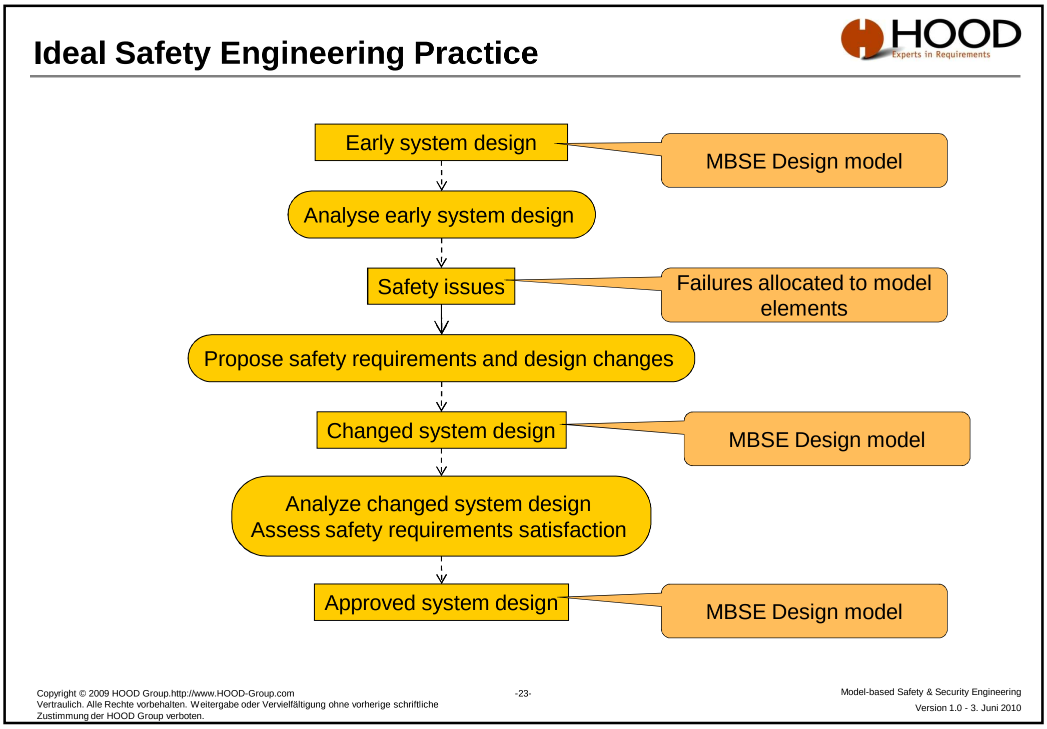
2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

6 Summary



Ideal Safety Engineering Practice

Early system design

MBSE Design model

Analyse early system design

Safety issues

Failures allocated to model elements

Propose safety requirements and design changes

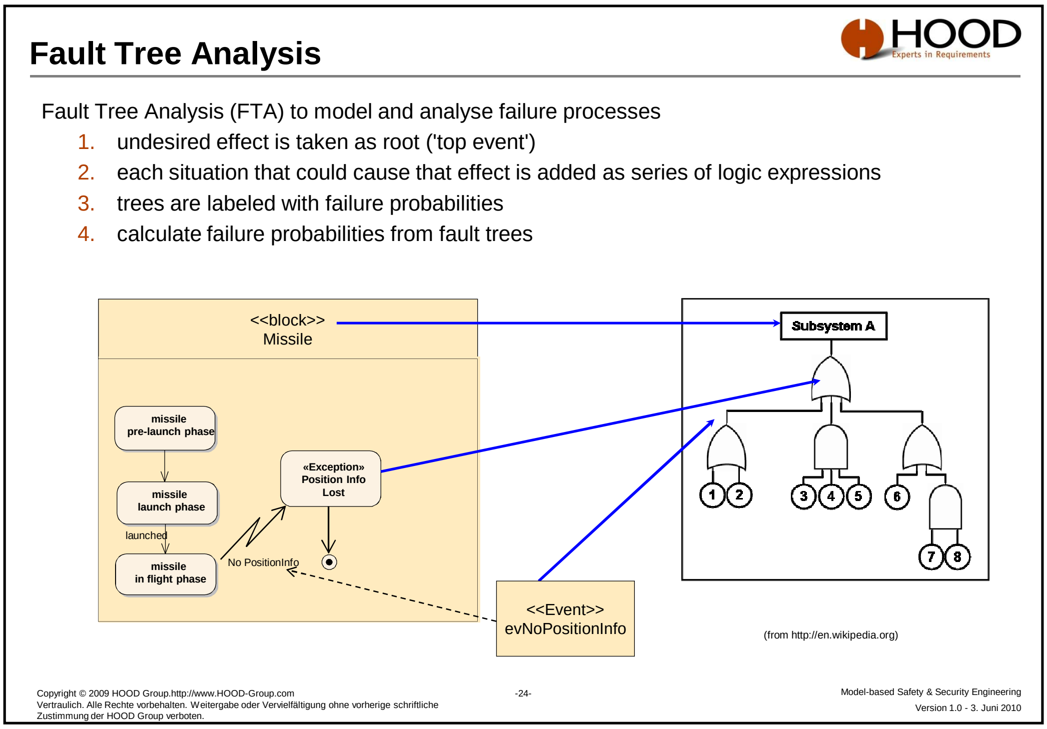
Changed system design

MBSE Design model

Analyze changed system design
Assess safety requirements satisfaction

Approved system design

MBSE Design model



Fault Tree Analysis

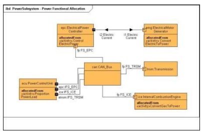
Fault Tree Analysis (FTA) to model and analyse failure processes

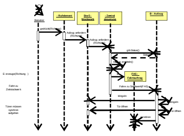
1. undesired effect is taken as root ('top event')
2. each situation that could cause that effect is added as series of logic expressions
3. trees are labeled with failure probabilities
4. calculate failure probabilities from fault trees

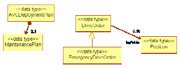
(from http://en.wikipedia.org)

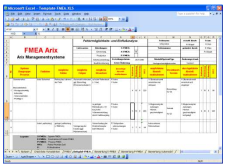
Failure Modes and Effects Analysis

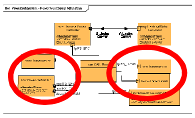
1. Identify system components/ structure
   - Exists in IBDs of DoDAF SV-1
2. Define functions of components
   - Exists as result of DoDAF SV-10c
3. Analysis failures
   a. Allocate possible failure to components
   b. Analyse failure impact based on data/material flows
      - DoDAF SV-10c + DoDAF SV11
4. Asses risks
   1. Failure impact
   2. Failure occurance probability
   3. Failure detection probability
   ➢ Risk priority number (RPN)
5. Improve system design
   ➢ Model based









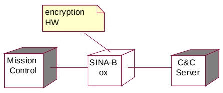


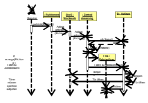
Reliability Availability Maintainability Sustainability (RAMS)

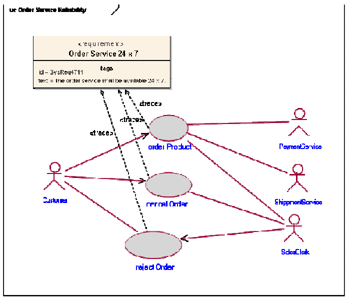
Identify system items failures/ out of order

➔ IBDs of physical architecture/ deployment diagrams

1. Identify local impact
   ➔ Collaboration of physical items
2. Identify site impact
3. Identify impact on overall system functionality
4. Check reliability/ availability requirements
5. Calculate RAMS based on
   - Mean Time Between Failure (MTBF)
   - Cycle replacement time
   - …

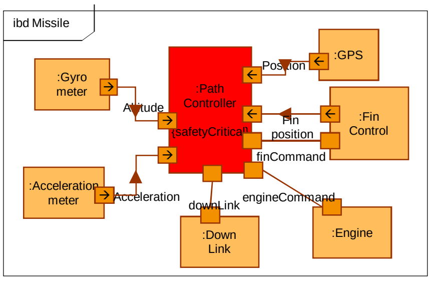


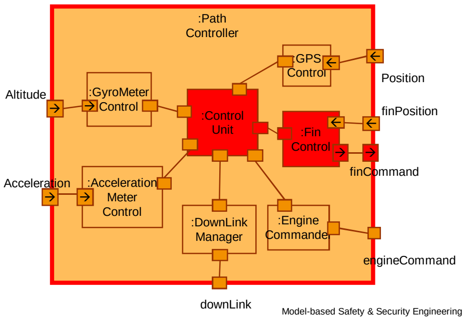




Safety Criticality Analysis

1. Identify safety critical system components
   - Based on system structure
2. Analyze „propagation“ of safety critical parts
   - Model based Analysis
3. System design improvement under safety aspects





Content

1 HOOD Group

2 SysML out-of-the-box

3 SysML Safety & Security Viewpoint

4 Using SysML Safety & Security Enhancement

5 SysML Support for Safety & Security Engineering

6 Summary

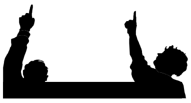
Summary

- MBSE SysML out of the box: No specific safety & security view
- Enhancement of SysML by safety & security profile
  - Viewpoint, stereotypes, properties, etc.
- Process: embedded in overall engineering process
- SysML can be used for capturing of security and safety aspects
- SysML can be used in an MBSE approach for
  - Hazard analysis
  - Fault tree analysis
  - Failure mode and effects analysis (FMEA)
  - Criticality assessment
  - Risk assessment and risk management
  - Probabilistic Risk Assessment
- SysML Safety & Security profile should be standardized
- Tool-interfaces should be standardized

Discussion

Thanks for your attention!

Questions & Discussion



Please contact me: Dr. Rudolf Hauber
Senior Consultant HOOD Group
Responsible for Aerospace and Defense
Rudolf.Hauber@HOOD-Group.com
+49 173 394 1162