

DNV IT Global Services
Safety Engineering / Management
in the automotive industry



Enhancing Trust and Confidence in IT

**Automotive SPIN Italia 4° Workshop on Automotive Software
Torino, 11.12.2009**

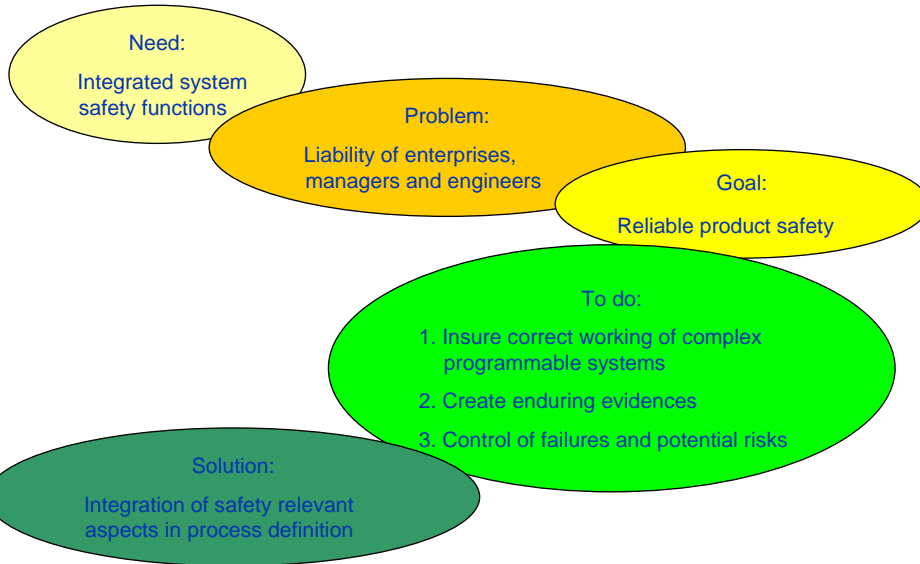
Dr. Klaus Hanke

Content

- Introduction
- **S**afety **M**anagement **C**enter
- Project experience



Introduction

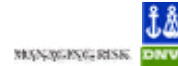


Version 1.0

19 January 2009

Slide 3

Performing safety projects



- DNV ITGS supports all potentially involved areas:
 - The **process definition** for all relevant working steps of a production
 - The **computation models** for evaluating safety, dependability and robustness
 - The implementation as well as its **evaluation**, and the compilation of **confirmations** for relevant requirements



Version 1.0

19 January 2009

Slide 4

Safety Management Centre (SMC)

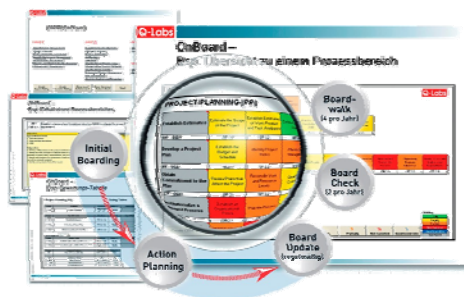


■ System/product safety assessment (system und process focus)

- Initial and repeatable status analysis using the DNV OnBoard™ – method
Analysis of the processes and the **compliance**
- Identification of strengths and weaknesses and the safety relevant room for improvement
- Documentation of risks using the DNV Easy-Risk-Manager – Tool

■ Safety process improvement (process focus)

- Definition and introduction of an aligned process model
- Supplementation of existing and definition of additional required processes and roles
- Execution of role specific training (**safety process manager**)
- Compilation of check lists, templates, utilities and methods



Version 1.0

19 January 2009

Slide 5

Safety Management Centre (SMC)



Version 1.0

19 January 2009

Slide 6

Safety Management Centre (SMC)



■ Safety risk analysis (system focus)

- Systematic identification and classification of risks concerning the system layer as well as software, electronics, mechanics and hydraulics (hazard analysis)
- Consideration and appraisal of causes and effects
- Definition of counter measures
- Compilation of reports and certificates

■ Safety engineering und management (system focus)

- Operational support starting with a **system safety programme**
- Compilation of functional safety concepts (FSK)
- Compilation of the safety documentation (safety management plan)
- System safety verification & validation including of the needed certificates
- Safety analysis of a system in relation to compliance with relevant safety standards, engineering standards, requirements and guidelines
- Knowledge transfer

Version 1.0

19 January 2009

Slide 7

Standards, methods and tools



■ Standards (deep knowledge)

- IEC 61508
„Functional safety of electrical/ electronic/programmable electronic safety-related systems“
- ISO WD 26262 “Automotive E/E safety engineering”
- VDA 4 “Securing the quality before serial production – securing the quality during product implementation methods and operation“
- VDI 2220, VDI 2221, VDI 2222-2, VDI 2206, VDI 2803 - VDI Papers
- +SAFE - a Safety Extension of CMMI-DEV, V 1.2

■ Methods and Tools (experience)

- FMEA – analysis of the possibility of errors and of effects
- FTA – Fault tree analysis
- HAZOP - Hazard and Operability method
- ETA – Event tree analysis
- Markov Analysis
- Matlab Simulink – from the company: „The MathWorks“
- SysML - Systems modelling language
- UML 2.0 - Unified modelling language
- SDL - Systems modelling language
- VHDL - Very High Speed Integrated Circuit Hardware Description Language

Version 1.0

19 January 2009

Slide 8

■ active safety systems

- Risk assessment, Safety Concept and System Safety Requirements
 - Hazard analysis and hazard classification (ISO WD 26262 and IEC 61508)
 - Safety Goals and Functional Safety Concept
 - Safety Requirement Specification
 - System Safety Program Plan
 - Preliminary Hazard List and Analysis including risk assessment
 - System Safety Requirements Specification
- Safety Design Constraints
 - Support System Design Definition
 - Cascade Safety Requirements to Sub-Systems and Components
 - Safety design constraints
 - System architectural design

■ active safety systems cont.

- System Safety Validation and Verification Plan
 - Define Safety Verification and Validation
- System Safety Documentation Support
 - Safety Plan
 - Preliminary Hazard Analysis Report
 - Functional Safety Concept
 - Safety Requirement Specification
 - Open Issue List/Hazard Log
- System Safety Management and Administration
 - Tracking and solving of open safety requirement (whole development lifecycle)
 - Initiate, organize and host Safety Working Group Meetings

Feature Interaction



- Feature Interaction are side effects, which are caused by parallelism of system features
- Usually several steering features access to one actuating element
- Using a unrestricted parallelism
 - A steering control of a feature may not be anymore possible (problem: security)
 - A steering control of some feature may disturb each other which is perceived by the driver as malfunction or drop out (problem: reliability)
- The feature interaction must be descript and analysed in a way, that enables you reducing risks in security and reliability

Main idea for a solution



- Discrete and continuous effect interrelations are represented by BDD (block diagram) using SysML. For parallel and concurring actions the semantic of SDL (specification and description language) may be used
- Quantitative effect interrelations are represented by variables and equations (imported into Simulink)
- Feature interaction can be resolved by using IDEF-0 (integrated definition method) level architecture:
 - in the control level a **feature scheduler** and a **state monitor** are required
 - in the mechanism level a **delimiter** will guarantee admissibility of values
- The level architectures can be represented by a combination of hierarchy- and block diagrams (BDD, IBD)

www.dnv.com/ITGS

Contact DNV IT GS Germany

Dr. Klaus Hanke +49 173 66 888 01

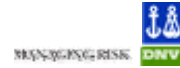
Backup slides

Feature Interaction



Adobe Acrobat
Document

Feature Interaction



- Overall system as an informal control cycle
- Aggregation hierarchy (bdd)
- Effect graphic (ibd)
- Variables and equations (par)
- Functional flow in the activity chart (act)
- Level model IDEF-0
- Resolution of the feature interaction by level architecture