2022 MathWorks
中国汽车年会

系统化的ASPICE、功能安全和信息安全实施方法

程晖, 开发部部长 · KOSTAL

MathWorks®

目录

CONTENTS

01 公司简介

02 标准分析与读解

03 体系化的开发流程

04 统一的产品架构

05 一体化的实施工具和方法

1

公司简介

科世达–家族经营，四代传承

KOSTAL

1912 – 第一代

Leopold Kostal

“电器化”

恰如其分

“可持续性和节约资源是我们的第二天性。”

“可持续理念连结人类和自然–––天人合一。”

同舟共济

“电控化”

Kurt Kostal

1935 – 第二代

1972 – 第三代

Helmut Kostal

“全球化”

倾情而为

“作为一个组织，我们能为自然和谐采取可持续和有效的措施。 ”

“作为一个百年诞辰的公司，足以证明我们能够长期持续发展。”

共塑未来

“生态化”

Andreas Kostal

2008 – 第四代

产品组合-智能能源&人机交互

智能能源

驱动出行

功率电子类产品

车载充电机

DC/DC–转换器

充电控制单元

舒适电子类产品

门、座椅、尾门模块

车身域控制器

无钥匙进入系统

人机交互

感知生活

驾驶控制类产品

转向柱模块

线控排挡

天窗模块

舒适控制类产品

驾驶辅助系统

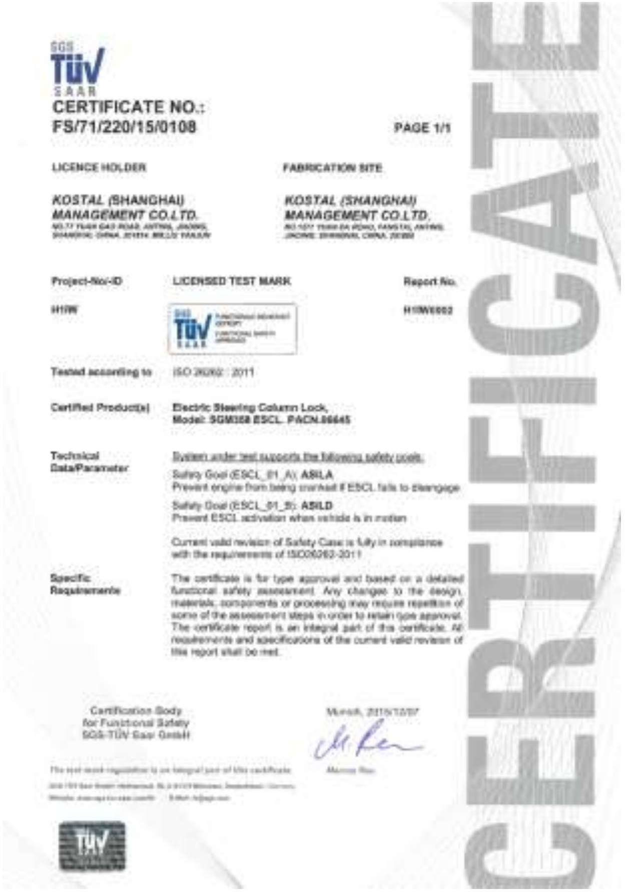
显示类、智能表面

功能安全经验

KOSTAL 有着丰富的功能安全经验，ASILA-ASILD.
科世达集团开发过超过150个有功能安全要求的产品.
从IEC开始，KOSTAL有着超过15年的功能安全设计经验.

Door sw. / Module

Roof Module



CERTIFICATE NO.:
FS/71/220/15/0108

PAGE 1/1

LICENCE HOLDER	FABRICATION SITE
KOSTAL (SHANGHAI) MANAGEMENT CO.LTD.	KOSTAL (SHANGHAI) MANAGEMENT CO.LTD.

Project-No/-ID	LICENSED TEST MARK	Report No.
H1IW		H1IW6002

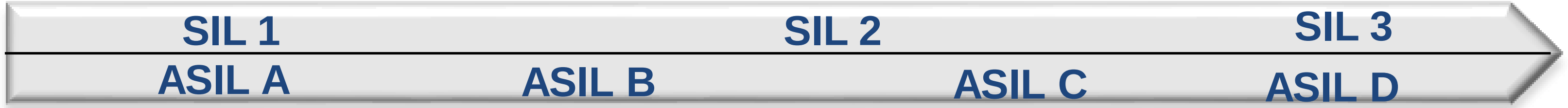
Tested according to	ISO 26262 : 2011
Certified Product(s)	Electric Steering Column Lock, Model: SGM358 ESCL PACN.86645
Technical Data/Parameter	System under test supports the following safety goals: Safety Goal (ESCL_01_A): **ASILA** Prevent engine from being cranked if ESCL fails to disengage Safety Goal (ESCL_01_B): **ASILD** Prevent ESCL activation when vehicle is in motion Current valid revision of Safety Case is fully in compliance with the requirements of ISO26262-2011
Specific Requirements	The certificate is for type approval and based on a detailed functional safety assessment. Any changes to the design, materials, components or processing may require repetition of some of the assessment steps in order to retain type approval. The certificate report is an integral part of this certificate. All requirements and specifications of the current valid revision of this report shall be met.

Certification Body
for Functional Safety
SGS-TÜV Saar GmbH

Munich, 2015/12/07

Marcus Rau

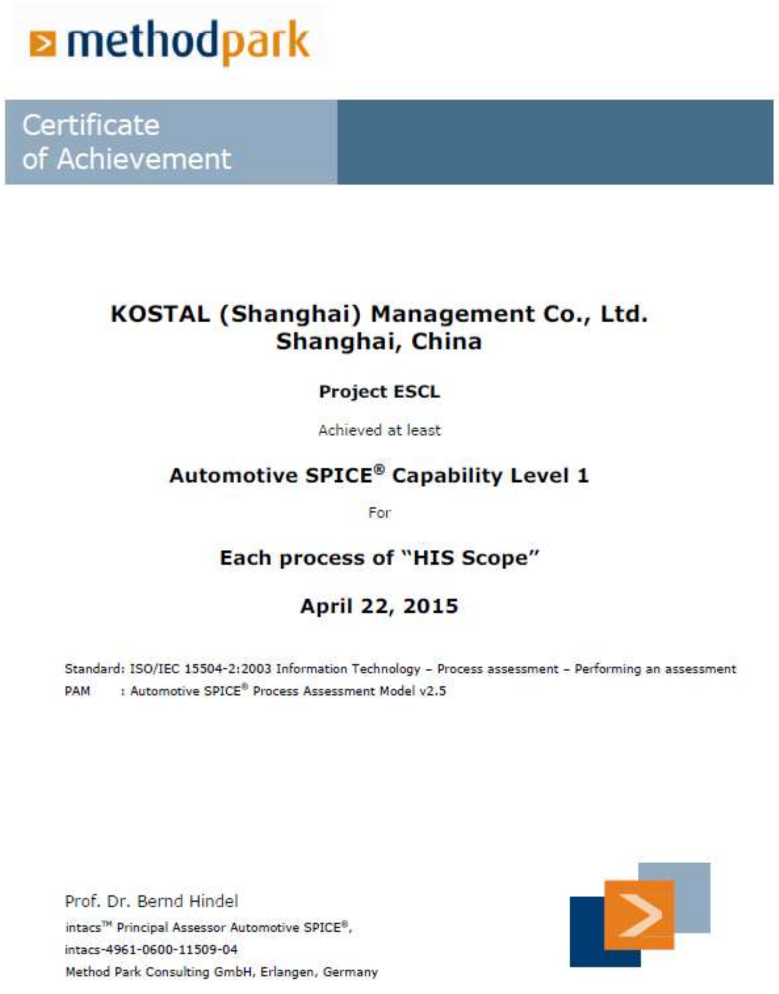
The test mark regulation is an integral part of this certificate



SIL 1 | SIL 2 | SIL 3

ASIL A | ASIL B | ASIL C | ASIL D

ASPICE经验



methodpark

Certificate of Achievement

KOSTAL (Shanghai) Management Co., Ltd.
Shanghai, China

Project ESCL

Achieved at least

Automotive SPICE® Capability Level 1

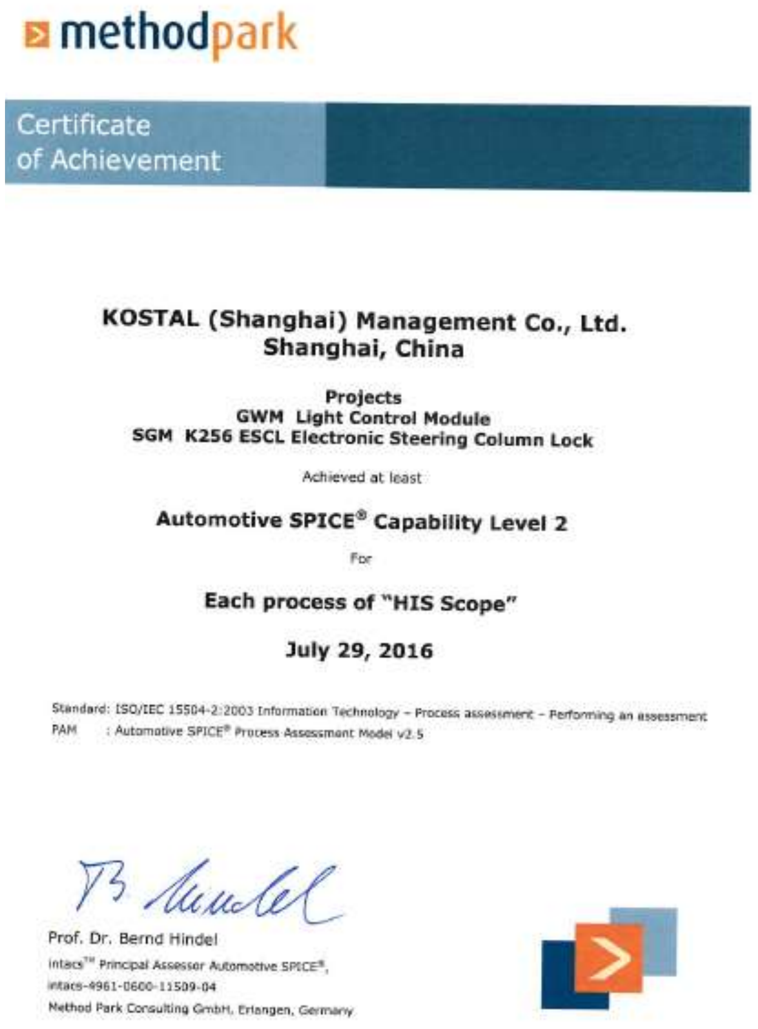
For

Each process of "HIS Scope"

April 22, 2015

Standard: ISO/IEC 15504-2:2003 Information Technology – Process assessment – Performing an assessment
PAM : Automotive SPICE® Process Assessment Model v2.5

Prof. Dr. Bernd Hindel
intacs™ Principal Assessor Automotive SPICE®,
intacs-4961-0600-11509-04
Method Park Consulting GmbH, Erlangen, Germany



methodpark

Certificate of Achievement

KOSTAL (Shanghai) Management Co., Ltd.
Shanghai, China

Projects
GWM Light Control Module
SGM K256 ESCL Electronic Steering Column Lock

Achieved at least

Automotive SPICE® Capability Level 2

For

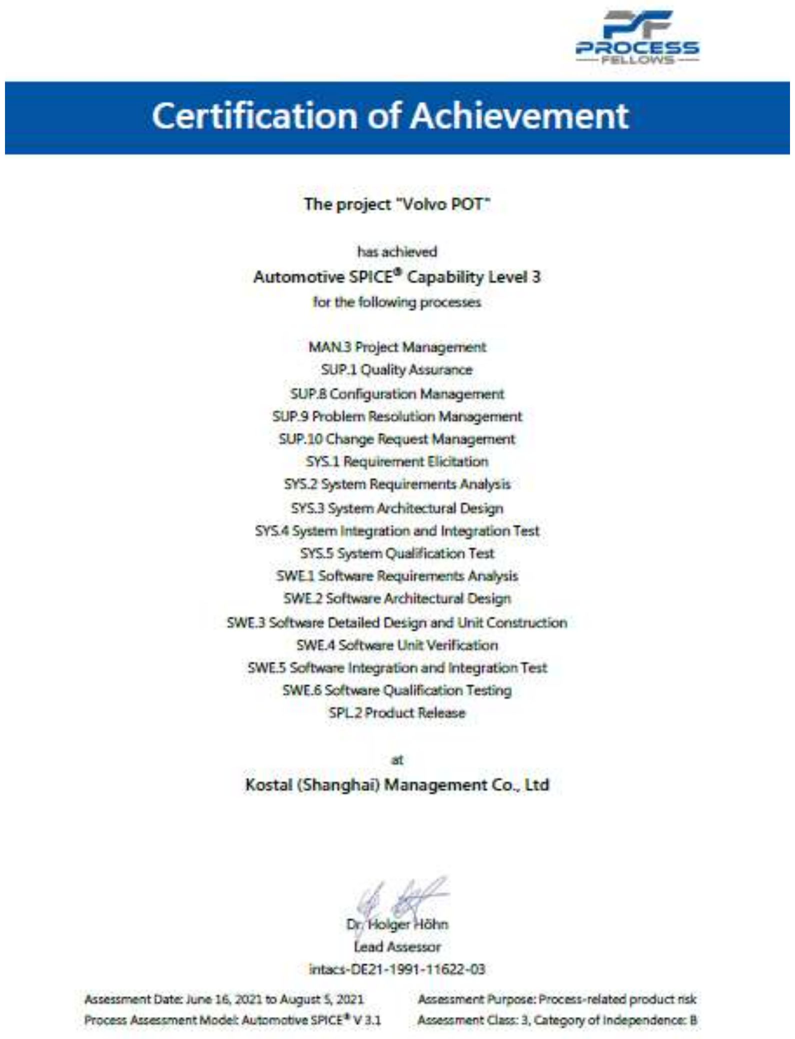
Each process of "HIS Scope"

July 29, 2016

Standard: ISO/IEC 15504-2:2003 Information Technology – Process assessment – Performing an assessment
PAM : Automotive SPICE® Process Assessment Model v2.5

B Hindel

Prof. Dr. Bernd Hindel
intacs™ Principal Assessor Automotive SPICE®,
intacs-4961-0600-11509-04
Method Park Consulting GmbH, Erlangen, Germany



PROCESS FELLOWS

Certification of Achievement

The project "Volvo POT"

has achieved

Automotive SPICE® Capability Level 3

for the following processes

MAN.3 Project Management
SUP.1 Quality Assurance
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
SYS.1 Requirement Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
SYS.5 System Qualification Test
SWE.1 Software Requirements Analysis
SWE.2 Software Architectural Design
SWE.3 Software Detailed Design and Unit Construction
SWE.4 Software Unit Verification
SWE.5 Software Integration and Integration Test
SWE.6 Software Qualification Testing
SPL.2 Product Release

at

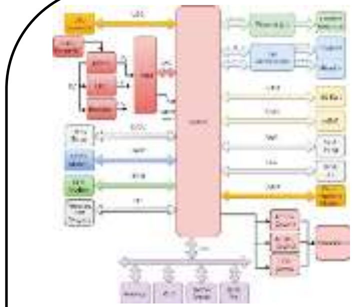
Kostal (Shanghai) Management Co., Ltd

Dr. Holger Höhn
Lead Assessor
intacs-DE21-1991-11622-03

Assessment Date: June 16, 2021 to August 5, 2021
Process Assessment Model: Automotive SPICE® V 3.1

Assessment Purpose: Process-related product risk
Assessment Class: 3, Category of Independence: B

AE4 Responsibility

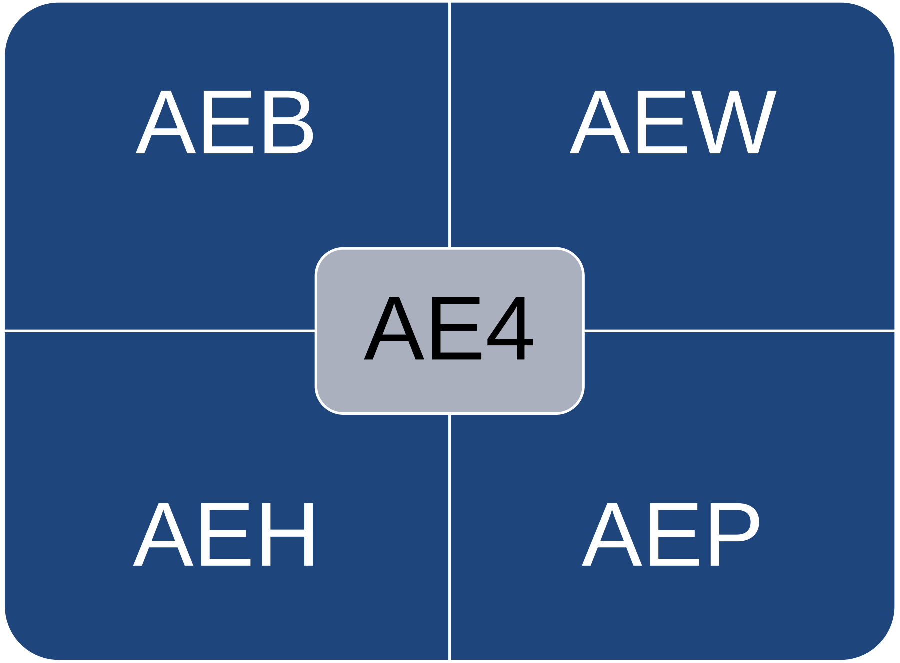


Hardware Design

PCB Layout

EMC TEST

Build Block Worst Case



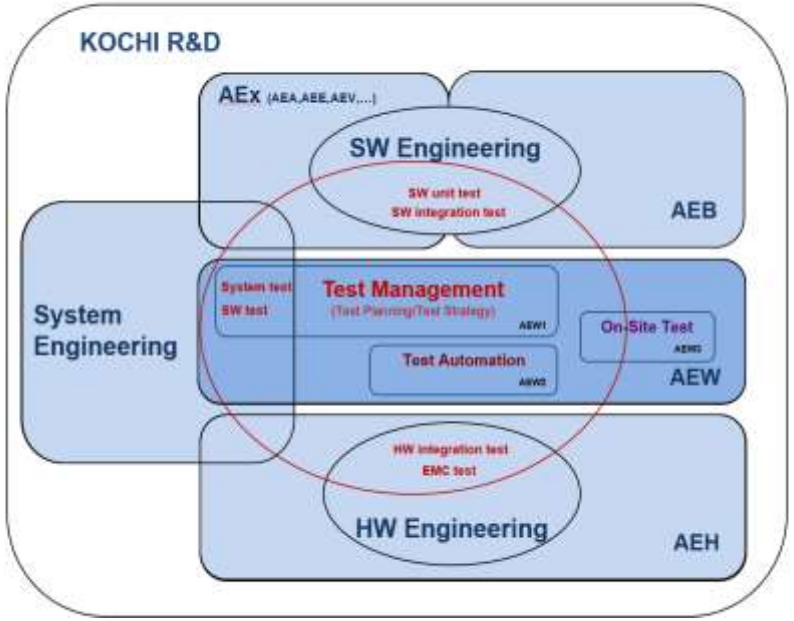
AEB

AEW

AE4

AEH

AEP



KOCHI R&D

1 Analysis & Planning
2 Design & Development
3 Quality Assurance
4 Implementation & Deployment
5 Maintenance & Support
Development Process

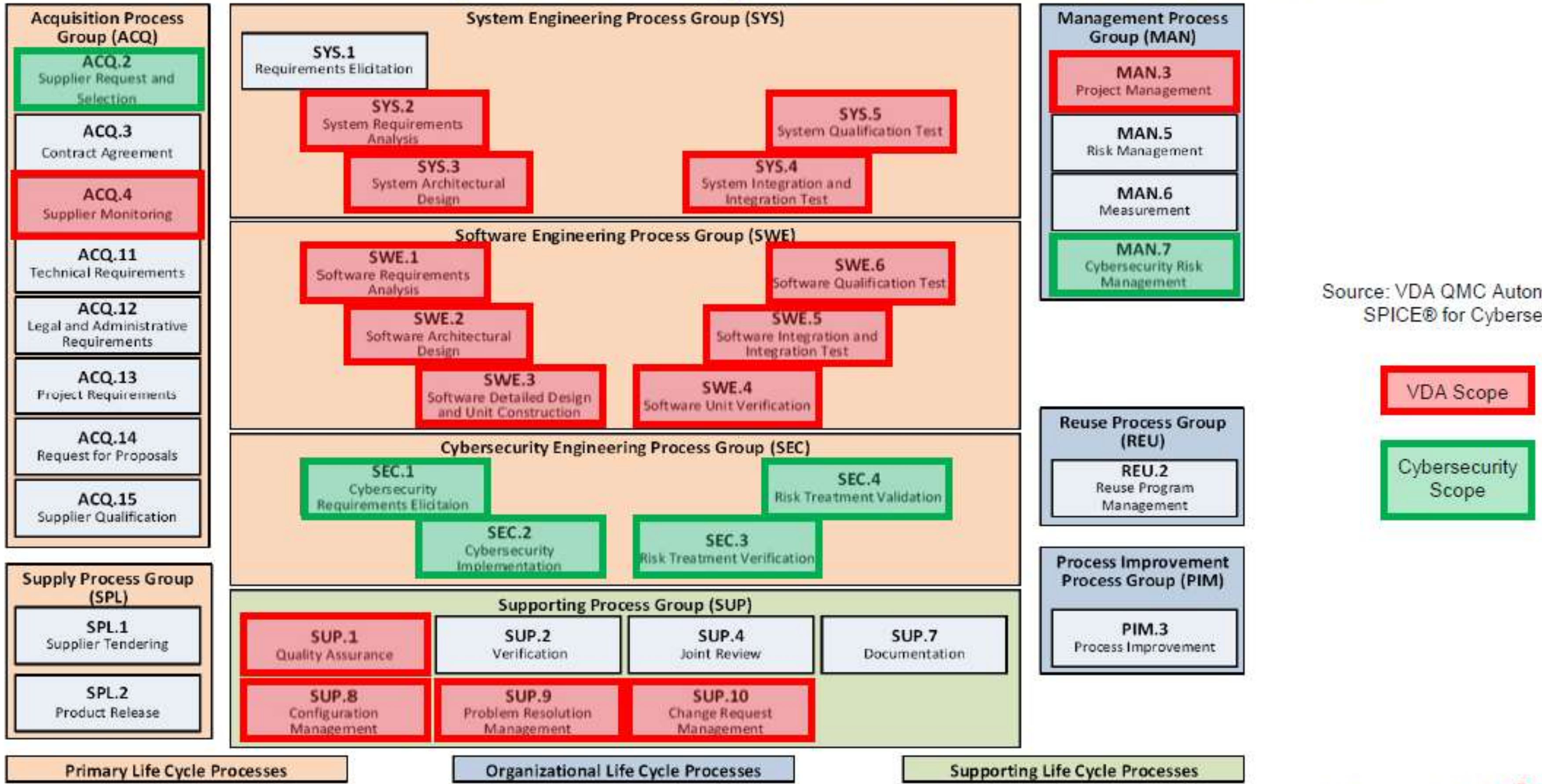
System Engineering

- Functional Safety
- Cyber Security
- FMEA
- System Architecture
- Simulation and Optical

2

标准分析与读解

Integrated Automotive SPICE® 3.1 and Automotive SPICE® for Cybersecurity Process Reference Model



Acquisition Process Group (ACQ)
- ACQ.2 Supplier Request and Selection
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

Supply Process Group (SPL)
- SPL.1 Supplier Tendering
- SPL.2 Product Release

System Engineering Process Group (SYS)
- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Software Engineering Process Group (SWE)
- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Cybersecurity Engineering Process Group (SEC)
- SEC.1 Cybersecurity Requirements Elicitaion
- SEC.2 Cybersecurity Implementation
- SEC.3 Risk Treatment Verification
- SEC.4 Risk Treatment Validation

Supporting Process Group (SUP)
- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.4 Joint Review
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management

Management Process Group (MAN)
- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement
- MAN.7 Cybersecurity Risk Management

Reuse Process Group (REU)
- REU.2 Reuse Program Management

Process Improvement Process Group (PIM)
- PIM.3 Process Improvement

Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

Source: VDA QMC Automotive SPICE® for Cybersecurity

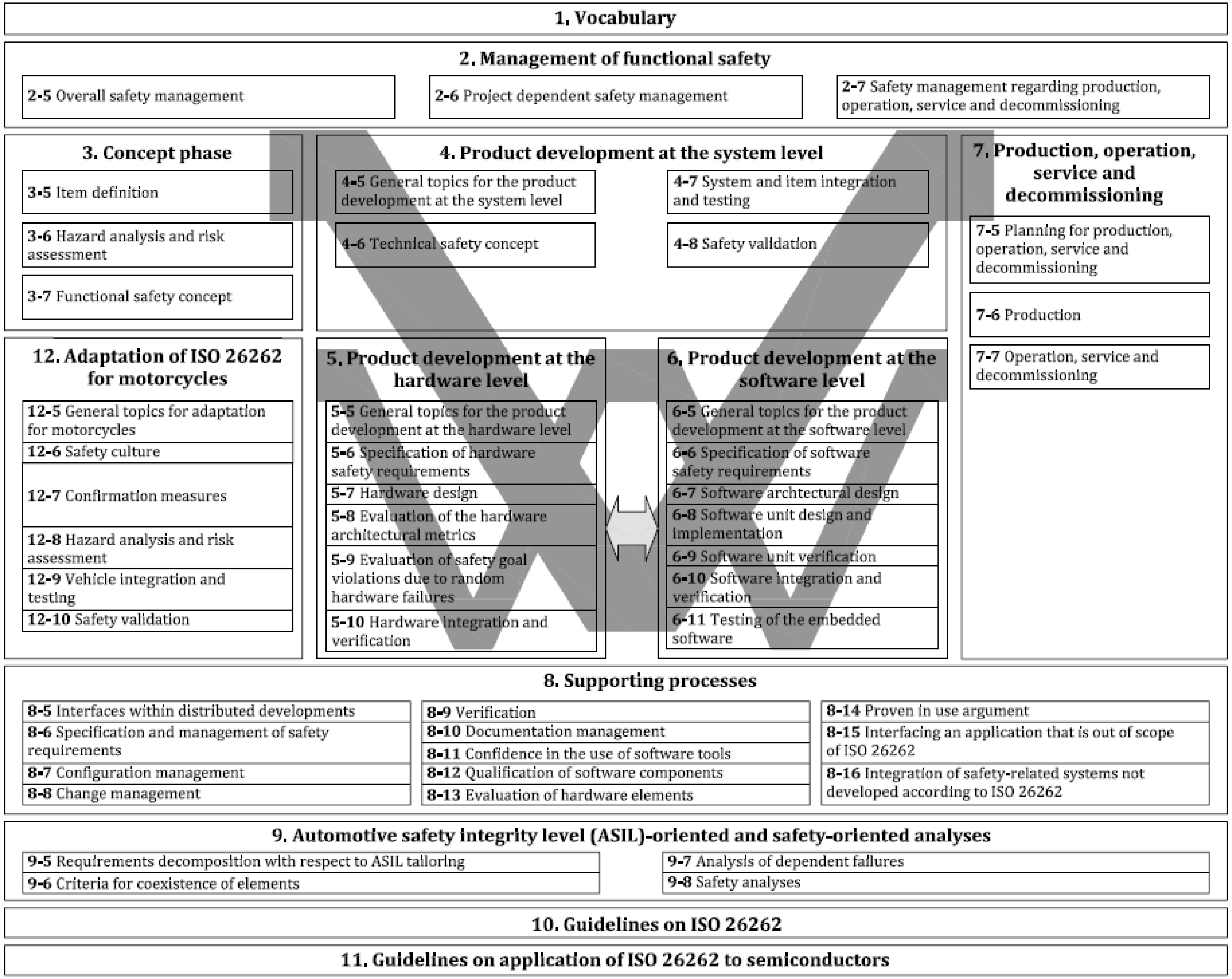
🟥 VDA Scope

🟩 Cybersecurity Scope

9 intacs™ - News for the assessor training scheme

intacs.info
International Assessor Certification Scheme™

ASPiCE、功能安全和信息安全



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Project dependent safety management

2-7 Safety management regarding production, operation, service and decommissioning

3. Concept phase

3-5 Item definition

3-6 Hazard analysis and risk assessment

3-7 Functional safety concept

4. Product development at the system level

4-5 General topics for the product development at the system level

4-6 Technical safety concept

4-7 System and item integration and testing

4-8 Safety validation

7. Production, operation, service and decommissioning

7-5 Planning for production, operation, service and decommissioning

7-6 Production

7-7 Operation, service and decommissioning

12. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

12-8 Hazard analysis and risk assessment

12-9 Vehicle integration and testing

12-10 Safety validation

5. Product development at the hardware level

5-5 General topics for the product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Evaluation of the hardware architectural metrics

5-9 Evaluation of safety goal violations due to random hardware failures

5-10 Hardware integration and verification

6. Product development at the software level

6-5 General topics for the product development at the software level

6-6 Specification of software safety requirements

6-7 Software archtectural design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing of the embedded software

8. Supporting processes

8-5 Interfaces within distributed developments

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

8-9 Verification

8-10 Documentation management

8-11 Confidence in the use of software tools

8-12 Qualification of software components

8-13 Evaluation of hardware elements

8-14 Proven in use argument

8-15 Interfacing an application that is out of scope of ISO 26262

8-16 Integration of safety-related systems not developed according to ISO 26262

9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

9-7 Analysis of dependent failures

9-8 Safety analyses

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Management Process:

2

Development Process:

System:

4-5,4-7同ASPiCE

4-6, 4-8为特殊需求, 过程管控同ASPiCE

Hardware:

5-5, 5-7, 5-8, 5-10同ASPiCE

5-6,5-9为特殊需求, 过程管控同ASPiCE

Software:

6-5, 6-7, 6-8, 6-9, 6-10, 6-11同ASPiCE

6-6为特殊需求, 过程管控同ASPiCE

Supporting:

8-5, 8-6, 8-7,8-8, 8-9,8-10基本同ASPiCE

8-11, 8-12, 8-13,8-14, 8-15,8-16作为平台化建设来处理, 不单独针对项目。

9-5,9-6,9-7,9-8过程管控同ASPiCE

Technical Design:

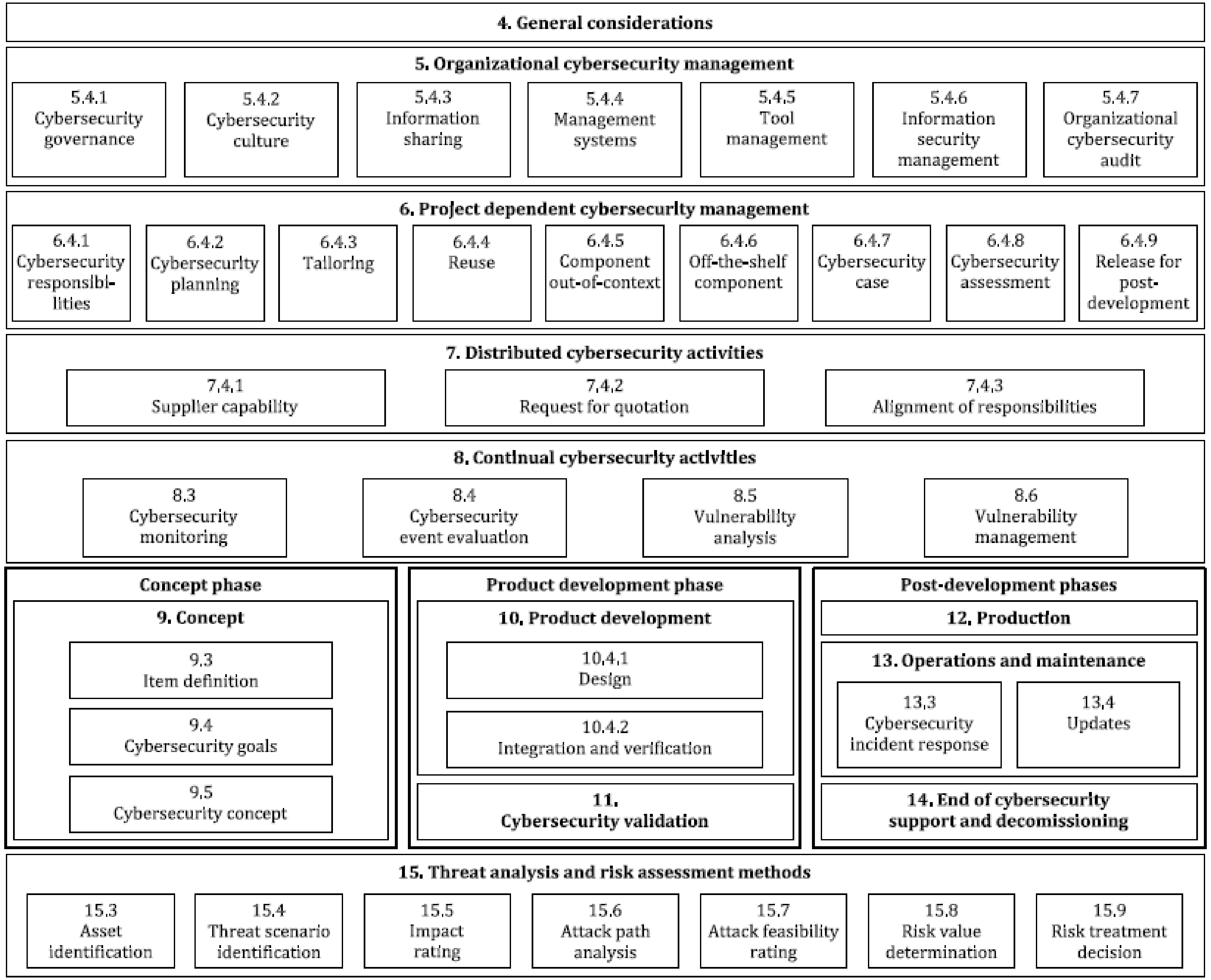
3章, 4-6,4-8,5-6,5-9,6-6,9章的作为产品设计的要求融入架构设计

系统架构

硬件架构

软件架构

ASPiCE、功能安全和信息安全



4. General considerations

5. Organizational cybersecurity management

- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Information sharing
- 5.4.4 Management systems
- 5.4.5 Tool management
- 5.4.6 Information security management
- 5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

- 6.4.1 Cybersecurity responsibilities
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring
- 6.4.4 Reuse
- 6.4.5 Component out-of-context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

7. Distributed cybersecurity activities

- 7.4.1 Supplier capability
- 7.4.2 Request for quotation
- 7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

- 8.3 Cybersecurity monitoring
- 8.4 Cybersecurity event evaluation
- 8.5 Vulnerability analysis
- 8.6 Vulnerability management

Concept phase

9. Concept

- 9.3 Item definition
- 9.4 Cybersecurity goals
- 9.5 Cybersecurity concept

Product development phase

10. Product development

- 10.4.1 Design
- 10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

- 13.3 Cybersecurity incident response
- 13.4 Updates

14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods

- 15.3 Asset identification
- 15.4 Threat scenario identification
- 15.5 Impact rating
- 15.6 Attack path analysis
- 15.7 Attack feasibility rating
- 15.8 Risk value determination
- 15.9 Risk treatment decision

Organization and ISMS/CSMS

5,7,8(IT&RD),12

Management Process:

6

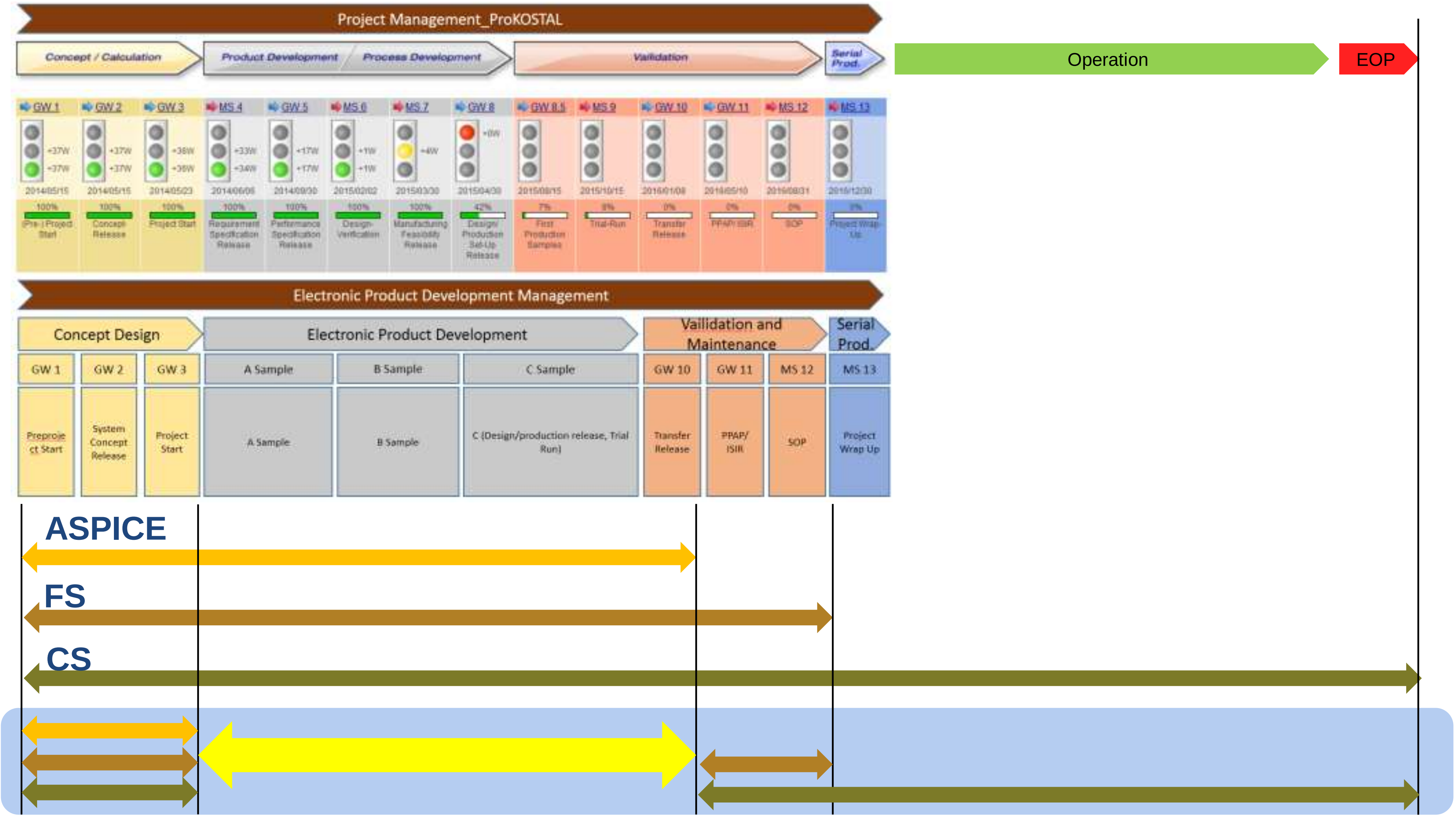
Development Process:

9,10,12

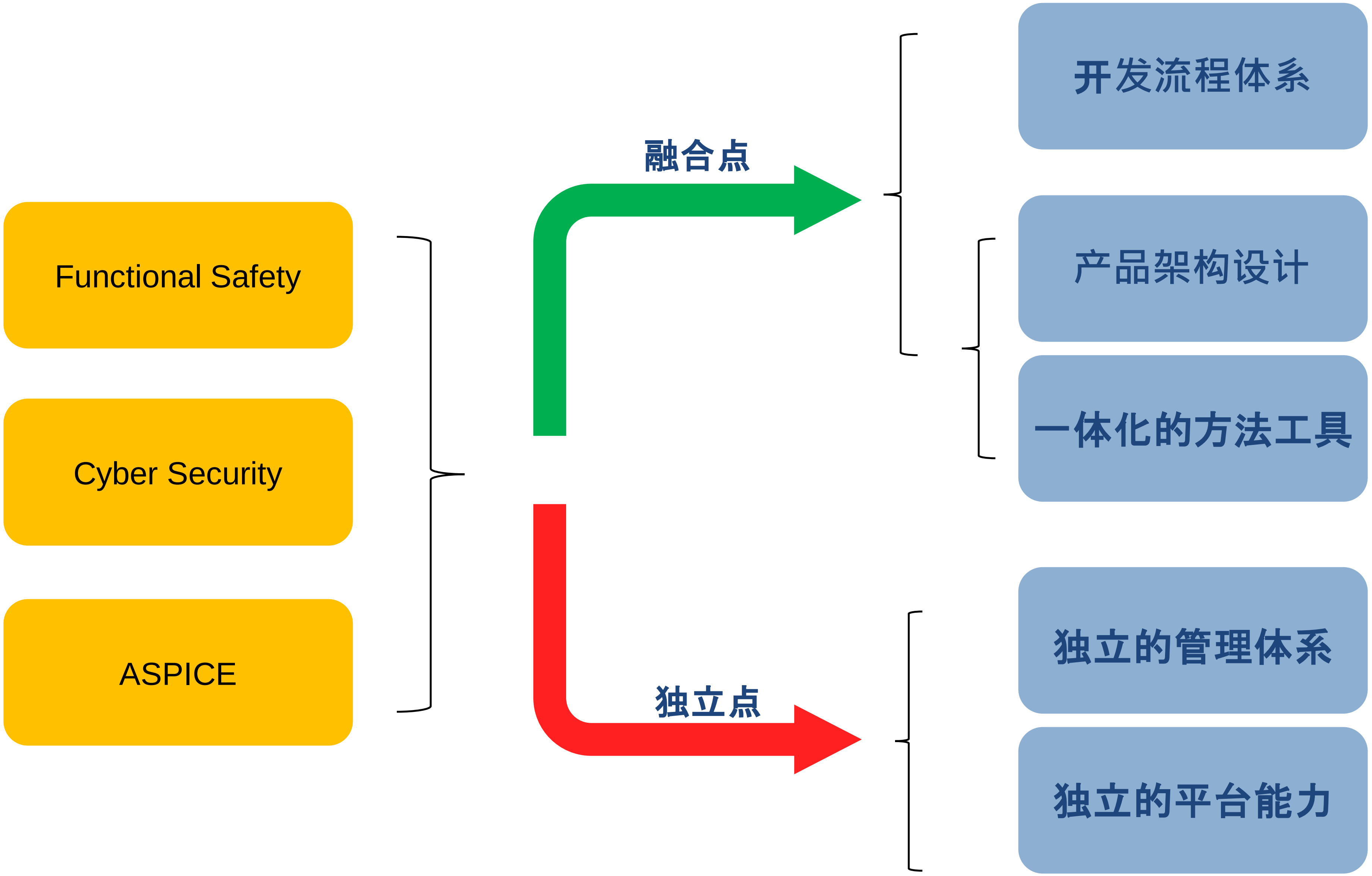
Technical Design:

9,10,15

融合点 ： 流程--项目全过程和产品生命周期



功能安全、信息安全和ASPiCE融合点



Functional Safety

Cyber Security

ASPICE

融合点

独立点

开发流程体系

产品架构设计

一体化的方法工具

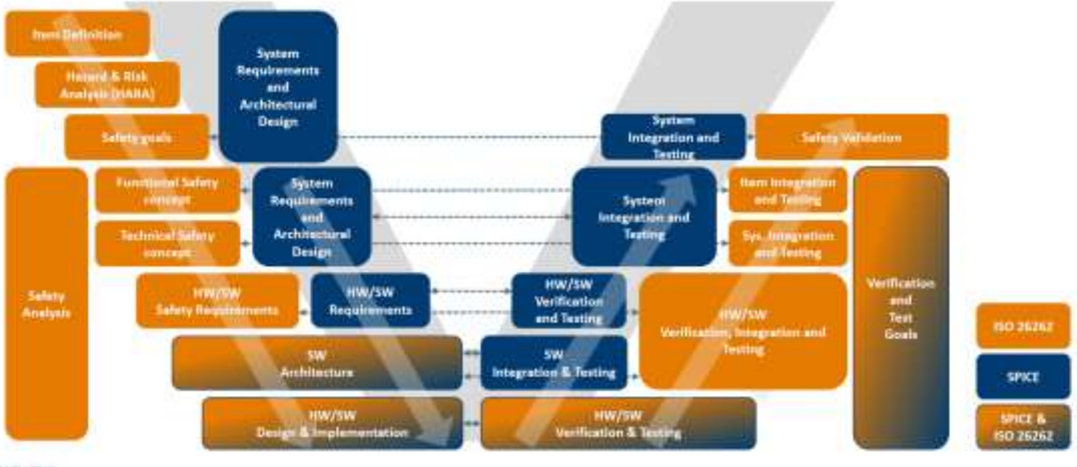
独立的管理体系

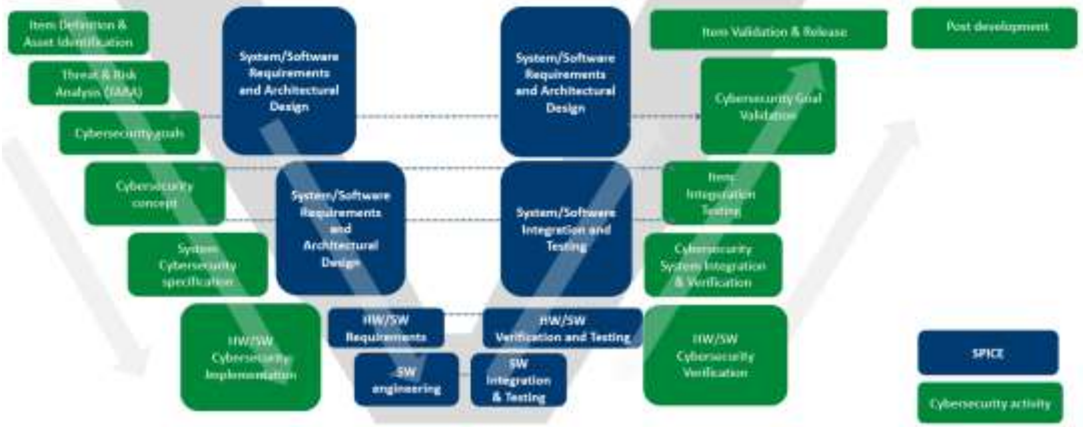
独立的平台能力

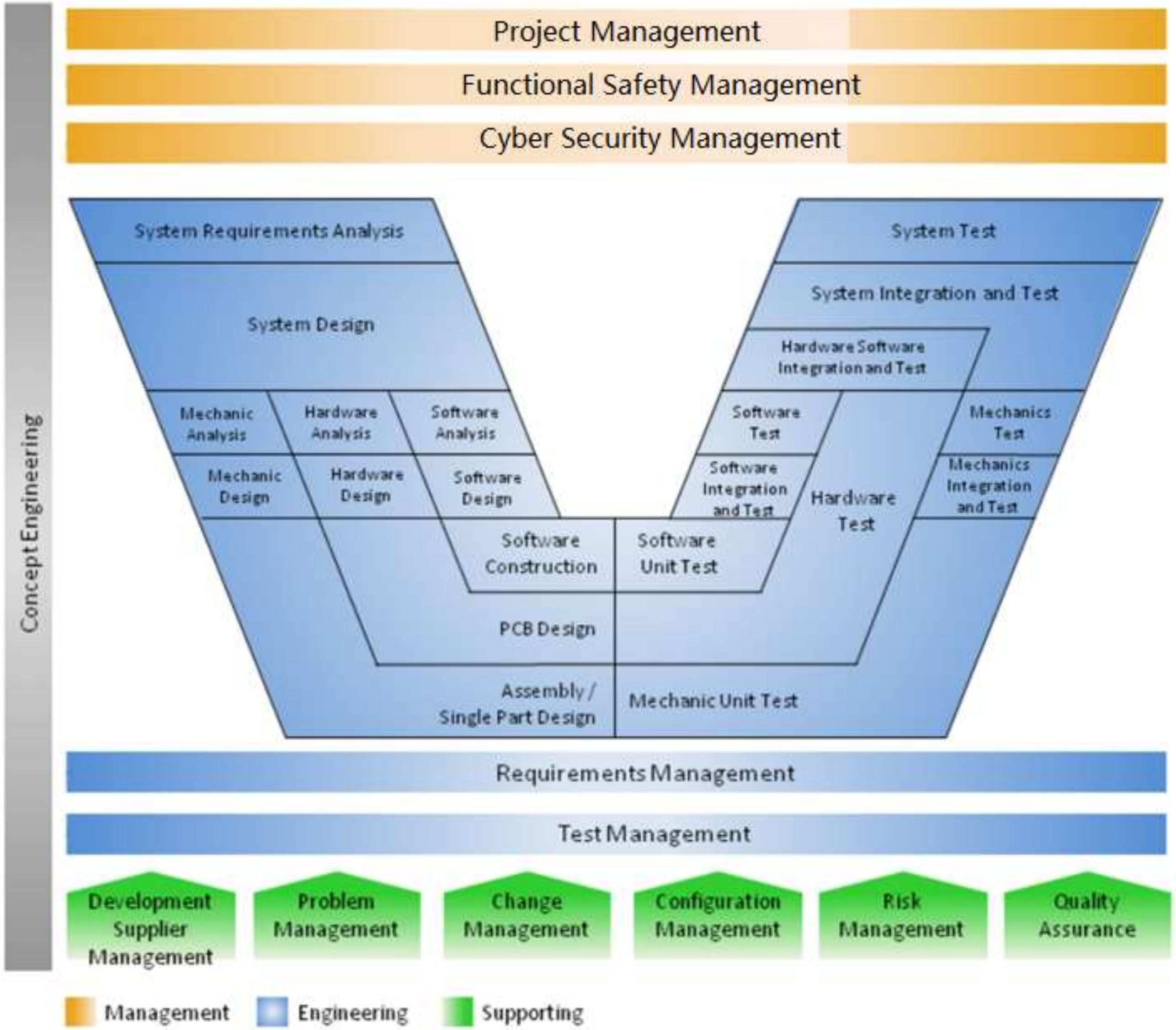
3

体系化的开发流程

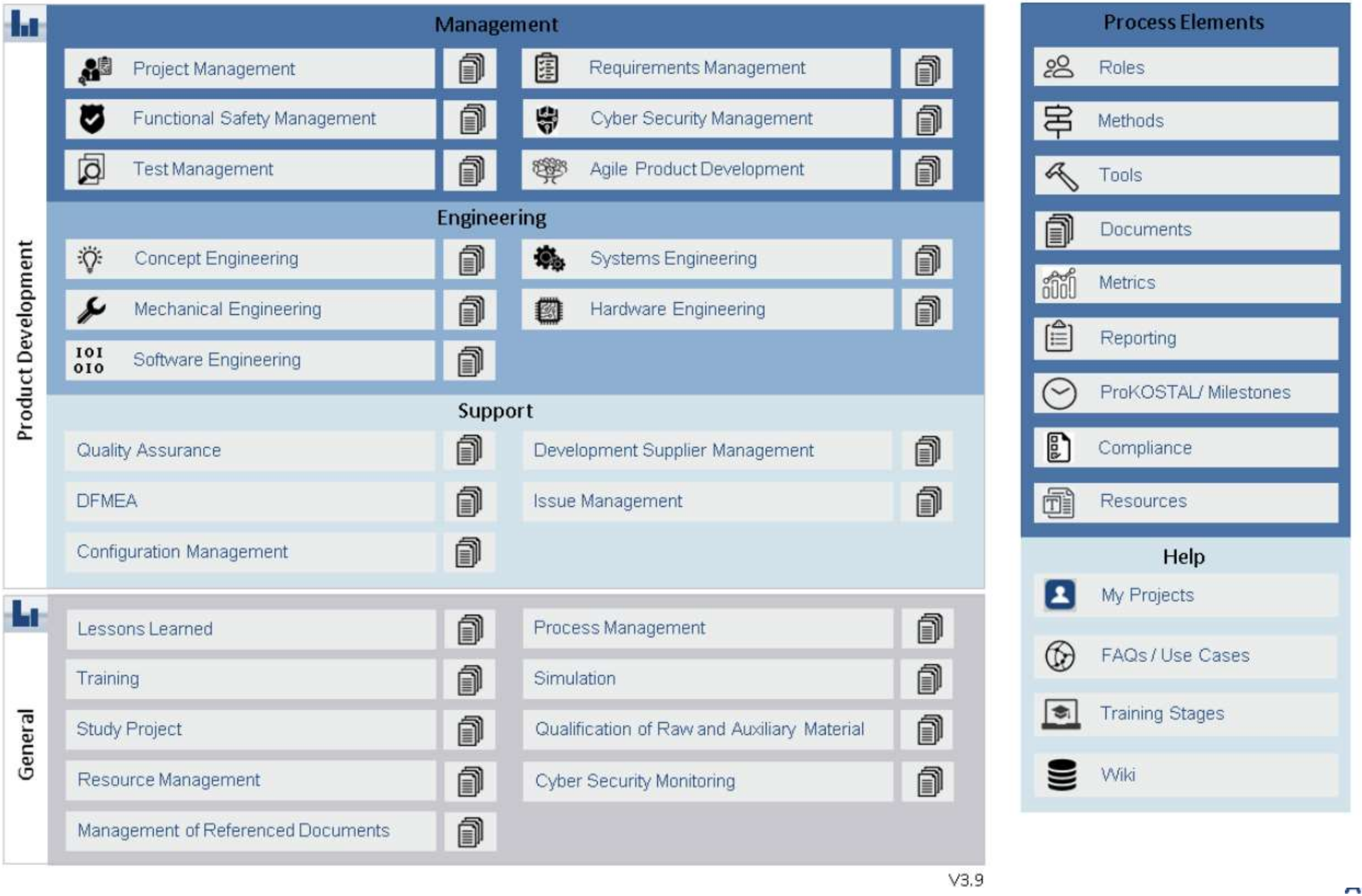
融合点 ： 流程– 最终效果


Item Definition
Hazard & Risk Analysis (HARA)
Safety goals
System Requirements and Architectural Design
System Integration and Testing
Safety Validation
Safety Analysis
Functional Safety concept
Technical Safety concept
System Requirements and Architectural Design
System Integration and Testing
Item Integration and Testing
Sys. Integration and Testing
Verification and Test Goals
HW/SW Safety Requirements
HW/SW Requirements
HW/SW Verification and Testing
HW/SW Verification, Integration and Testing
SW Architecture
SW Integration & Testing
HW/SW Design & Implementation
HW/SW Verification & Testing
ISO 26262
SPICE
SPICE & ISO 26262


Item Definition & Asset Identification
Threat & Risk Analysis (TARA)
Cybersecurity goals
System/Software Requirements and Architectural Design
System/Software Requirements and Architectural Design
Item Validation & Release
Post development
Cybersecurity Goal Validation
Cybersecurity concept
System Cybersecurity specification
System/Software Requirements and Architectural Design
System/Software Integration and Testing
Item Integration Testing
Cybersecurity System Integration & Verification
HW/SW Cybersecurity Implementation
HW/SW Requirements
SW engineering
HW/SW Verification and Testing
SW Integration & Testing
HW/SW Cybersecurity Verification
SPICE
Cybersecurity activity


Project Management
Functional Safety Management
Cyber Security Management
Concept Engineering
System Requirements Analysis
System Design
Mechanic Analysis
Hardware Analysis
Software Analysis
Mechanic Design
Hardware Design
Software Design
Software Construction
PCB Design
Assembly / Single Part Design
System Test
System Integration and Test
Hardware Software Integration and Test
Software Test
Mechanics Test
Software Integration and Test
Hardware Test
Mechanics Integration and Test
Software Unit Test
Mechanic Unit Test
Requirements Management
Test Management
Development Supplier Management
Problem Management
Change Management
Configuration Management
Risk Management
Quality Assurance
Management
Engineering
Supporting

融合点 ： 流程--体系



Product Development

Management

- Project Management
- Requirements Management
- Functional Safety Management
- Cyber Security Management
- Test Management
- Agile Product Development

Engineering

- Concept Engineering
- Systems Engineering
- Mechanical Engineering
- Hardware Engineering
- Software Engineering

Support

- Quality Assurance
- Development Supplier Management
- DFMEA
- Issue Management
- Configuration Management

General

- Lessons Learned
- Process Management
- Training
- Simulation
- Study Project
- Qualification of Raw and Auxiliary Material
- Resource Management
- Cyber Security Monitoring
- Management of Referenced Documents

Process Elements

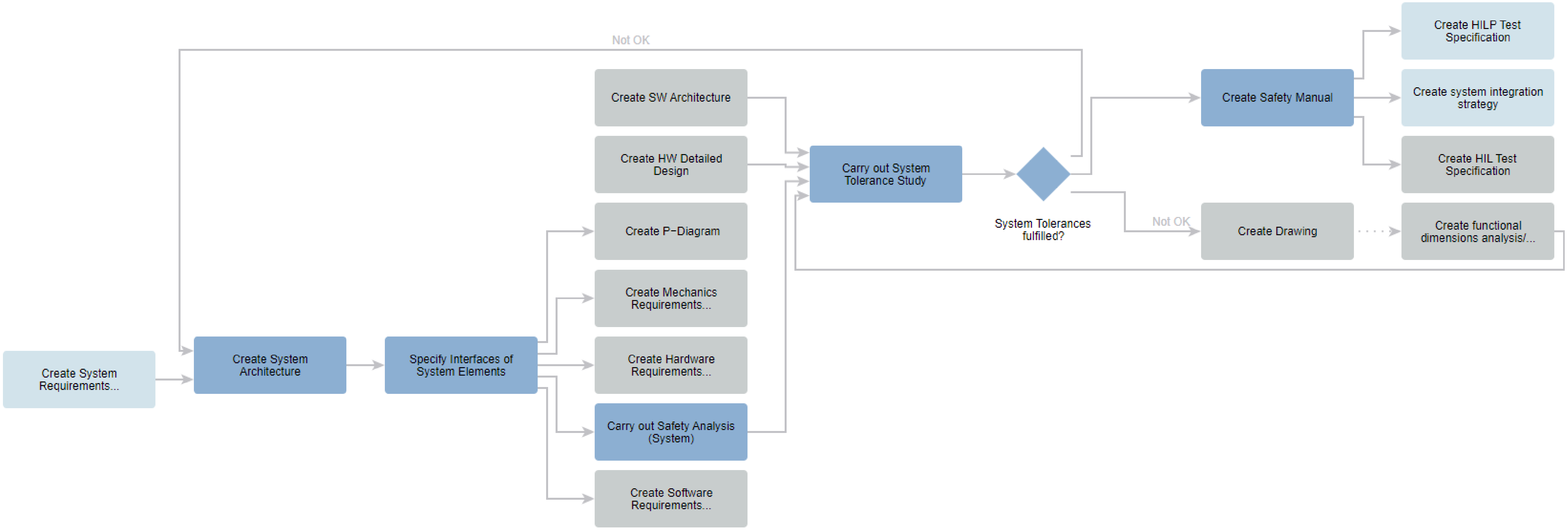
- Roles
- Methods
- Tools
- Documents
- Metrics
- Reporting
- ProKOSTAL/ Milestones
- Compliance
- Resources

Help

- My Projects
- FAQs / Use Cases
- Training Stages
- Wiki

V3.9

融合点 ： 流程

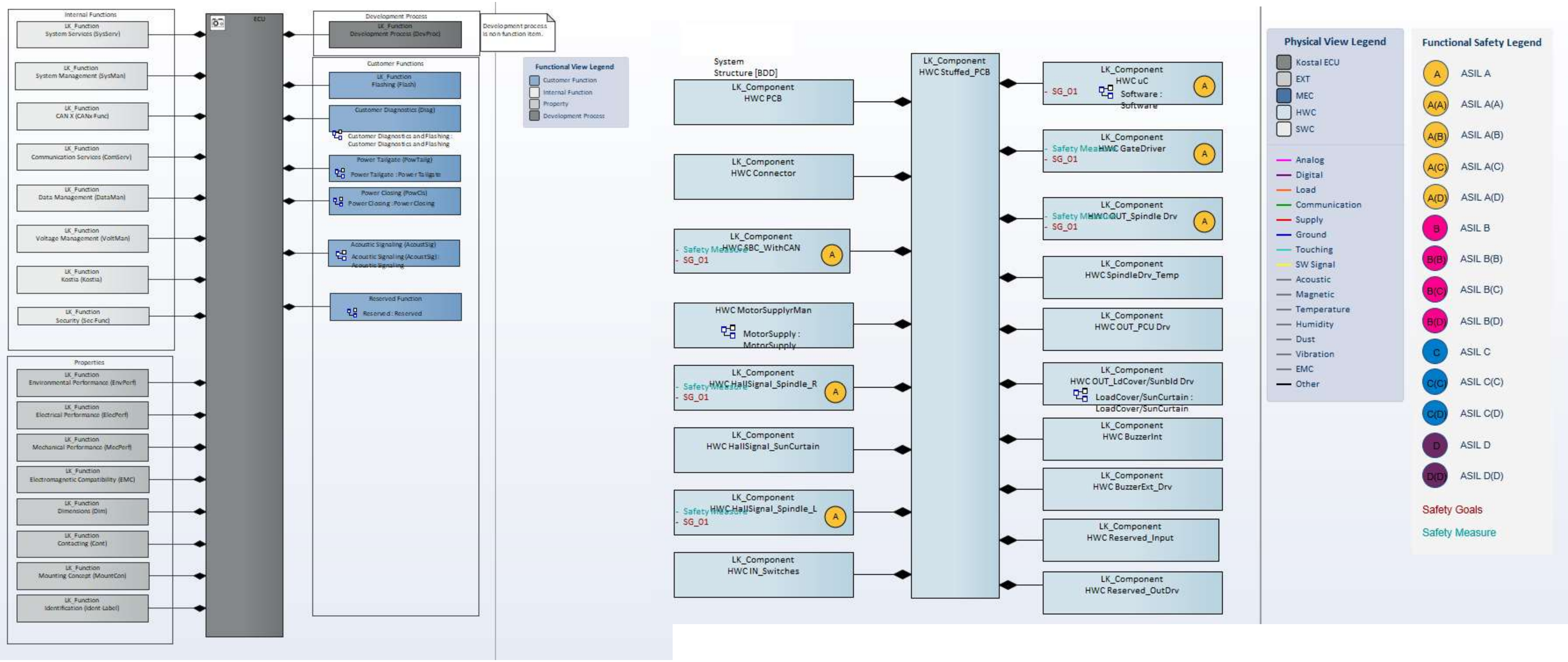


Not OK
Create SW Architecture
Create HW Detailed Design
Create P–Diagram
Create Mechanics Requirements...
Create Hardware Requirements...
Carry out Safety Analysis (System)
Create Software Requirements...
Create System Requirements...
Create System Architecture
Specify Interfaces of System Elements
Carry out System Tolerance Study
System Tolerances fulfilled?
Not OK
Create Safety Manual
Create Drawing
Create HILP Test Specification
Create system integration strategy
Create HIL Test Specification
Create functional dimensions analysis/...

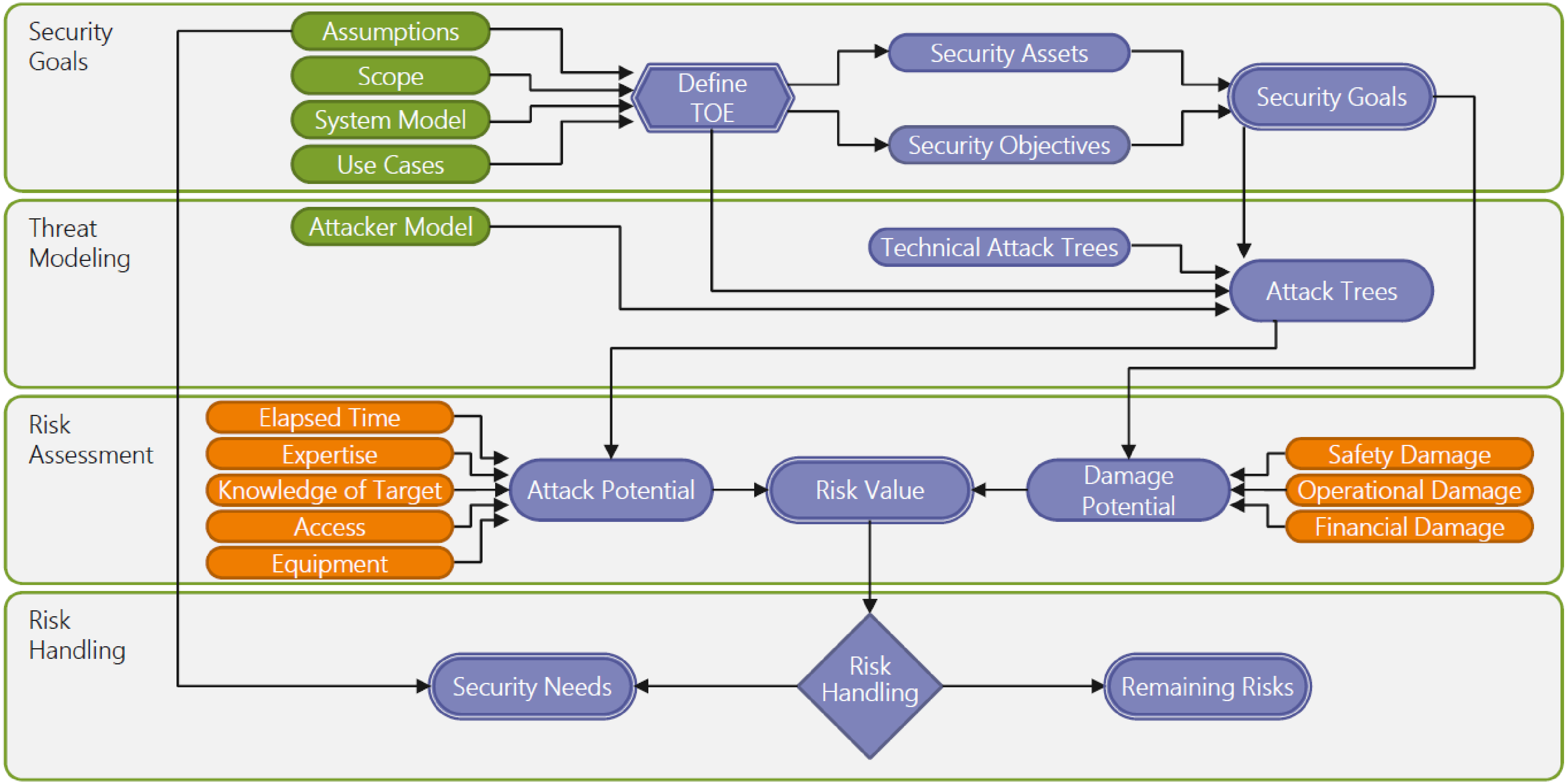
4

统一的产品架构

融合点 ： 产品架构—功能安全


Internal Functions
LK_Function System Services (SysServ)
LK_Function System Management (SysMan)
LK_Function CAN X (CANx Func)
LK_Function Communication Services (ComServ)
LK_Function Data Management (DataMan)
LK_Function Voltage Management (VoltMan)
LK_Function Kostia (Kostia)
LK_Function Security (Sec Func)
Properties
LK_Function Environmental Performance (EnvPerf)
LK_Function Electrical Performance (ElecPerf)
LK_Function Mechanical Performance (MecPerf)
LK_Function Electromagnetic Compatibility (EMC)
LK_Function Dimensions (Dim)
LK_Function Contacting (Cont)
LK_Function Mounting Concept (MountCon)
LK_Function Identification (Ident Label)
ECU
Development Process
LK_Function Development Process (DevProc)
Development process is non function item.
Customer Functions
LK_Function Flashing (Flash)
Customer Diagnostics (Diag)
Customer Diagnostics and Flashing : Customer Diagnostics and Flashing
Power Tailgate (PowTailg)
Power Tailgate : Power Tailgate
Power Closing (PowCls)
Power Closing : Power Closing
Acoustic Signaling (AcoustSig)
Acoustic Signaling (AcoustSig) : Acoustic Signaling
Reserved Function
Reserved : Reserved
Functional View Legend
Customer Function
Internal Function
Property
Development Process
System Structure [BDD]
LK_Component HWC PCB
LK_Component HWC Connector
LK_Component HWC SBC_WithCAN
Safety Measure
SG_01
A
HWC MotorSupplyrMan
MotorSupply : MotorSupply
LK_Component HWC HallSignal_Spindle_R
Safety Measure
SG_01
A
LK_Component HWC HallSignal_SunCurtain
LK_Component HWC HallSignal_Spindle_L
Safety Measure
SG_01
A
LK_Component HWC IN_Switches
LK_Component HWC Stuffed_PCB
LK_Component HWC uC
SG_01
Software : Software
A
LK_Component HWC GateDriver
Safety Measure
SG_01
A
LK_Component HWC OUT_Spindle Drv
Safety Measure
SG_01
A
LK_Component HWC SpindleDrv_Temp
LK_Component HWC OUT_PCU Drv
LK_Component HWC OUT_LdCover/Sunbld Drv
LoadCover/SunCurtain : LoadCover/SunCurtain
LK_Component HWC BuzzerInt
LK_Component HWC BuzzerExt_Drv
LK_Component HWC Reserved_Input
LK_Component HWC Reserved_OutDrv
Physical View Legend
Kostal ECU
EXT
MEC
HWC
SWC
Analog
Digital
Load
Communication
Supply
Ground
Touching
SW Signal
Acoustic
Magnetic
Temperature
Humidity
Dust
Vibration
EMC
Other
Functional Safety Legend
A ASIL A
A(A) ASIL A(A)
A(B) ASIL A(B)
A(C) ASIL A(C)
A(D) ASIL A(D)
B ASIL B
B(B) ASIL B(B)
B(C) ASIL B(C)
B(D) ASIL B(D)
C ASIL C
C(C) ASIL C(C)
C(D) ASIL C(D)
D ASIL D
D(D) ASIL D(D)
Safety Goals
Safety Measure

融合点 ： 产品架构--信息安全设计

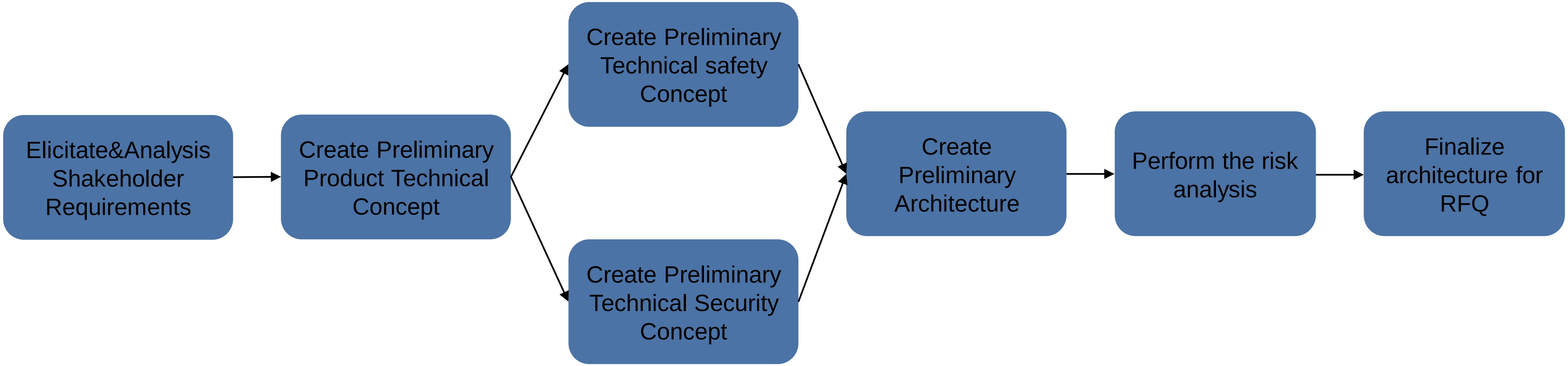


Secure Boot	Secure Flash	Secure Debug	SecOC	Secure Coding
30%	100%	100%	20%	100%

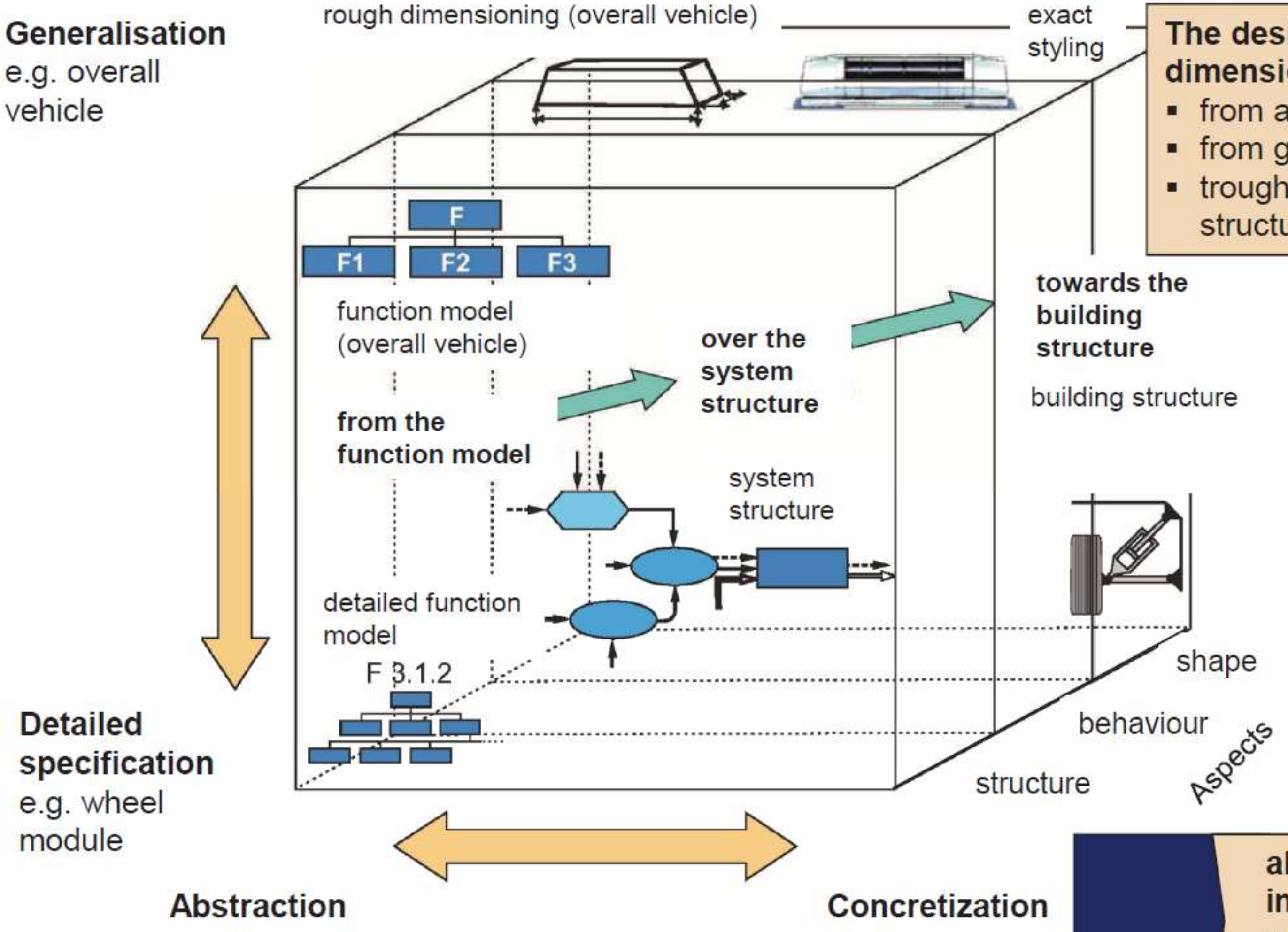
融合点 ： 产品架构

Item definition
Hazard analysis and risk assessment
Functional safety concept
Item definition
Cyber Security Goals
Cyber Security concept

Requirement for quotation
Preliminary functional architecture


Elicitate&Analysis Shakeholder Requirements
Create Preliminary Product Technical Concept
Create Preliminary Technical safety Concept
Create Preliminary Technical Security Concept
Create Preliminary Architecture
Perform the risk analysis
Finalize architecture for RFQ

融合点 ： 产品架构-- Feature base design



The design space constists of 3 dimensions:

- from abstract towards concrete
- from general towards detailed
- trough the aspects (e.g. function, structure, behaviour, shape etc.)

all these dimensions are important for systems engineering as well as for functional safety

5

一体化的实施工具和方法

融合点 ：一体化的工具方法

MBD 助力 ASPICE 认证

- 基于模型设计

图形化设计

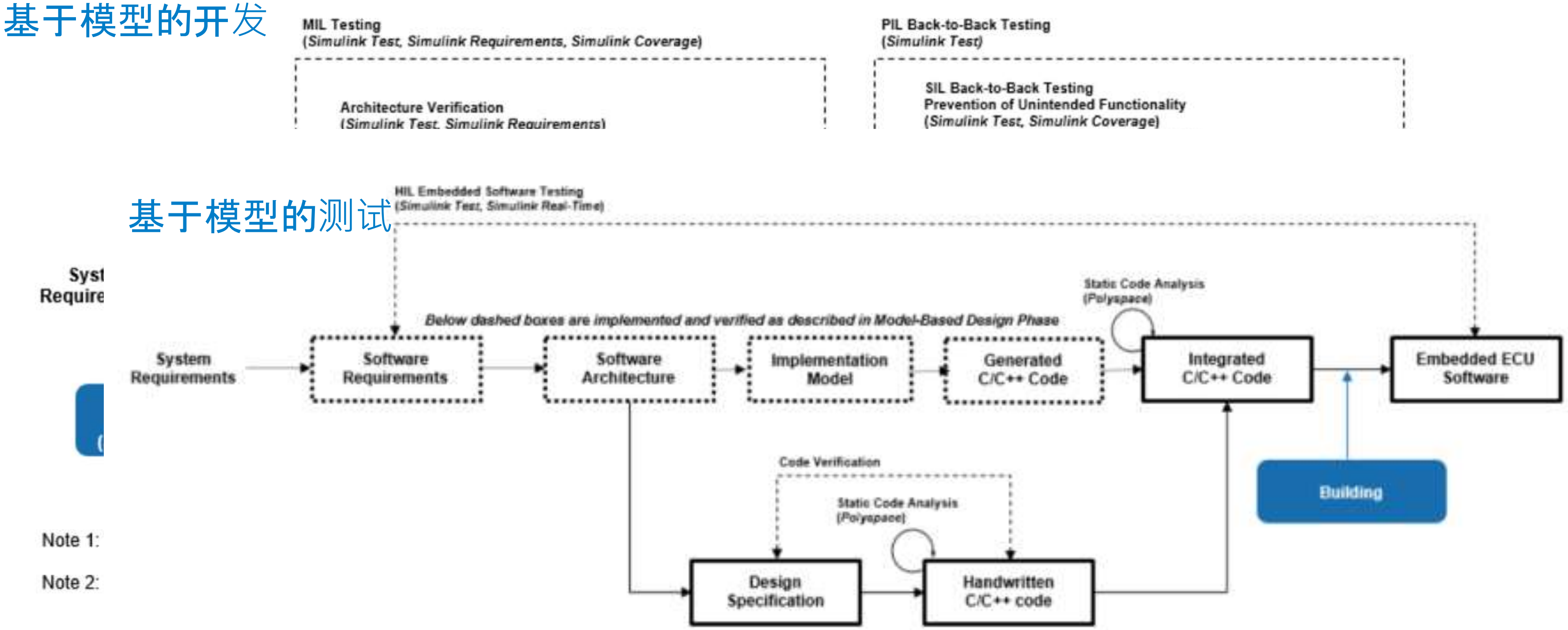
- 简洁、明确
- 便于交流
- 便于维护

代码自动生成

- 开发效率
- 代码品质

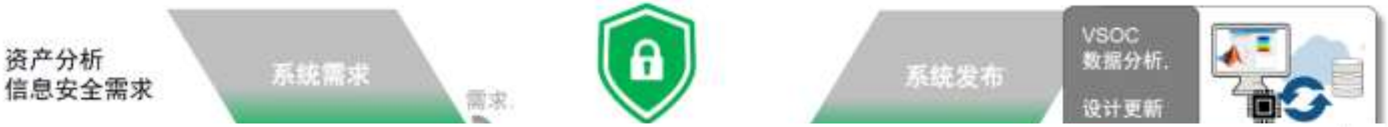
基于模型的开发

基于模型的测试



融合点 ：一体化的工具方法

KOSTAL



需求分配

TARA分析

安全设计

和建模

代码

“左移” – 模型级信息安全规则检查

Design Verifier

Model Advisor

- 识别：
  - 不推荐
  - 非确定
  - 设计缺
- 结果：
  - 防止最
  - 证明不
  - 验证用
  - 生成更
- 其他：
  - 与智能

满足预期更新要求的设计监控

Model Transformer

Clone Detector

Metrics Dashboard

- 复杂度
  - 模
  - 克
  - 变
- 信息安
  - 利
    内
  - 每

代码级规则检查和漏洞分析

Polyspace Code Verifier

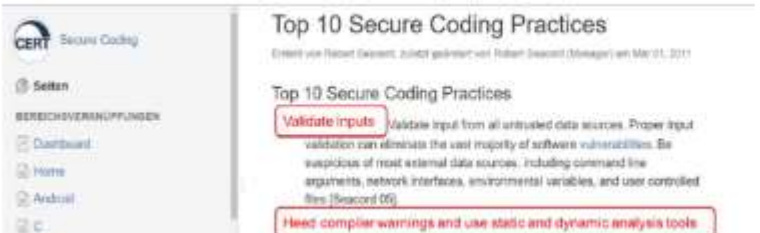
信息安全编码规范

- CERT C(++)
- ISO/IEC TS 17961:2013
- MISRA C:2012
- CWE
- 加密检查、污点分析…

代码鲁棒性

- 针对所有输入和程序状态
  - 越界数组访问？
  - 无效指针？除零运算？
- 针对目标处理器
  - 浮点错误？软浮点？
  - 中断和竞争条件？
  - 堆栈大小？内存泄漏？

+



Top 10 Secure Coding Practices

Erstellt von Robert Seacord, zuletzt geändert von Robert Seacord (Manager) am Mar 01, 2011

Top 10 Secure Coding Practices

Validate inputs Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files [Seacord 05].

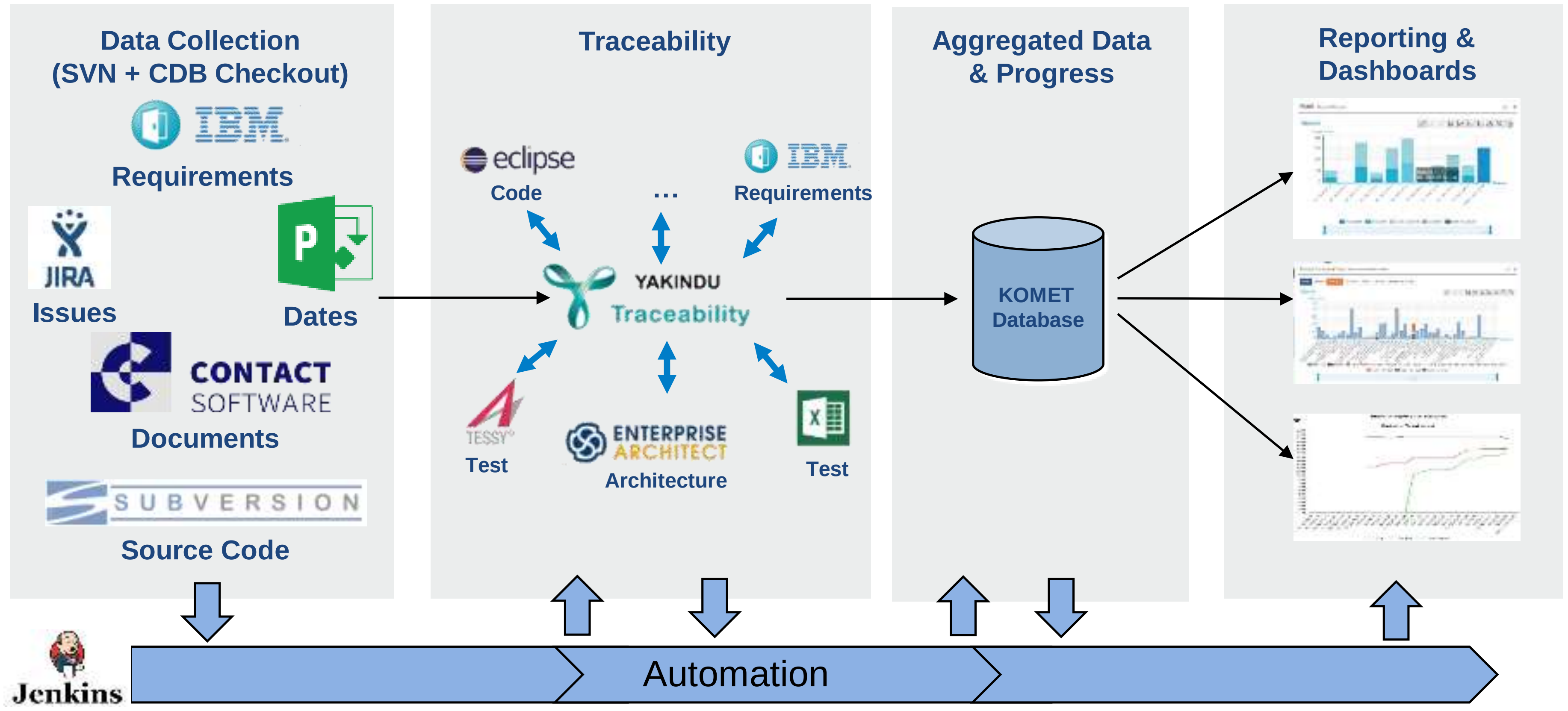
Heed compiler warnings and use static and dynamic analysis tools

保密性
完整性
可用性

测试不可行时

RIK

融合点 ：一体化的工具方法



Data Collection (SVN + CDB Checkout)

IBM Requirements

JIRA Issues

Dates

CONTACT SOFTWARE Documents

SUBVERSION Source Code

Traceability

eclipse Code

…

IBM Requirements

YAKINDU Traceability

TESSY Test

ENTERPRISE ARCHITECT Architecture

Test

Aggregated Data & Progress

KOMET Database

Reporting & Dashboards

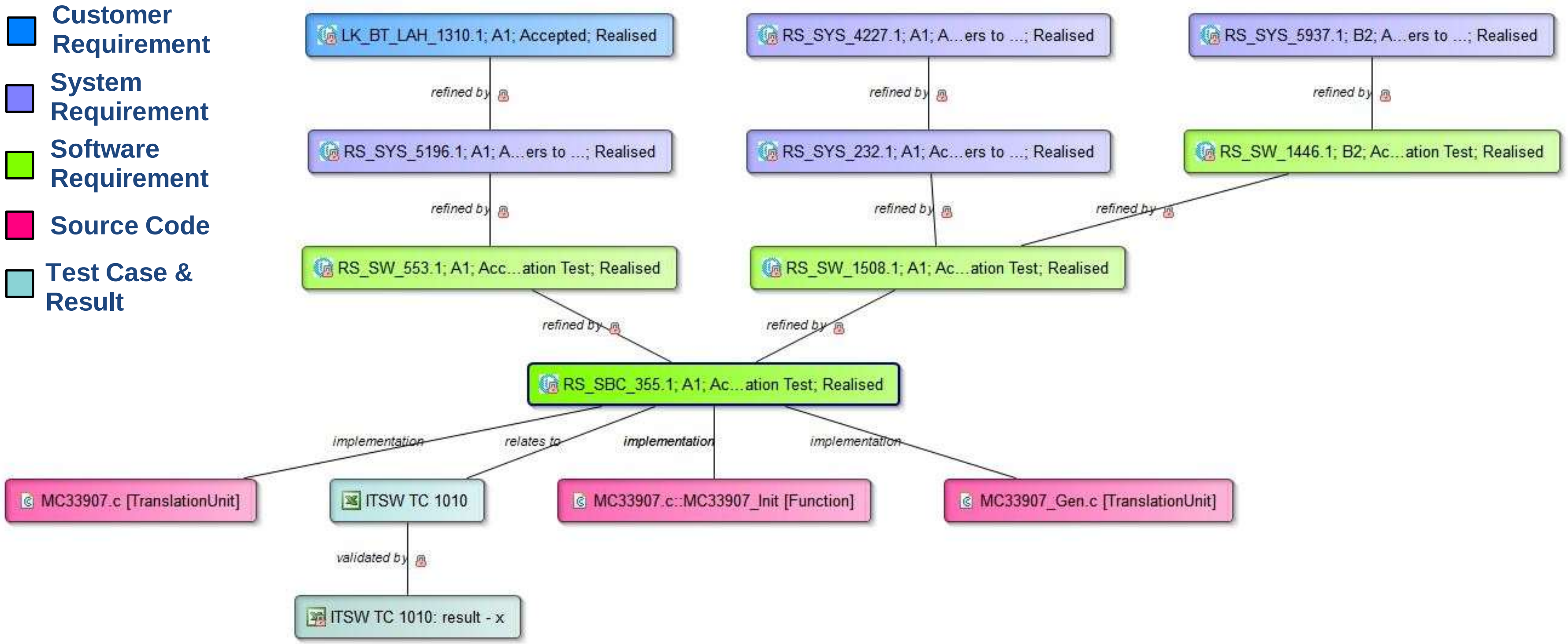
Jenkins

Automation

融合点 ：一体化的工具方法

把所有的开发过程通过一个系统连接起来

把从需求、设计、实施、测试等所有过程的追溯用最直观的方法表示出来



🟦 Customer Requirement

🟪 System Requirement

🟩 Software Requirement

🟥 Source Code

▨ Test Case & Result

LK_BT_LAH_1310.1; A1; Accepted; Realised

RS_SYS_4227.1; A1; A...ers to ...; Realised

RS_SYS_5937.1; B2; A...ers to ...; Realised

refined by

RS_SYS_5196.1; A1; A...ers to ...; Realised

RS_SYS_232.1; A1; Ac...ers to ...; Realised

RS_SW_1446.1; B2; Ac...ation Test; Realised

RS_SW_553.1; A1; Acc...ation Test; Realised

RS_SW_1508.1; A1; Ac...ation Test; Realised

RS_SBC_355.1; A1; Ac...ation Test; Realised

implementation

relates to

MC33907.c [TranslationUnit]

ITSW TC 1010

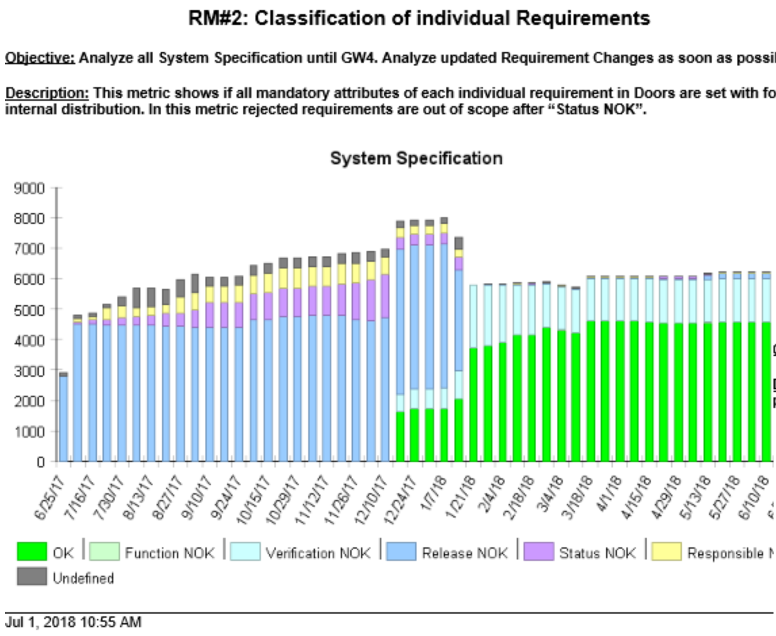
MC33907.c::MC33907_Init [Function]

MC33907_Gen.c [TranslationUnit]

validated by

ITSW TC 1010: result - x

系统化的开发过程管理（项目管理、功能安全管理、信息安全管理）



RM#2: Classification of individual Requirements

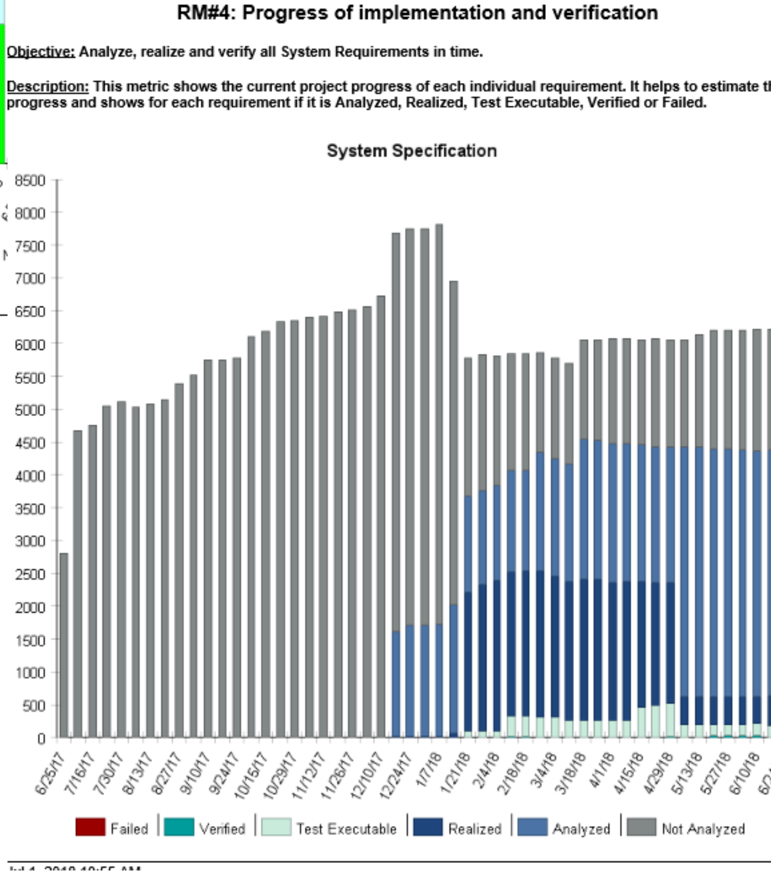
Objective: Analyze all System Specification until GW4. Analyze updated Requirement Changes as soon as possible.

Description: This metric shows if all mandatory attributes of each individual requirement in Doors are set with focus on internal distribution. In this metric rejected requirements are out of scope after "Status NOK".

System Specification

🟩 OK | Function NOK | Verification NOK | Release NOK | Status NOK | Responsible N
Undefined

Jul 1, 2018 10:55 AM



RM#4: Progress of implementation and verification

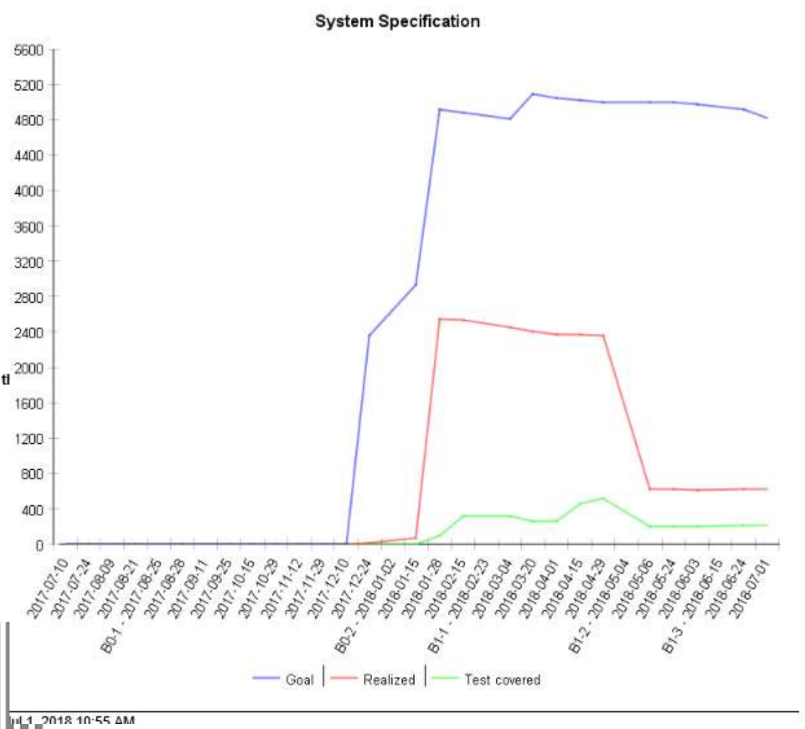
Objective: Analyze, realize and verify all System Requirements in time.

Description: This metric shows the current project progress of each individual requirement. It helps to estimate tl progress and shows for each requirement if it is Analyzed, Realized, Test Executable, Verified or Failed.

System Specification

Failed | Verified | Test Executable | Realized | Analyzed | Not Analyzed

Jul 1, 2018 10:55 AM



System Specification

Goal | Realized | Test covered

Jul 1, 2018 10:55 AM

Conclusion 总结

- 分析了ASPiCE、功能安全、信息安全对开发过程要求的异同点，定义系统化的开发流程
- 根据各自的特点定义各自的技术规范和管理体系
- 将三个规范的需求和设计在项目启动时统一到系统需求和系统架构
- 用一个统一的实施过程来同时实现三个标准的对开发的要求
  - 有效的开发设计测试工具
  - 统一的报表系统
- 用三个独立的标准分别进行审核

2022 MathWorks
中国汽车年会

Thank you

MathWorks