intacs.info
International Assessor Certification Scheme™

INTACS Cybersecurity SPICE

VDA Automotive SYS
2019-06-27

André Zeh
Thomas Liedtke
Steffen Zindler

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

intacs.info
International Assessor Certification Scheme™

Introduction

Task: How to integrate cyber security aspects into an assessment model

Intacs working group with

- currently 25 members
- from OEMs, suppliers and consultants
- with skills in Automotive SPICE® and/or cyber security

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

Aim and targets

- Based on known assessment standards like ASpice
  - Reuse existing results and reviews
  - Integration of cyber security in existing process landscape
- Covering entire lifecycle including
  - Development
  - Production
  - After sales
- Based on best practice
- Ensure “Security by Design”

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

Basic concept

- Plug-in concept for Automotive SPICE®
  - No changes to the Automotive SPICE® standard
  - Automotive SPICE® as basic requirement
  - New processes for cyber security (similar to HW SPICE and Mechnical SPICE)
  - New outcomes and new base practices in existing processes

- Compliant to upcoming standards (e.g. ISO/SAE 21434) and recommendations (e.g. UNECE)

Agenda

Introduction

Aim and targets

Basic concept

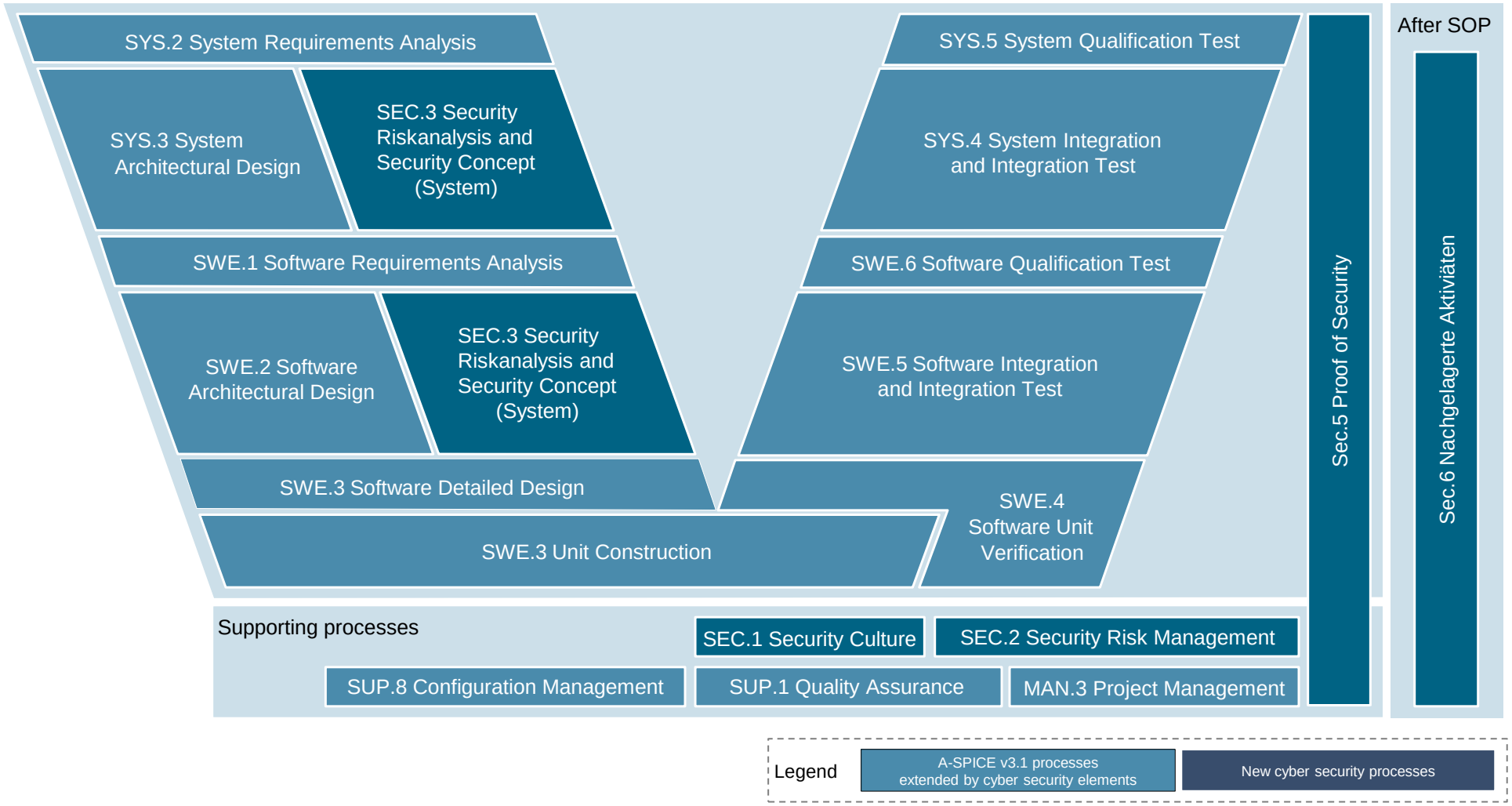
Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

Adjusted V-Modell for „Intacs Cybersecurity SPICE“



Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

intacs.info
International Assessor Certification Scheme™

Additional Processes for Cybersecurity which come on top

SEC.1: Security Culture

Purpose:

- establish agreed upon **security objectives**, develop an appropriate **security strategy** and to establish **policies** and **practices** which will strengthen **security awareness** throughout the organization

Additional Base practices:

- Establish a **company-wide Cybersecurity strategy**
- Established **Cybersecurity over all levels** of the organization
- Provide necessary resources for a **secure development**
- Ensure **Cybersecurity compliance**

⇒ **Concept and idea very similar to Functional Safety**

SEC.2: Security Risk Management

Purpose:

- **identify, analyse, track** and **resolve security threats** in a documented and traceable fashion so as to ensure that security risks are held to an accepted level

Additional Base practices:

- Create a **strategy** for the Cybersecurity risk management
- Identify **Cybersecurity threats**
- Ensure **treatment** of all security risks
- **Monitor** and **communicate** security risks

⇒ **Overal performance of cybersecurity risk management**

SEC.3: Security Risk Analysis and Security Concept on System Architectural Design

Purpose:

- identify **assets**, which are then correlated with the identified threats and the potential resulting damage so as to derive an overview and **evaluation** of **risks**. **Appropriate controls** are then specified to mitigate the level of remaining risk, reducing it to an acceptable level

Additional Base practices:

- Perform **Cybersecurity threat analysis** of the System Architectural Design
- Perform a **risk evaluation** of the System Architectural Design
- Assess the system risks
- Define **appropriate controls** for each not accepted system risk
- **Update** the **System Requirements** and the System Architectural Design
- **Communicate the results** of the Cybersecurity Risk Analysis
- **Verify** the Security Risk Analysis
- Establish **bidirectional traceability**

SEC.4: Security Risk Analysis and Security Concept on Software Architectural Design

Purpose:

- extend the results of SEC.3 to provide detailed coverage of the Software Architecture Design

Additional Base practices:

- Perform a **Cybersecurity vulnerability analysis** of the Software Architectural Design
- Perform a **risk evaluation** of the Software Architectural Design
- Assess the software system risks
- Define **appropriate controls** for each not accepted software system risk
- Update requirements and architectural design
- **Communicate the results**
- **Verify** the security risk analysis on Software Architectural Design
- Establish **bidirectional traceability**

SEC.5: Proof of Cybersecurity

Purpose:

- **demonstrate product compliance** with all security requirements by providing traceability from the customer security requirements through to the final, successful test results. This traceability will reference all documentation generated during the development process, allowing reviews of controls and clear visibility of remaining risks.

Additional Base practices:

- Conduct **an independent assessment** of the Cybersecurity
- **Communicate** the proof of Cybersecurity to all stakeholders

⇒ **Cybersecurity Assessment has to capture all relevant Cybersecurity Activities**

SEC.6: Ensure cybersecure operation

Purpose:

- **ensure** the **lasting security** of the deployed product as the environment evolves over the course of time

Additional Base practices:

- Define a **strategy for post-production activities**
- Define **escalation paths**
- Conduct **market** and **field observation**
- Conduct a **Weakness analysis**
- Define **resolution measures**
- **Consider findings** the current developments

⇒ **Cybersecurity means to take care for the complete life-cycle**

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

intacs.info
International Assessor Certification Scheme™

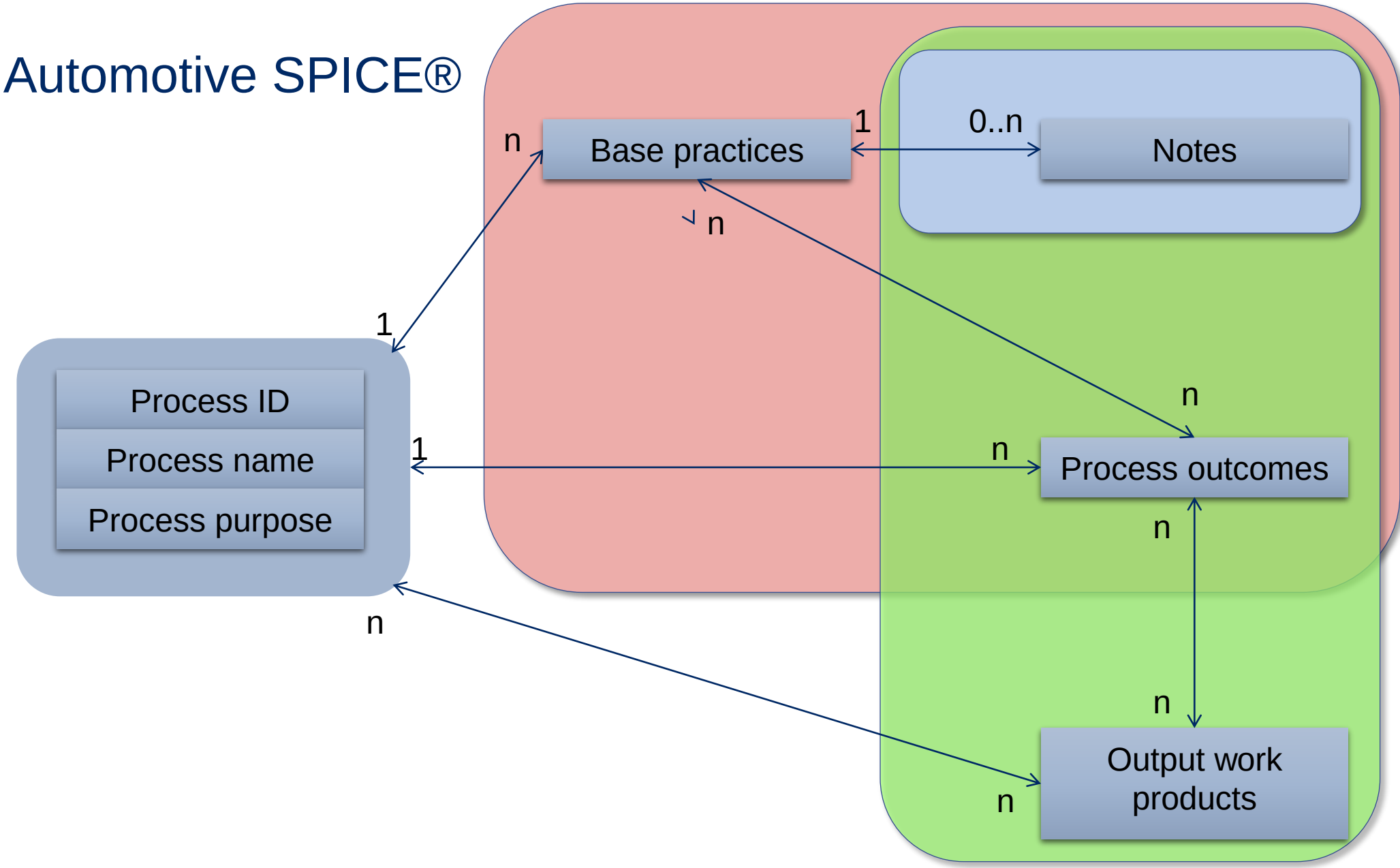
Structure of Automotive SPICE®

No additions: 18

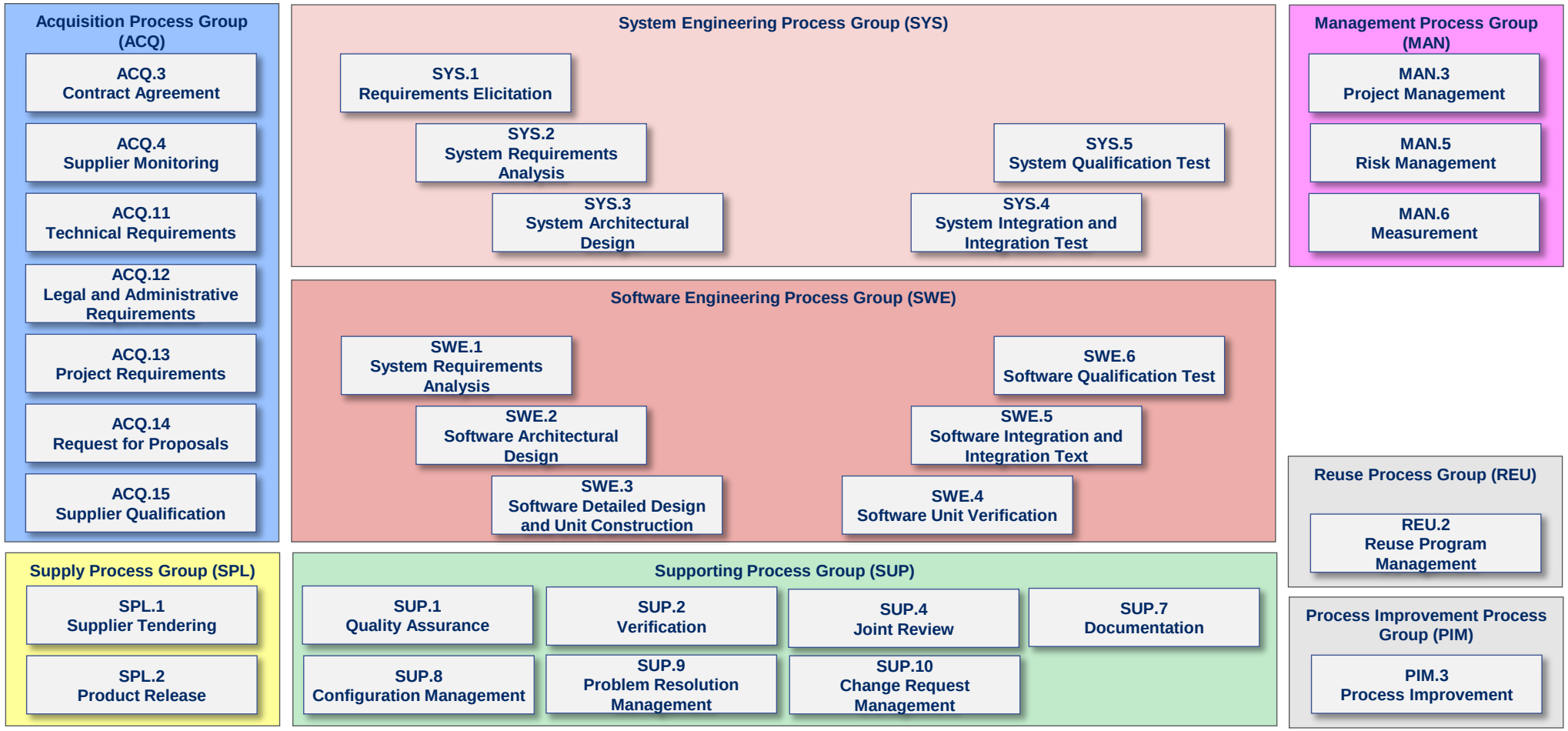
Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1



Structure of Automotive SPICE®



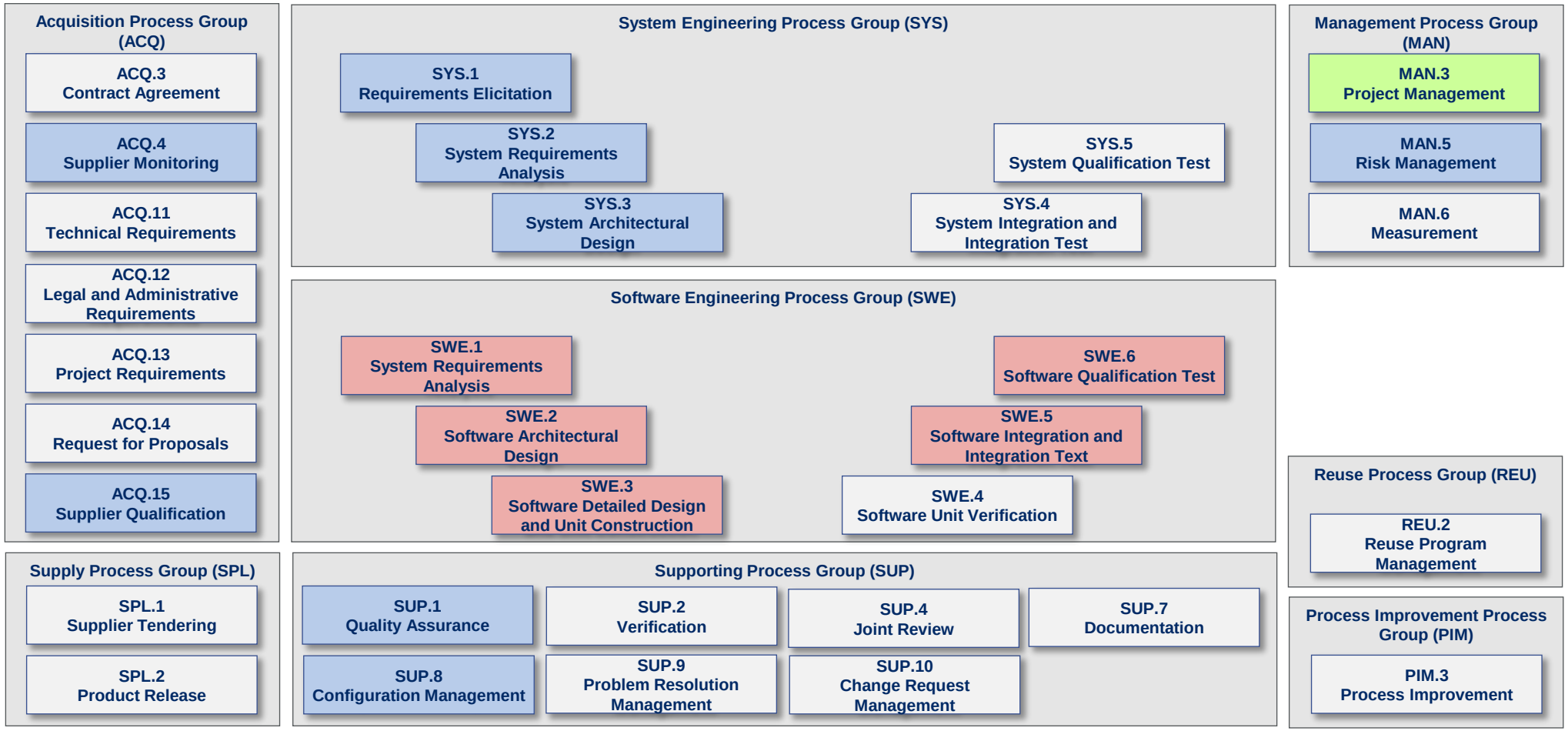
Complemented Processes

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1



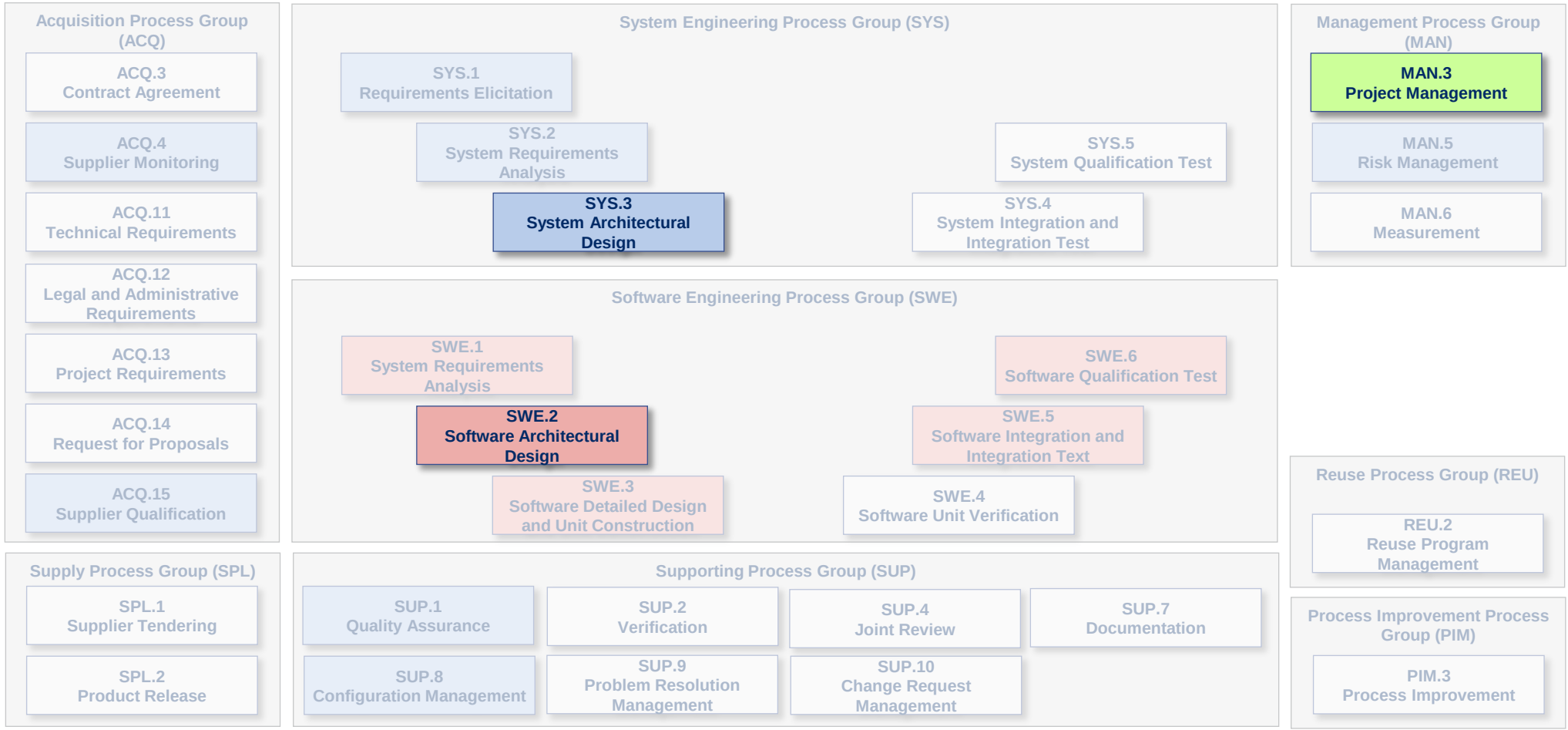
Complemented Processes

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1



Complemented Processes

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1

Base practices	**SYS.3.BP1: Develop system architectural design.** Develop and document the system architectural design that specifies the elements of the system with respect to functional and non-functional system requirements. [OUTCOME 1] *NOTE 1: The development of system architectural design typically includes the decomposition into elements across appropriate hierarchical levels.*

SYS.3.BP1.NOTE-Sec1:
The system architectural design should be capable to be used as the basis for the conduction of the security risk analysis on the system level. Refer **to SEC.2.BP-Sec2.**

Complemented Processes

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1

Base practices	
	SWE.2.BP1: Develop software architectural design. Develop and document the software architectural design that specifies the elements of the software with respect to functional and non-functional software requirements. [OUTCOME 1] *NOTE 1: The software is decomposed into elements across appropriate hierarchical levels down to the software components (the lowest level elements of the software architectural design) that are described in the detailed design.* **SWE.2.BP2: Allocate software requirements.** Allocate the software **SWE.2.BP3: Define interfaces of software elements.** Identify, develop **SWE.2.BP4: Describe dynamic behavior.** Evaluate and document the **SWE.2.BP5: Define resource consumption objectives.** Determine and **SWE.2.BP6: Evaluate alternative software architectures.** Define **SWE.2.BP7: Establish bidirectional traceability.** Establish bidirectional **SWE.2.BP8: Ensure consistency.** Ensure consistency between software **SWE.2.BP9: Communicate agreed software architectural design.**

Complemented Processes

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1

Base practices	**SWE.2.BP1: Develop software architectural design.** Develop and document the software architectural design that specifies the elements of the software with respect to functional and non-functional software requirements. [OUTCOME 1] *NOTE 1: The software is decomposed into elements across appropriate hierarchical levels down to the software components (the lowest level elements of the software architectural design) that are described in the detailed design.*

SWE2.BP-Sec1: Reduce likelihood of propagation of attacks. The software security architectural design has to reduce the likelihood that compromise of assets within one architectural element would result in propagation of the attack to other architectural elements. [OUTCOME Sec1]

NOTE-Sec1: Security mechanisms are typically interface protection, secure data storage, firewalls, sand-boxes etc.

NOTE-Sec2: Architectural premises may be helpful on the software level.

NOTE-Sec3: Defense-in-depth approach could be applied.

No additions: 18

Notes added: 8

Notes, BPs, Outcomes added: 5

Notes, Outcomes, Output work products added: 1

Process outcomes	As a result of successful implementation of this process: 1) the scope of the work for the project is defined; 2) the feasibility of achieving the goals of the project with available resources and constraints is evaluated; 3) the activities and resources necessary to complete the work are sized and estimated; 4) interfaces within the project, and with other projects and organizational units, are identified and monitored; 5) plans for the execution of the project are developed, implemented and maintained; 6) progress of the project is monitored and reported; and 7) corrective action is taken when project goals are not achieved, and recurrence of problems identified in the project is prevented.
Output work products	08-12 Project plan → [OUTCOME 1, 3, 4, 5] 13-04 Communication record → [OUTCOME 4, 6] 13-16 Change request → [OUTCOME 7] 13-19 Review record → [OUTCOME 2, 7] 14-02 Corrective action register → [OUTCOME 7] 14-06 Schedule → [OUTCOME 3, 5] 14-09 Work breakdown structure → [OUTCOME 3, 4, 5] 14-50 Stakeholder groups list → [OUTCOME 4] 15-06 Project status report → [OUTCOME 4, 6]

08-Sec01: Security Plan → [OUTCOME 3, 4, 5]

Agenda

Introduction

Aim and targets

Basic concept

Adjusted V-Model

New processes

Add-Ons for existing Automotive SPICE® processes

Outlook

intacs.info
International Assessor Certification Scheme™

Outlook

- Review phase ongoing
- New active team members are welcome
- Searching for friendly user projects for piloting and lessons learned

Timeline	2019		2020	
	Q3	Q4	Q1	Q2
INTACS Cybersecurity SPICE	review of latest base line	piloting | friendly user	shape | lessons learned | review	alignment to ISO and UN-ECE | first public draft
ISO/SAE 21434		DIS 30.10.		FDIS 30.06.
UN-ECE	test phase			

intacs.info

International Assessor Certification Scheme™

DO YOU HAVE ANY QUESTIONS?

Icons: http://www.1001FreeDownloads.com Photos: www.unsplash.com, © Fotolia.de, kasko