Anforderungen IEC 62443 - Wann ist Was zu tun?

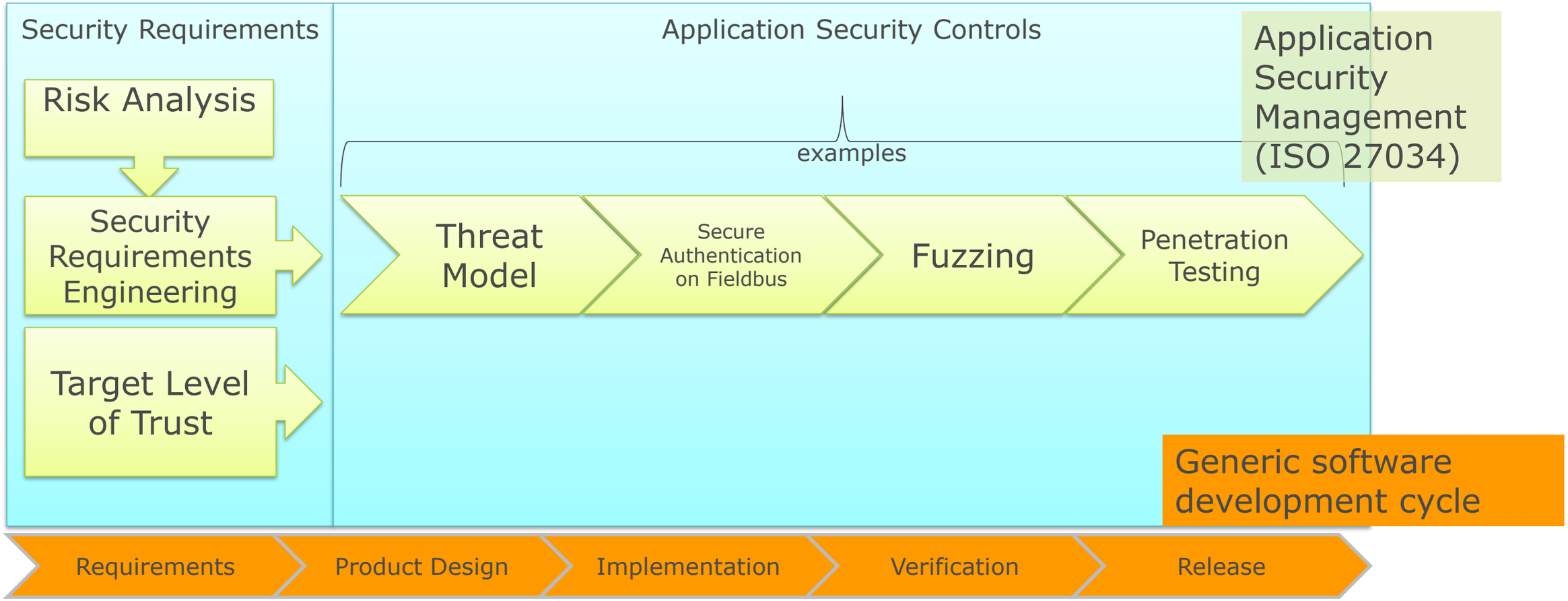
Einbindung von Security in bestehende Prozesse

Max Perner

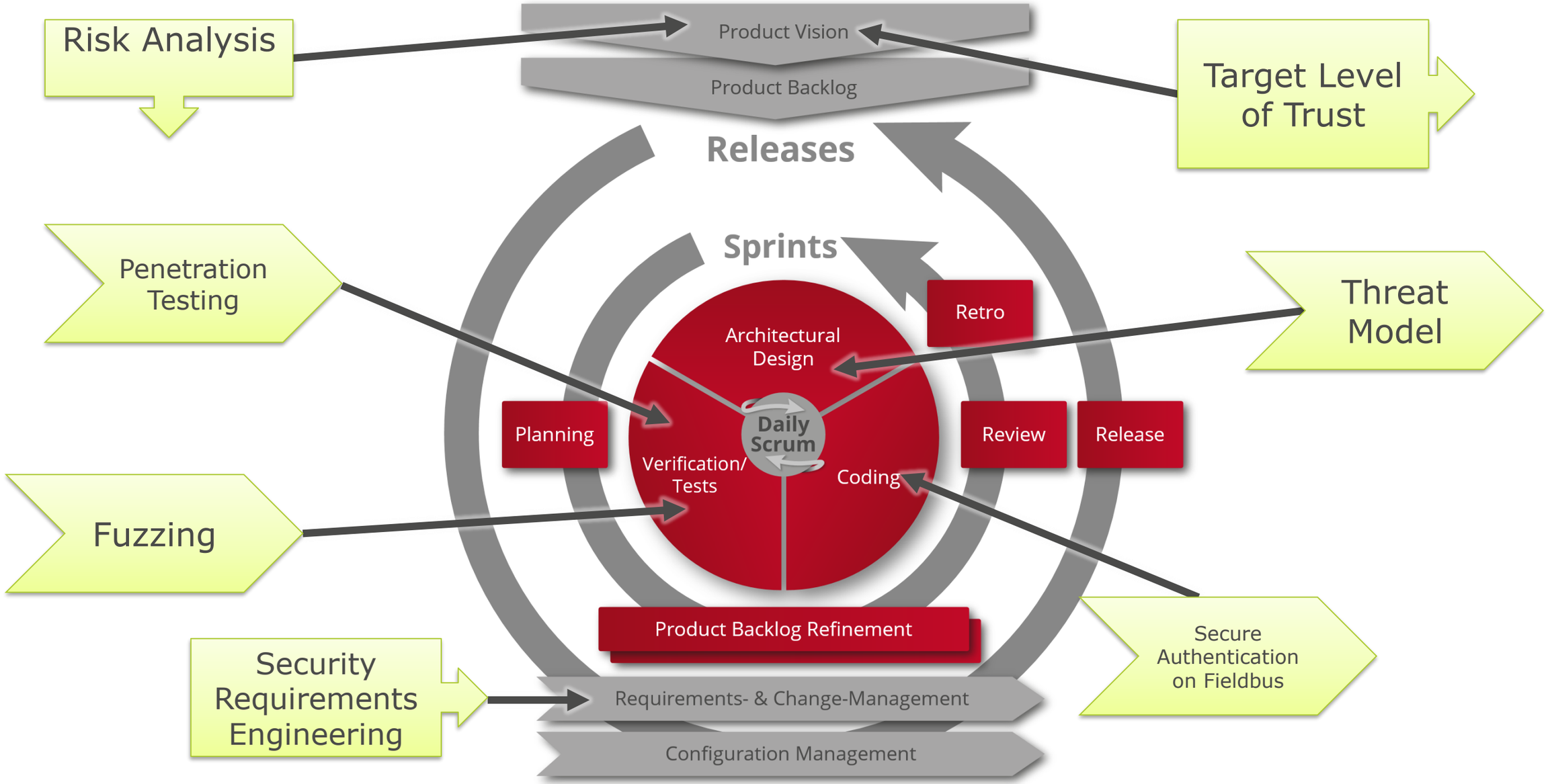
Agenda

1. Why?
   - Existing Process lacked Security.
2. How?
   - IEC 62443 Part 4
   - What must be done and documented?
   - Examples of implementation and synergy
   - Timing
3. Conclusions

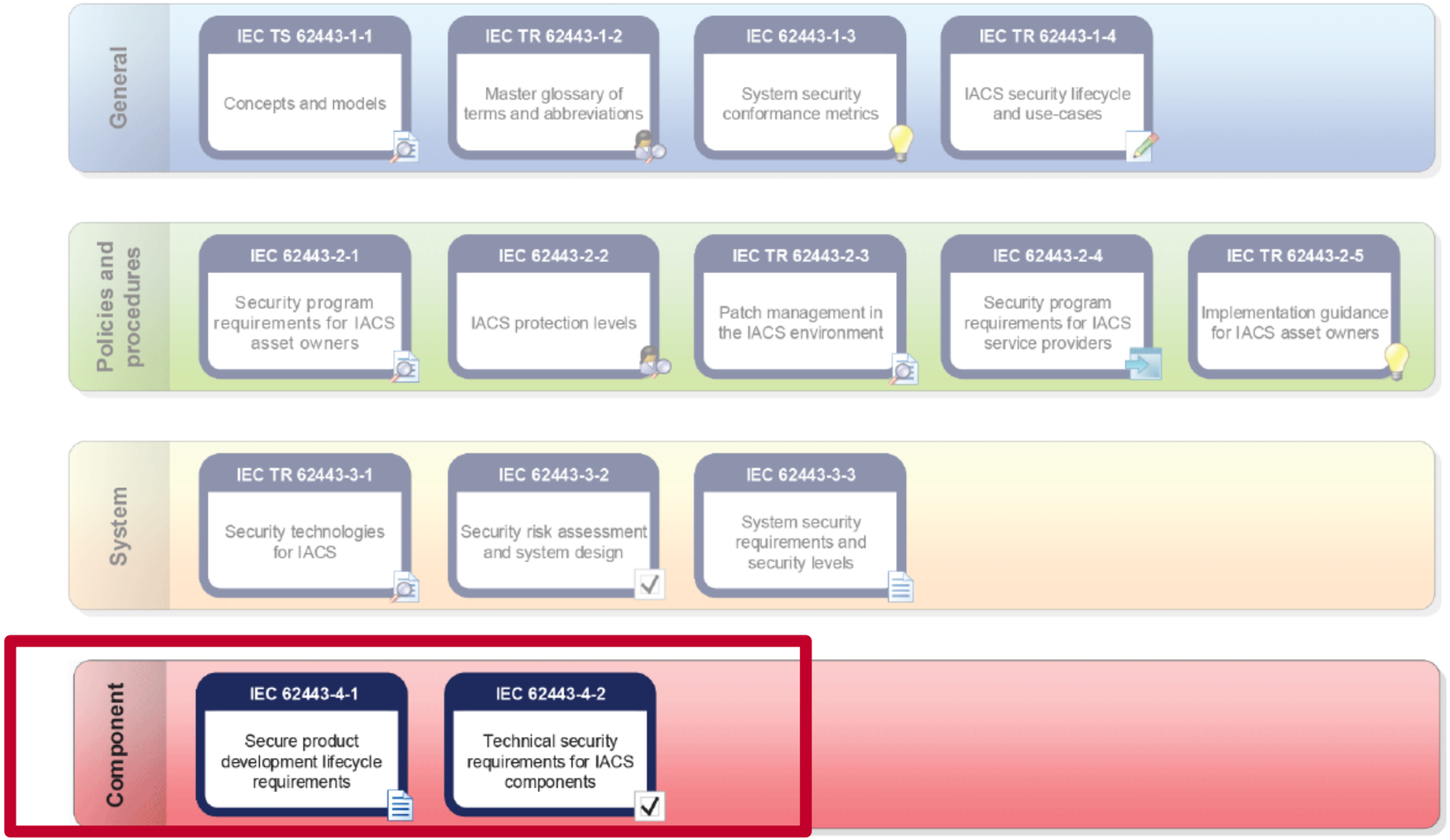
Process Integration



Process Integration



Overview IEC 62443



IEC 62443-4-1:2018 p.9

IEC 62443-4

IEC 62443-4-1 Practices	IEC 62443-4-2 Component Requirements
Secure product development lifecycle requirements	Technical security requirements for IACS components

Practices
Management
Requirements
V&V
Design
Implementation
Issues
Updates
Guidelines

Foundational Requirements
Identification & Authentication Control IAC
Use Control UC
System Integrity SI
Data Confidentiality DC
Restricted Data Flow RDF
Timely Response to Events TRE
Resource Availability RA

Requirements to document: Examples

62443-4-1:

SUM-2: Security update documentation

Practice 8: SG-* – Security guidelines

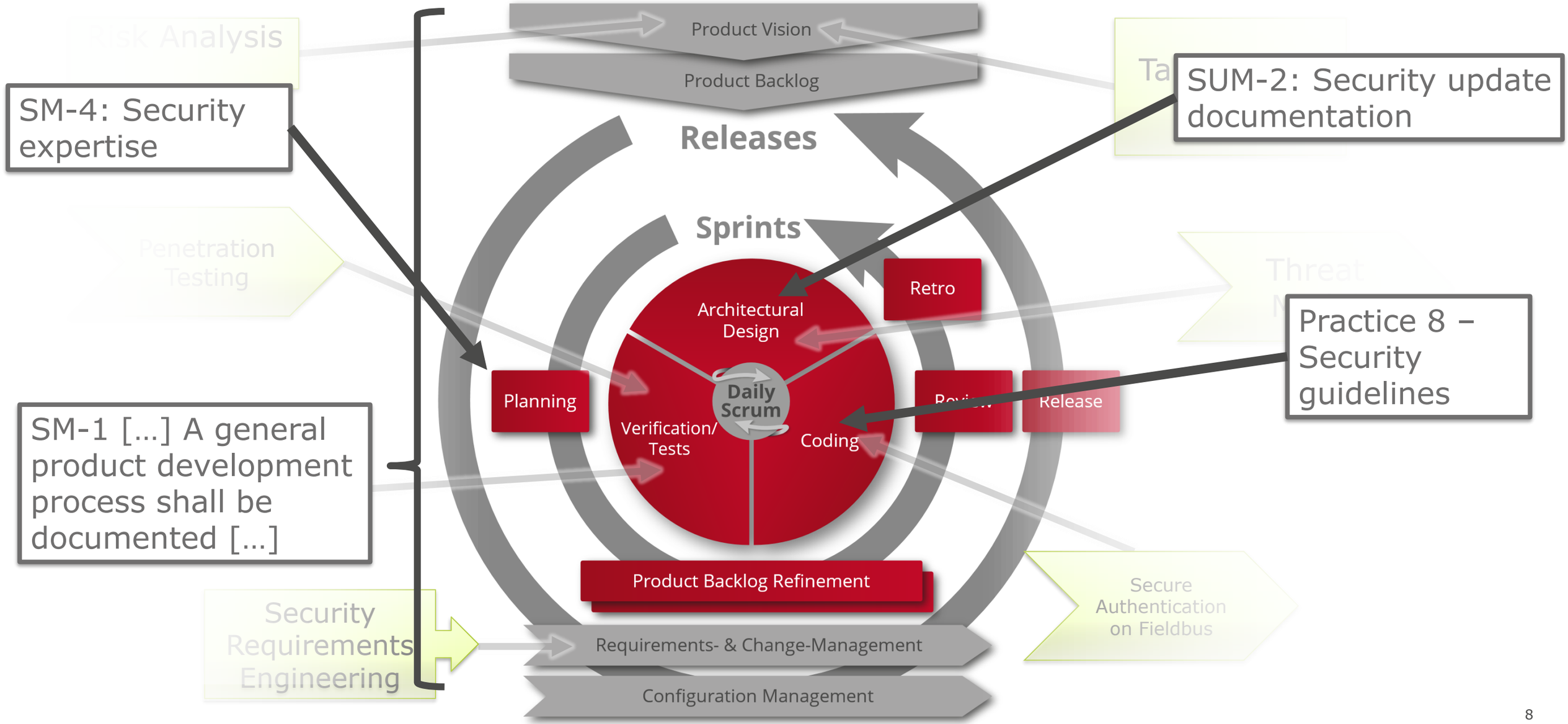
SM-1 […] A general product development/maintenance/support process shall be documented and enforced […]

SM-4: Security expertise: […] security training and assessment programs to ensure […] demonstrated security expertise appropriate […]

62443-4-2:

As defined in Practice 8 of IEC 62443-4-1, the product supplier will provide documentation on how to properly integrate the component into a system to meet a specific SL-T.

Interaction Between Process



Documentation

Security Concept

System Design

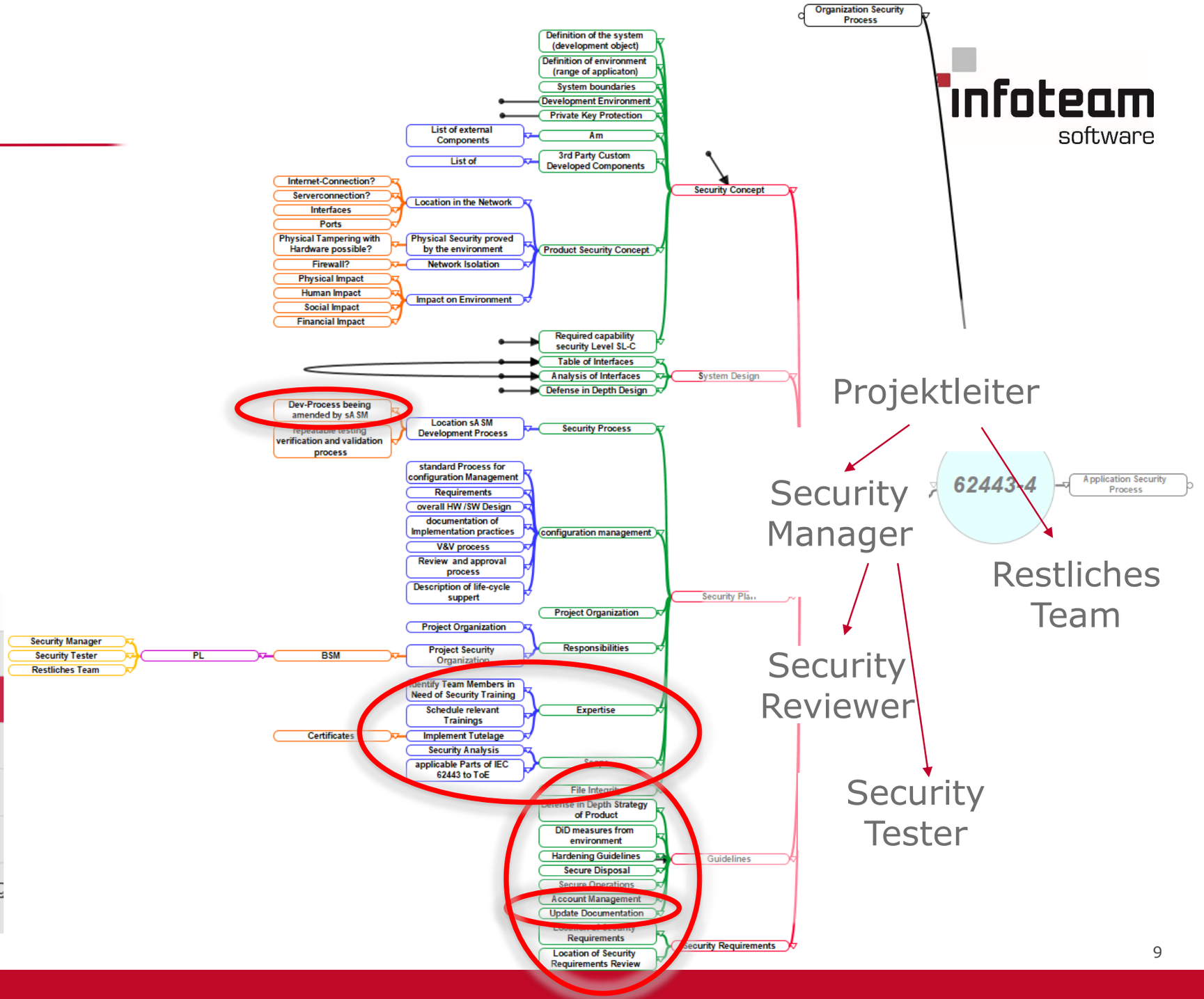
Security Plan

Security Requirements

Guidelines

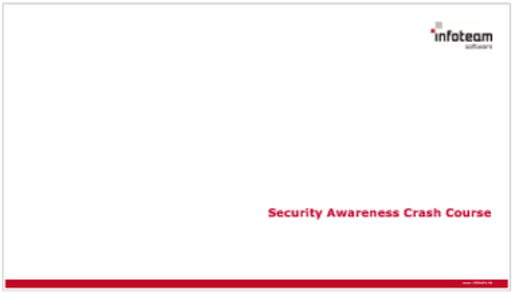
4.3 Checkliste Projektstart

LN.	*Tätigkeit*
Abschnitt 1	**Checkliste Projektstart**
1.	Wer ist verantwortlich für dieses Projekt?
2.	Folgt das Projekt einer Security Norm?
3.	Falls Ja: sind Konzept und Plan ausgefüllt?
4.	Sind Abweichungen von der normalen Vorg dokumentiert?



Security Awareness Crash Course
Example for SM-4

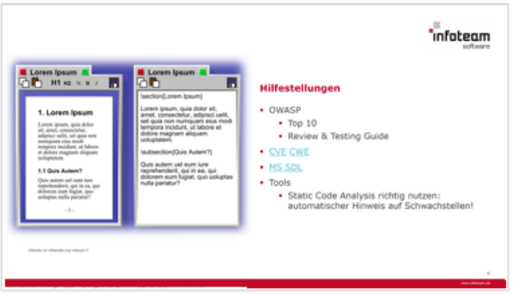
- Ziel: Sensibilisierung im Projekt Kick-off
- Best Practices
  - Lifecycle
  - Code Review
  - Coding Guidelines nach Programmiersprachen
  - Testing
  - Vulnerabilities vermeiden
- Anregungen zu Secure Design
- Hinweis auf Sicherheitsrichtlinien . . .
- Hinweis auf Ansprechpartner



1

2

3



4

5

6

7

8

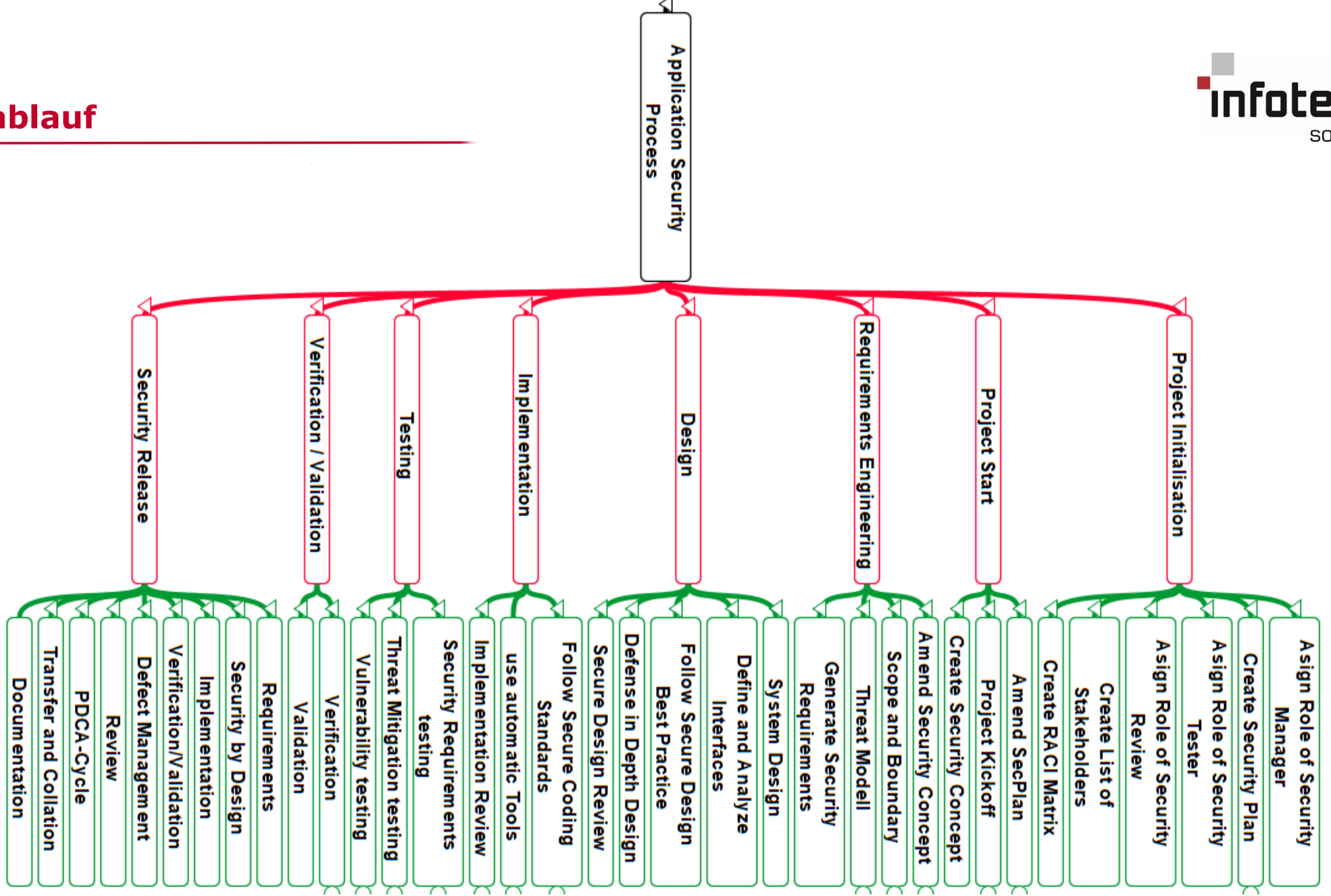
infoteam software

ASQF Secure Software Engineering

- **Lehrplaninhalte**
- Motivation und Grundverständnis
- Security Bedrohungsanalyse und Anforderungserhebung
- Konstruktives Secure Software Engineering und Architektur
- Analytisches Secure Software Engineering und Testen
- Abgesichertes Deployment und Betrieb
- Cyber Security im Software Lifecycle und Prozess

Ablauf im Prozess

Projektablauf



Conclusion

Existing Processes are used as much as possible

- Quality Management, Documentation and Requirements Engineering already have a high maturity if one does funcional safety
- 47 Practices = 47 Points to integrate for IEC 62443 Compliance

Benefits of following IEC 62443 for:

- Integrators: Lists of Interfaces and Ports
- Updates and follow-up projects: List of 3rd party software and evaluations
- Colleagues: Awareness and List of Best Practices

Kontakt

infoteam Software AG
Am Bauhof 9 | 91088 Bubenreuth | Deutschland

Telefon: +49 9131 78 00-0
Telefax: +49 9131 78 00-50
info@infoteam.de | www.infoteam.de

Alle verwendeten Hard- und Softwarenamen sind Handelsmarken und/oder eingetragene Marken der jeweiligen Hersteller.