Model-supported Risk Management

Rudolf Hauber

HOOD GmbH
Büro München
Keltenring 7
82041 Oberhaching
Germany

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

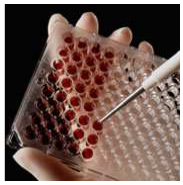
Content

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.





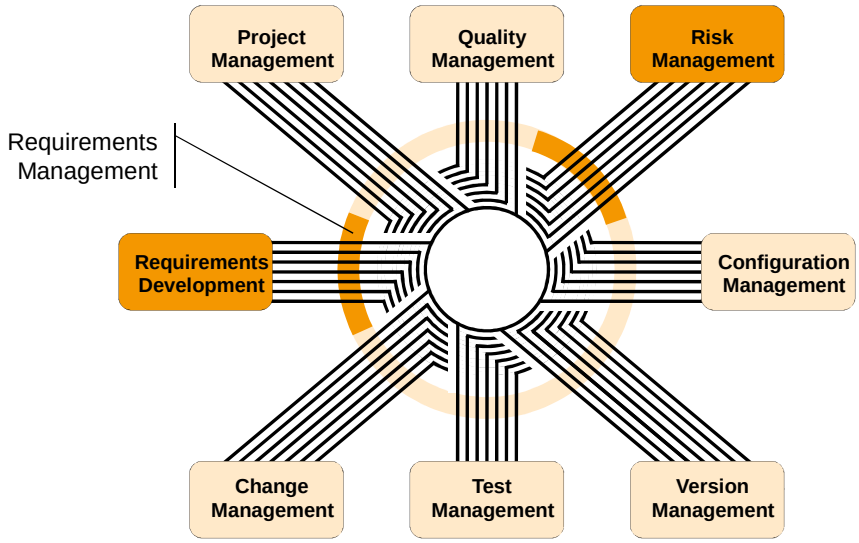


Einige Kunden, die Vertrauen in HOOD setzen

- **Automobilhersteller**
  - Adam Opel GmbH
  - Audi AG
  - BMW AG
  - Daimler AG
  - Volkswagen AG
- **Automobilzulieferer**
  - Hella KGaA Hueck& Co
  - Robert Bosch GmbH
  - TRW
- **Logistik/ Transportation**
  - Deutsche Bahn AG
  - Schenker Logistics
  - Siemens Mobility
  - Thales Group
- **IT/ Software-Development**
  - BMW AG
  - Volkswagen AG
  - Deutsche Nationalbibliothek
- **Luft- und Raumfahrt**
  - EADS
  - Astrium
  - Airbus
- **Medizintechnik**
  - Drägerwerk AG & Co. KGaA
  - Siemens Healthcare
  - CareFusion (Viasys Healthcare)
- **Telekommunikation**
  - Alcatel-Lucent
  - NetCologne Gesellschaft für Telekommunikation mbH
  - O2 Germany GmbH & Co. OHG
- **Banken und Versicherungen**
  - AXA Konzern AG
  - BMW Bank GmbH
  - Interpolis

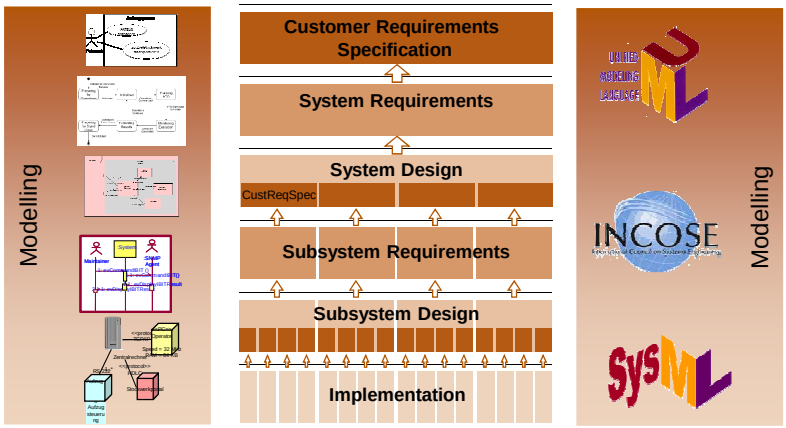
Our Expertise

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



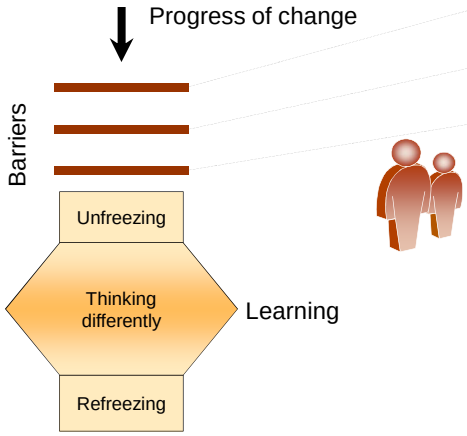
Model Based Systems Engineering (MBSE) Expertise

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



HOOD Guideline: Structure of Change

Process Improvement is not just a technical challenge.

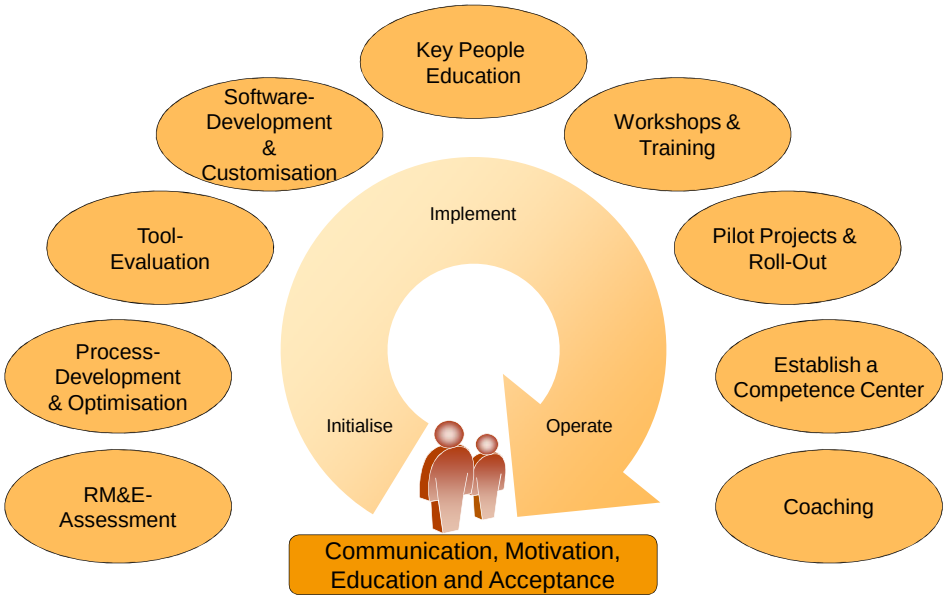


- Lack of discomfort/anxiety with present system
- Ignoring information that does not fit with the past
- Lack of psychological safety in the change, fear of loss of identity or integrity

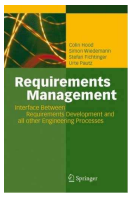
Recognising the barriers to change and helping people to overcome their anxiety, is necessary for successful change

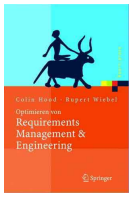
Source: Colin Hood 1997
Model of change based on work by Lewin 1947 and Schein 1961-1965

Services - Overview



HOOD- Excellence in Requirements



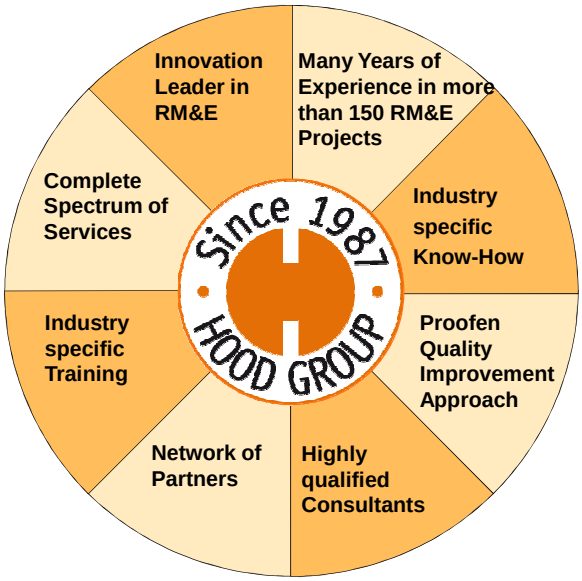


ReConf

SubConf

Hochschule Rosenheim
University of Applied Sciences

The benefits of working with HOOD

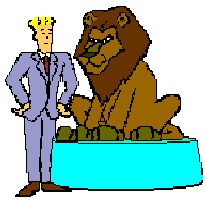


HCMs – Requirements Management & Definition

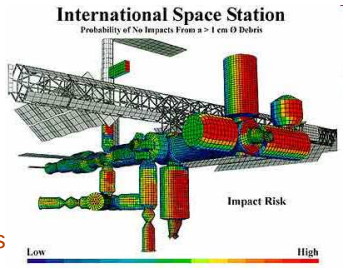
Content

Motivation

- There are a lot of risks
  - Financial
  - Contractual
  - Legal
  - Too late to market
  - Supplier
  - Technical
  - …..



- There are a lot of technical risks
  - New/unknown technique
  - Very high performance
  - Very high availability
  - Very high safety requirements
  - Very high security requirements
  - …



(from Wikimedia commons)

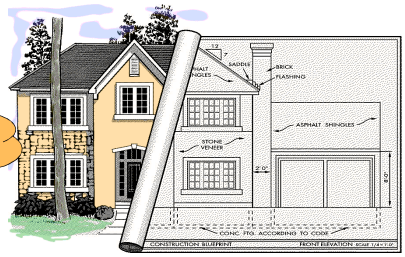
Motivation

Development of technical systems is not easy!

- Modeling is a well-established engineering techniqu
- Using models for problem area and solution area
  - reduces complexity
  - facilitates communication
  - eases re-use
  - reduces development risks

- Benefits for different stakeholders
  - Customers
  - Project management
  - Development
  - Quality assurance
  - Other stakeholders

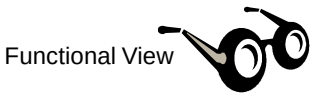
What about risk management?

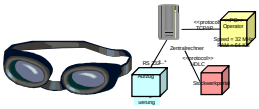


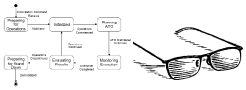
(Von Rational Websources)

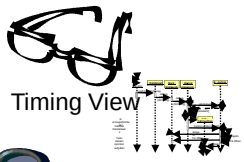
Views, models and diagrams

- 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



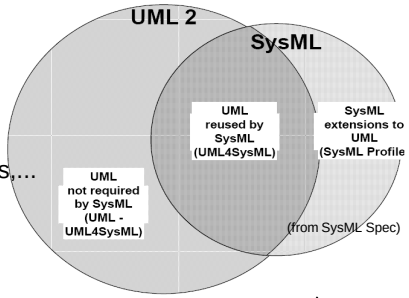






Why UML/SysML

- 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
  - Elements for risk identification & management



Content

SysML Safety Viewpoint

- Properties
  - risk severity
  - risk likelihood
  - hazard severity
  - hazard likelihood
  - criticality
  - …
- Stereotypes
  - Class <<Risk>>
  - Class <<Hazard>>
  - Class <<Threat>>
  - ….
- Views
  - System hazards, threads and risks
  - Safety mechanisms (Fault Tree Analysis,
  - Risk tracing
  - Risk mitigation measures

Risk Viewpoint

<<viewpoint>>

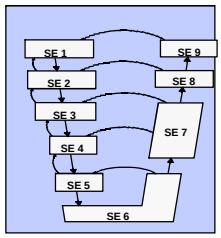
Stakeholders = ”Chief Engineer, Lead Architect, Safety Engineer, Risk Manager, Test Manager”
Concerns = “All risk management-relevant aspects”
Purpose = “This viewpoint addresses all risk management-relevant relevant aspects of the system; i.e.
- identify risks related to the technical solution and product safety,
- analyze hazards of the product,
- trace risks to system elements and requirements
- derive safety requirements from hazards in accordance with legal rules / laws,
- justify system measures and measures in the system environment for risk mitigation”

Languages = “SysML, UML, textual description”

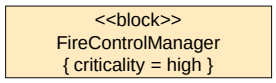
Content

Using UML/SysML for Risk & Safety Aspects

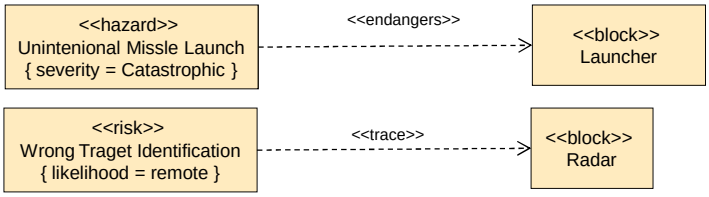
- Same examples of SysML capabilities to capture risk & safety aspects
  - Along the V-Model System development process



- SD-1.3 „Definition of Criticality and Quality Requirements "

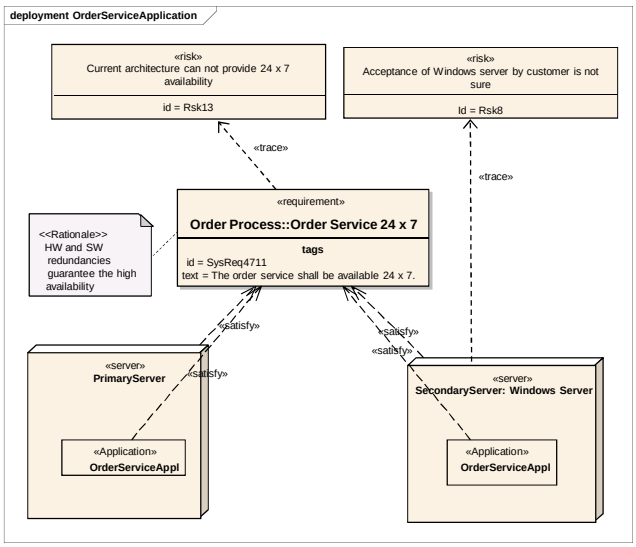


- SD-1.6 „Threat and Risk Analysis ": Consider safety, security and risk aspects

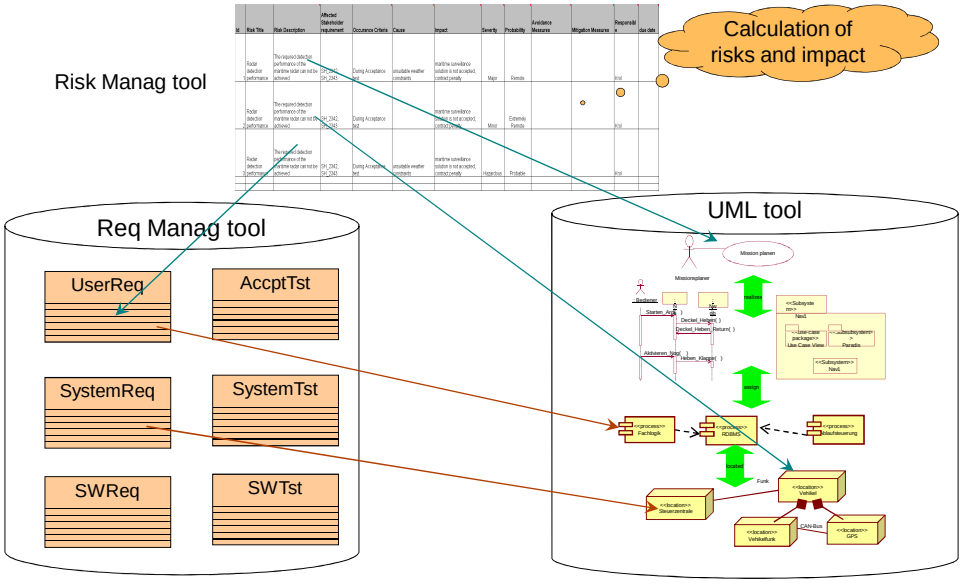


Using UML/SysML for Risk & Safety Aspects

- risk tracing to requirements and system elements is essential
- <<risk>> visualization of impact improves understanding
- Combining risk management with requirements and system engineering

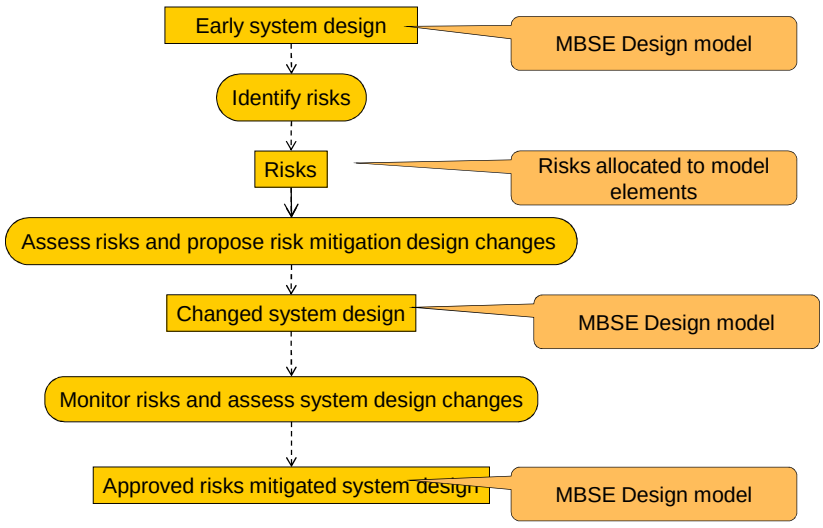


Risk Traceablity



Content

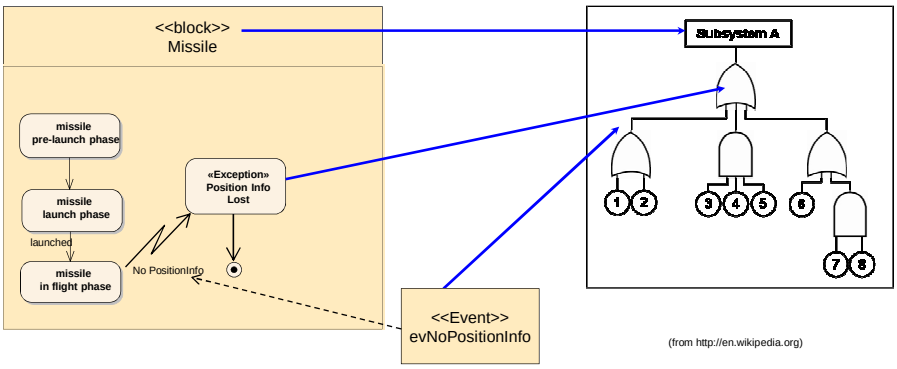
Ideal Technical Risk Management Practice



Fault Tree Analysis

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

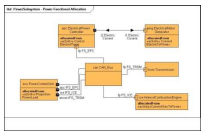
1. undesired effect is taken as root ('top event')
2. each situation that could cause that effect is added as series of logic expressions
3. trees are labeled with failure probabilities
4. calculate failure probabilities from fault trees

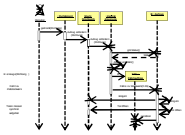


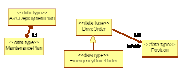
(from http://en.wikipedia.org)

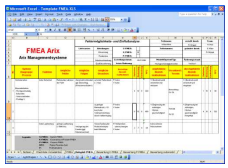
Failure Modes and Effects Analysis

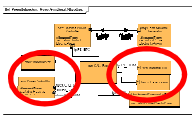
1. Identify system components/ structure
   - Exists in IBDs of DoDAF SV-1
2. Define functions of components
   - Exists as result of DoDAF SV-10c
3. Analysis failures
   a. Allocate possible failure to components
   b. Analyse failure impact based on data/material flows
      - DoDAF SV-10c + DoDAF 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









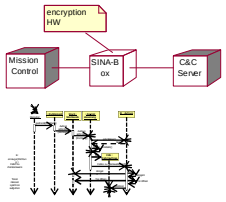


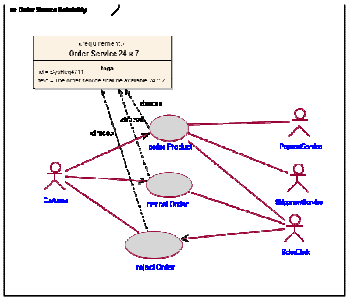
Reliability Availability Maintainability Sustainability (RAMS)

Identify system items failures/ out of order

➔ IBDs of physical architecture/ deployment diagrams

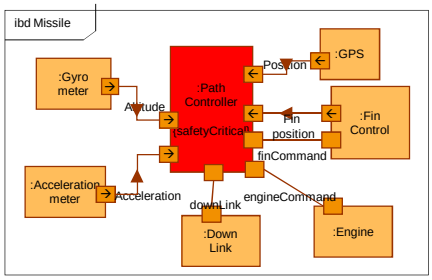
1. Identify local impact
   ➔ Collaboration of physical items
2. Identify site impact
3. Identify impact on overall system functionality
4. Check reliability/ availability requirements
5. Calculate RAMS based on
   - Mean Time Between Failure (MTBF)
   - Cycle replacement time
   - …

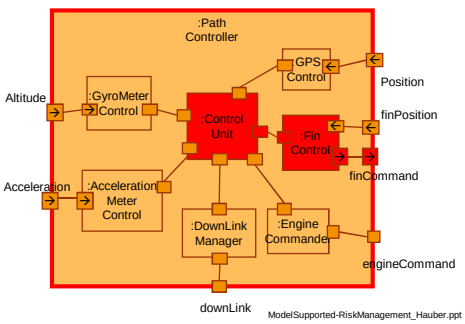




Safety Criticality Analysis

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

Summary

- MBSE SysML out of the box: No specific risks or safety & security view
- Enhancement of SysML by risk management profile
  - Viewpoint, stereotypes, properties, etc.
- Process: embedded in overall engineering process
- SysML can be used to capture and trace risk aspects
  - Main benefit: enhanced tracing from requirements and system architecture to risks
- SysML can be used in an MBSE approach for
  - Risk identification
  - Hazard analysis
  - Fault tree analysis
  - Failure mode and effects analysis (FMEA)
  - Criticality assessment
  - Risk assessment
- SysML Risks 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