Agile Methoden als Diagnose-Tool für den sicherheitskritischen Bereich

Christoph Schmiedinger

Frankfurter Entwicklertag 2015

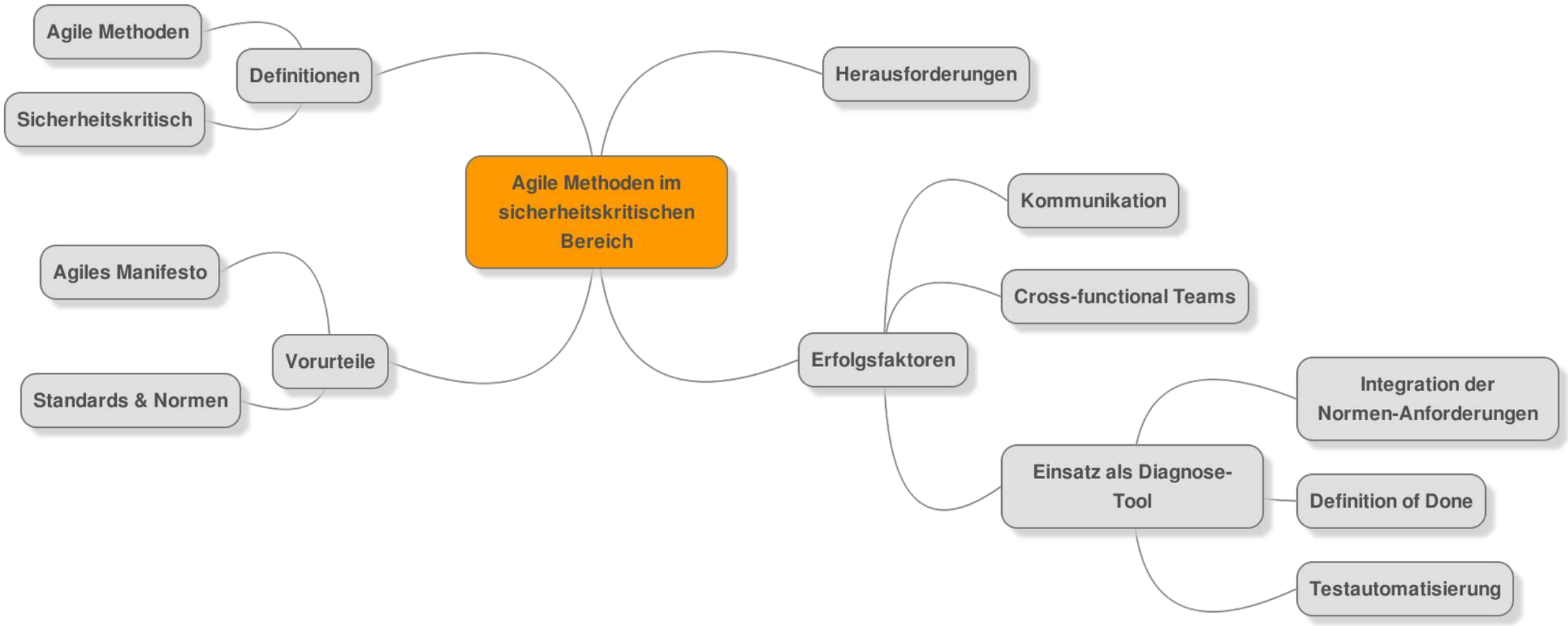
24.02.2015

Über mich

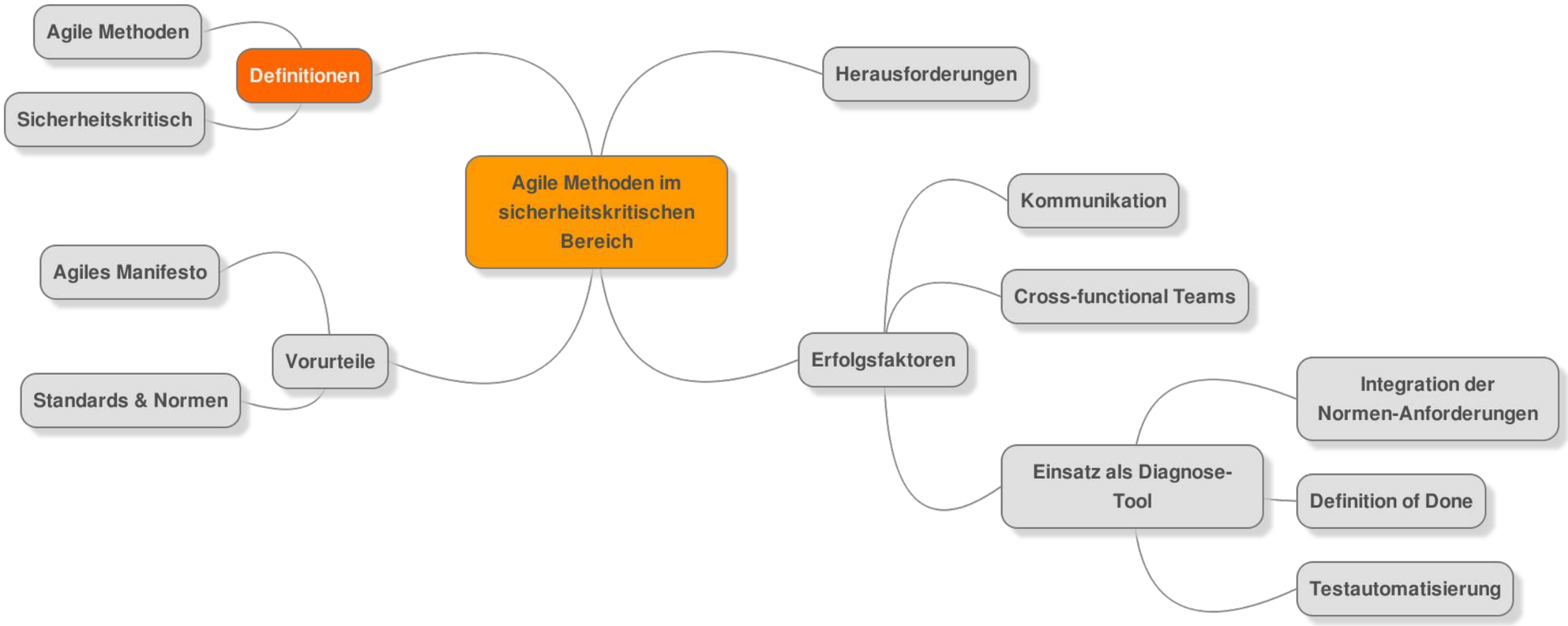
- Berufliche Erfahrung
  - 3 Jahre Projektabwicklung
  - 2 Jahre Product Owner
  - >1 Jahr Consulting

- Agile Schwerpunkte
  - Enterprise Applications
  - Safety-critical Applications

Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

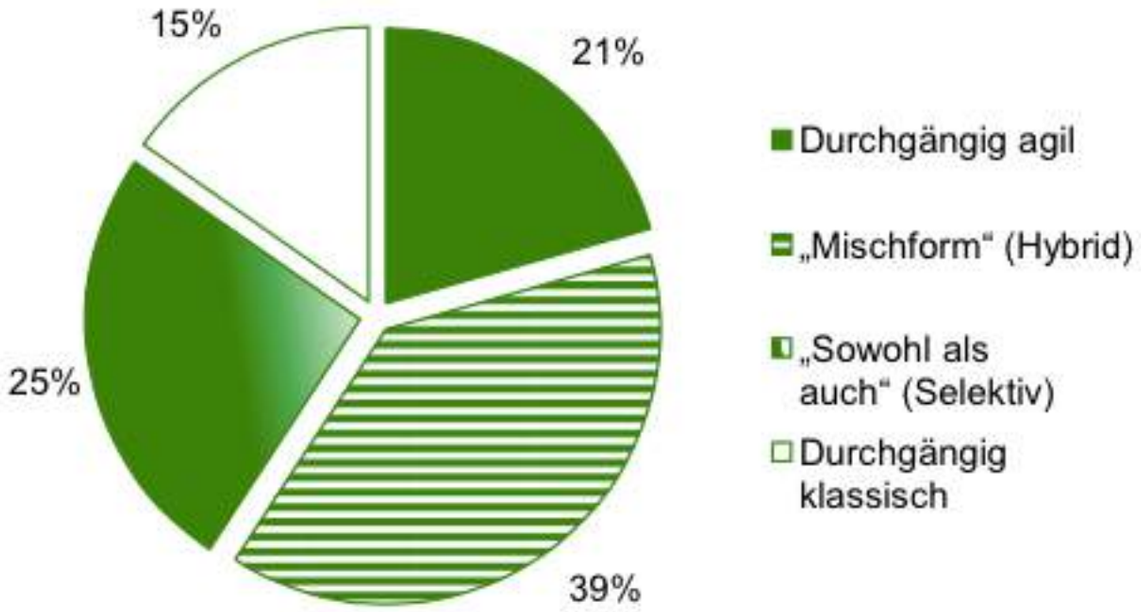
Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Agiles Manifesto
Cross-functional Teams
Vorurteile
Erfolgsfaktoren
Standards & Normen
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

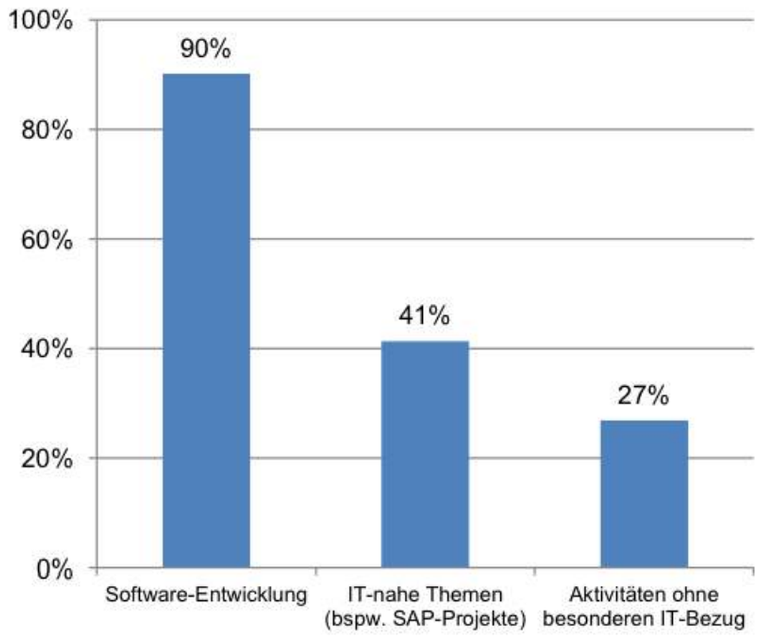
Agile Methoden?

Status Quo Agile 2014

Projekte/Entwicklungsprozesse werden im Tätigkeitsbereich geplant / durchgeführt…



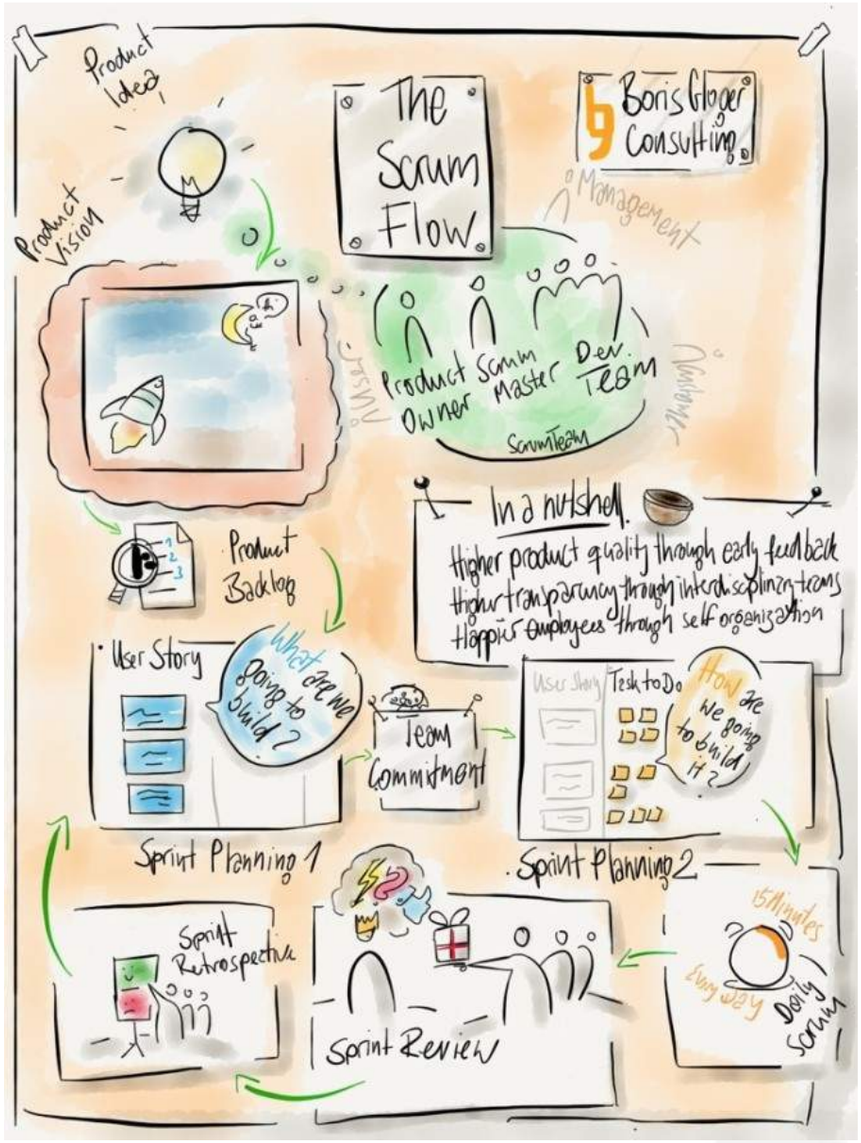
In welchen Themenbereichen nutzen Sie agile Methoden bzw. agiles Projektmanagement?



Status Quo Agile 2014 - Ergebnisbericht
http://www.hs-koblenz.de/rmc/fachbereiche/wirtschaft/forschung-projekte/forschungsprojekte/status-quo-agile/

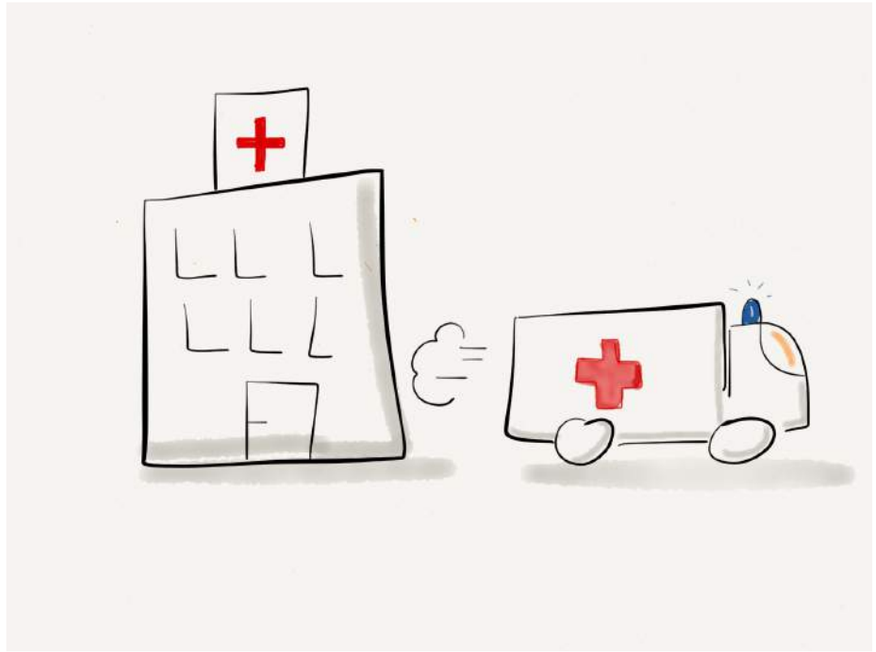
Agile Methoden!

- Populärste Methodik ist Scrum
- Erprobte Vorteile
  - Direkte Kommunikation der involvierten Mitarbeiter
  - Kurze Entwicklungszyklen in Iterationen
  - Kontinuierliche Lieferung eines potentiell nutzbaren Produkts

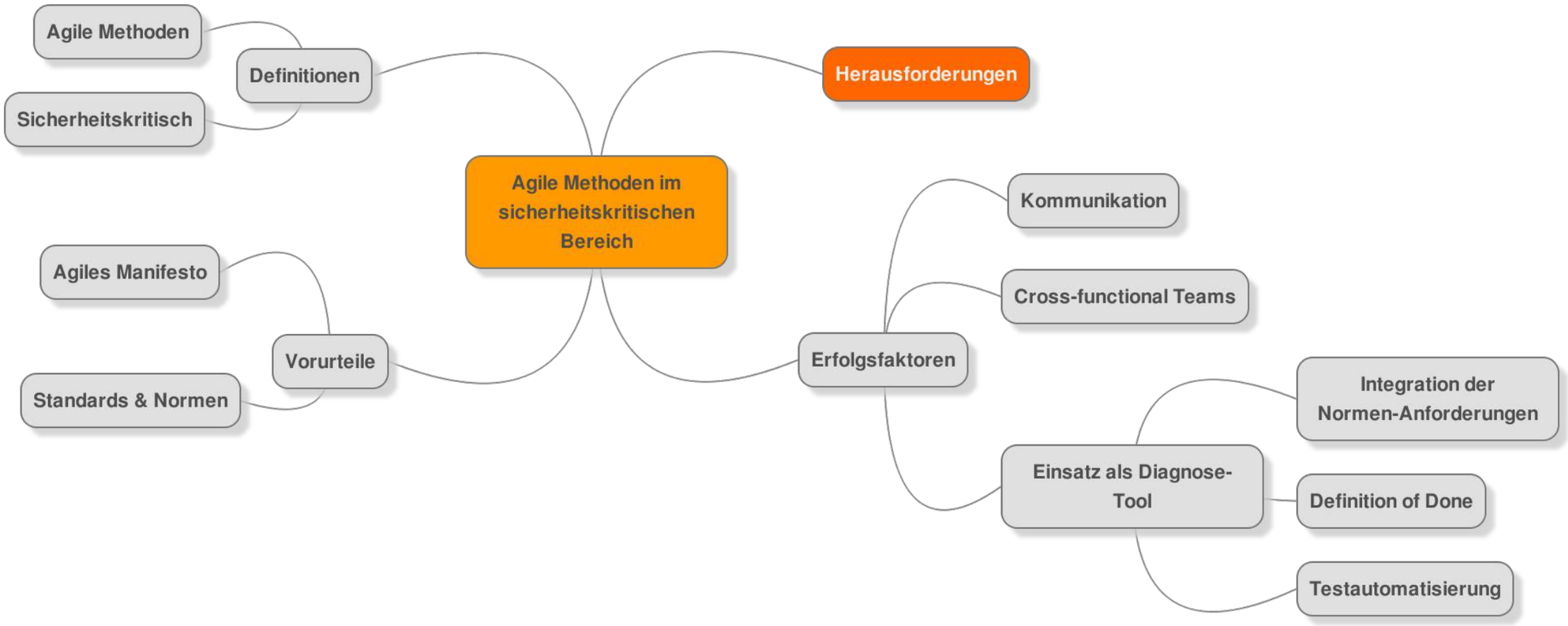


Sicherheitskritscher Bereich?

- Produkt hat im Fehlerfall ein großes Risiko hinsichtlich der Gefährdung von Mensch, Eigentum und/oder Umwelt
- Typische Branchen sind
  - Luft- und Raumfahrt
  - Automotive
  - Medizintechnik
  - Automatisation



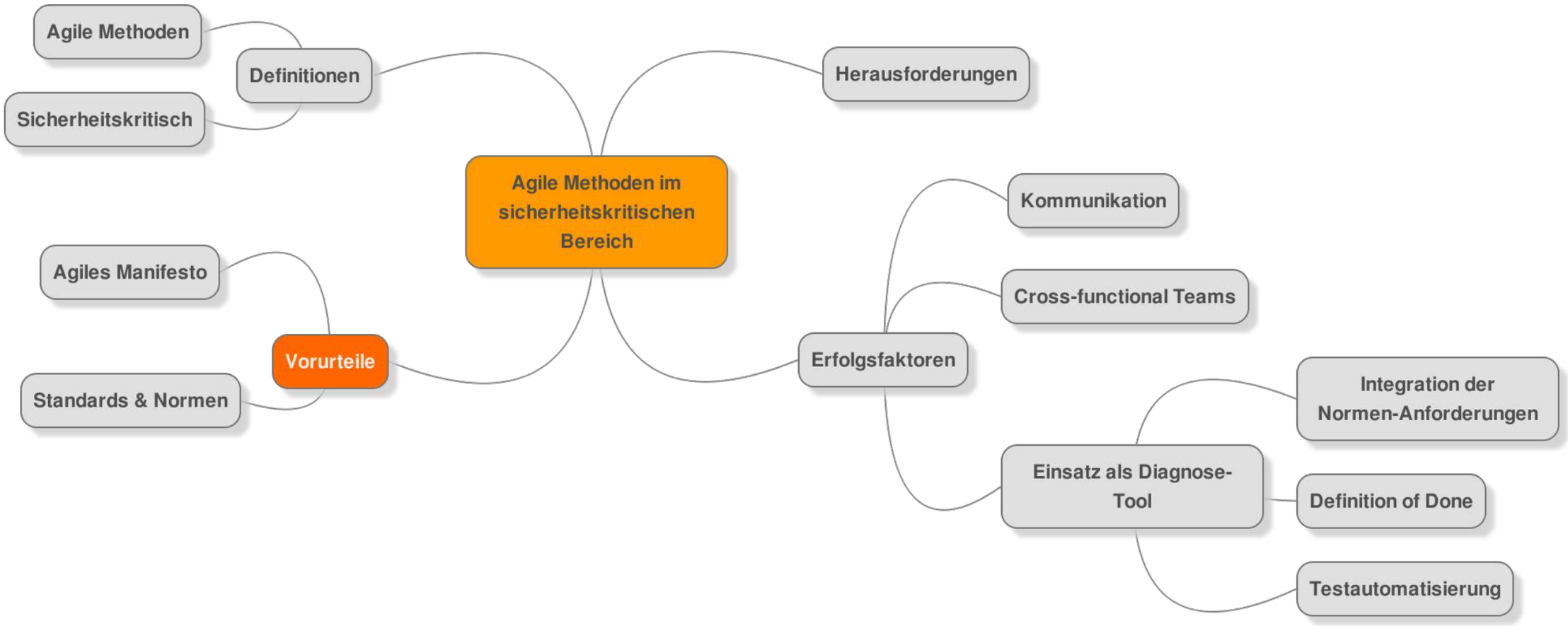
Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Agiles Manifesto
Cross-functional Teams
Vorurteile
Erfolgsfaktoren
Standards & Normen
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Aktuelle Herausforderungen

- Erhöhter Wettbewerb und damit verbundener Kostendruck
- Qualität & Sicherheit genießen weiterhin höchste Priorität
  - … werden aber zunehmend als vorausgesetzt angesehen
- Stärkerer Fokus auf funktionale Anforderungen
- Oft hohe Risikoaversion bezüglich neuer Technologien

Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Die Vorurteile

Agile Prinzipien und sicherheitskritische Entwicklung
Das passt so definitiv nicht, weil ...

- Missverständnis des agilen Manifests
  - Widerspruch in der Priorisierung der Werte
- Schlechte Beispiele von Scrum Implementierungen
  - Vorherrschendes „Chaos“
- Missinterpretation der Normenkonformität
  - Verbot von agilen Vorgehensweisen

Das Agile Manifest (2001)

Wir erschließen bessere Wege, Software zu entwickeln,
indem wir es selbst tun und anderen dabei helfen.
Durch diese Tätigkeit haben wir diese Werte zu schätzen gelernt:

Individuen und Interaktionen mehr als Prozesse und Werkzeuge
Funktionierende Software mehr als umfassende Dokumentation
Zusammenarbeit mit dem Kunden mehr als Vertragsverhandlung
Reagieren auf Veränderung mehr als das Befolgen eines Plans

Das heißt, obwohl wir die Werte auf der rechten Seite wichtig finden,
schätzen wir die Werte auf der linken Seite höher ein.

Das Agile Manifest (2001)

Wir erschließen bessere Wege, Software zu entwickeln,
indem wir es selbst tun und anderen dabei helfen.
Durch diese Tätigkeit haben wir diese Werte zu schätzen gelernt:

Individuen und Interaktionen mehr als Prozesse und Werkzeuge
Funktionierende Software mehr als umfassende Dokumentation
Zusammenarbeit mit dem Kunden mehr als Vertragsverhandlung
Reagieren auf Veränderung mehr als das Befolgen eines Plans

Das heißt, obwohl wir die Werte auf der rechten Seite wichtig finden,
schätzen wir die Werte auf der linken höher ein.

Zentrale Prinzipien von Safety

Das Agile Manifest (2001)

Wir erschließen bessere Wege, Software zu entwickeln,
indem wir es selbst tun und anderen dabei helfen.
Durch diese Tätigkeit haben wir diese Werte zu schätzen gelernt:

Individuen und Interaktionen mehr als Prozesse und Werkzeuge
Funktionierende Software mehr als umfassende Dokumentation
Zusammenarbeit mit dem Kunden mehr als Vertragsverhandlung
Reagieren auf Veränderung mehr als das Befolgen eines Plans

Das heißt, obwohl wir die[illegible] der rechten Seite wichtig finden,
schätzen wir di[illegible]inken Seite höher ein.

Erfolgsfaktoren
„jeder“ Entwicklung

Bedeutung der Normen

- Unterschiedlichste Normen
  - Branchenspezifisch

EN 61508

ISO 26262

DO-178C

EN 50128

IEC 62304

- Meist keine Vorschrift der Entwicklungsmethodik
  - Vorschrift eines festgesetzten & definierten Prozess
- ABER: Anforderungen an den Entwicklungsprozess orientieren sich an den traditionellen Phasen

Bedeutung der Normen

EN 61508 | ISO 26262 | DO-178C | EN 50128 | IEC 62304

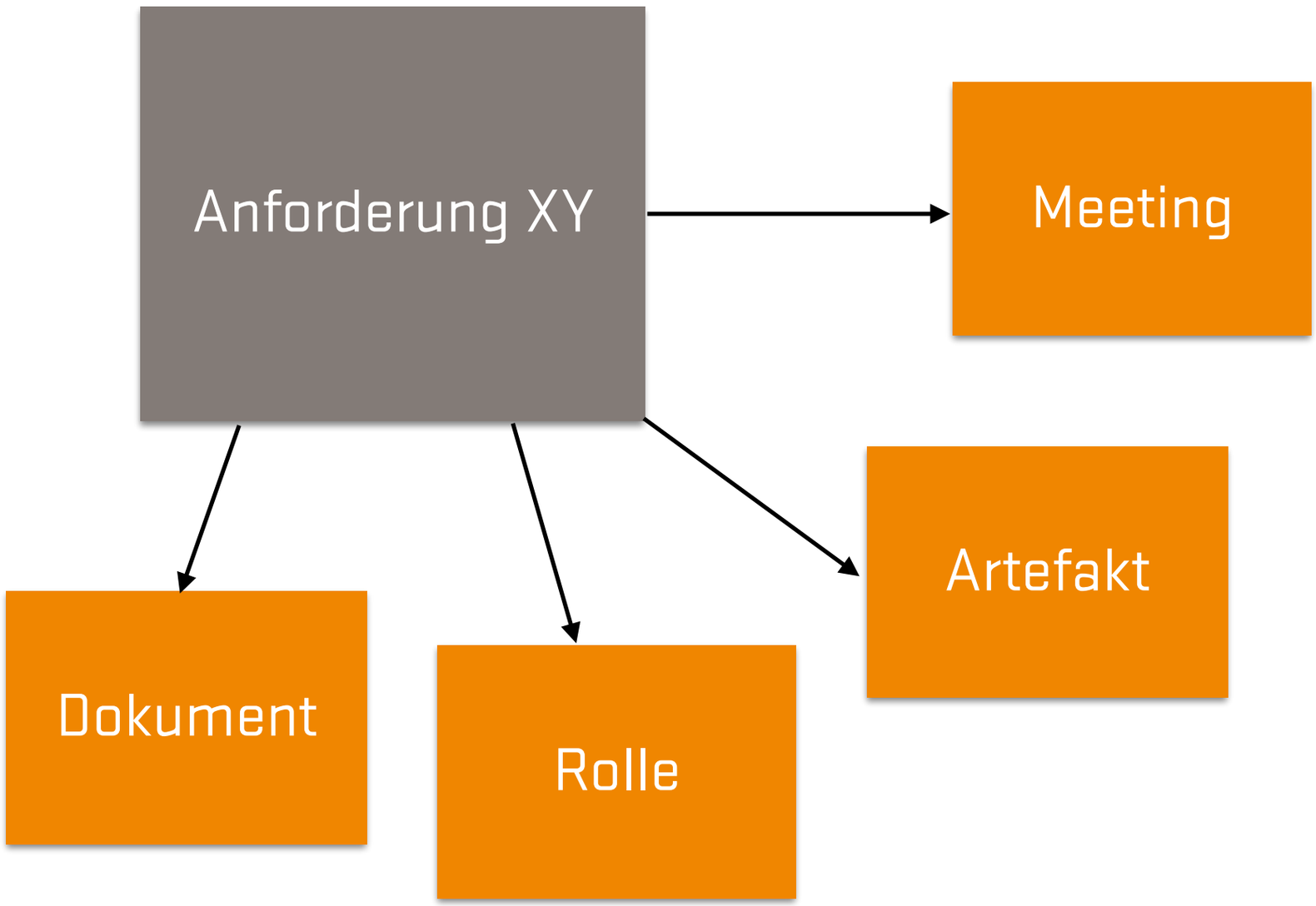
› Aus der Norm...

„Diese Norm schreibt dem Hersteller keine Organisationsstruktur vor oder welcher Teil der Organisation welchen Prozess, welche Aktivität oder welche Aufgabe durchführen soll. Diese Norm fordert nur, dass der Prozess, die Aktivität oder die Aufgabe durchgeführt wird, um die Einhaltung dieser Norm nachzuweisen.
Diese Norm macht keine Vorgaben für die Bezeichnung, das Format oder den expliziten Inhalt der Dokumentation, die zu erstellen ist. Diese Norm erfordert eine Dokumentation der Aufgaben, aber die Entscheidung, wie diese Dokumentation gestaltet wird, wird dem Benutzer der Norm überlassen.

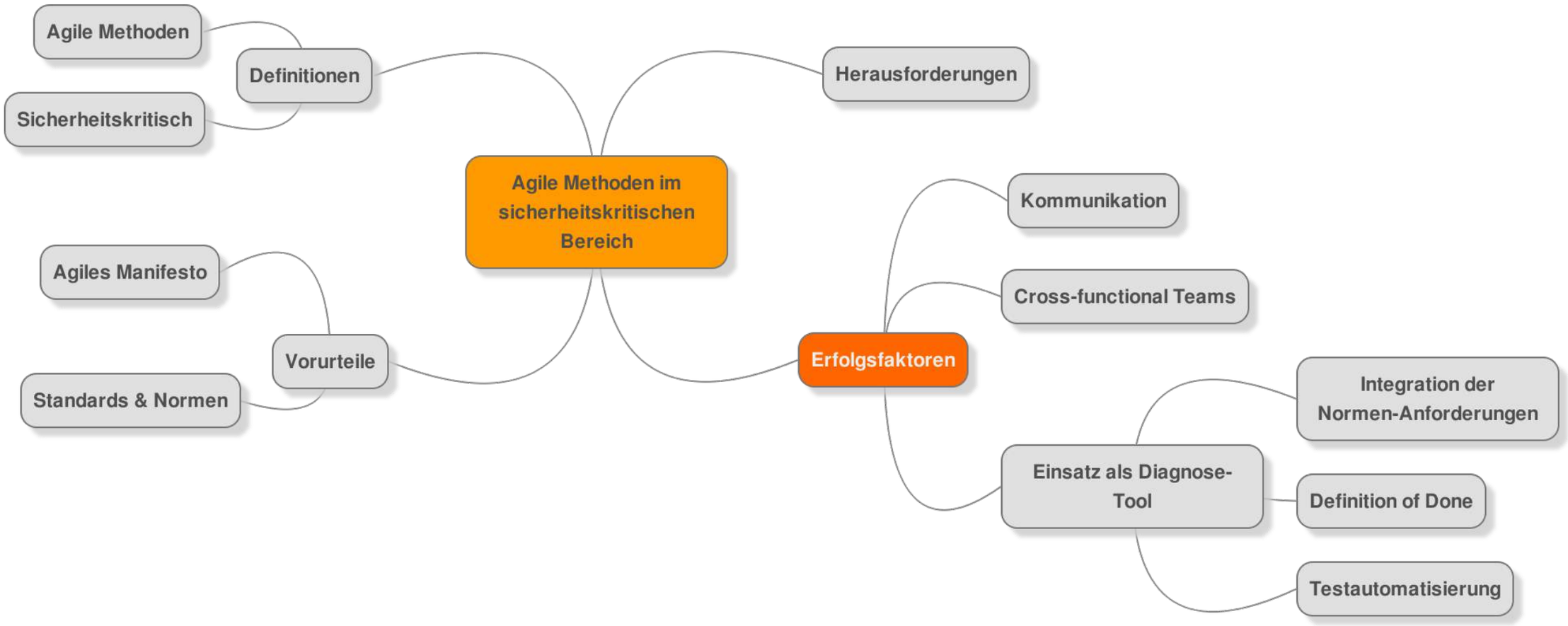
Diese Norm schreibt kein spezifisches Lebenszyklus-Modell vor. Die Anwender dieser Norm sind verantwortlich für die Auswahl eines Lebenszyklus-Modells für das Software-Projekt und für das Abbilden der Prozesse, Aktivitäten und Aufgaben dieser Norm auf dieses Modell.“

IEC 62304

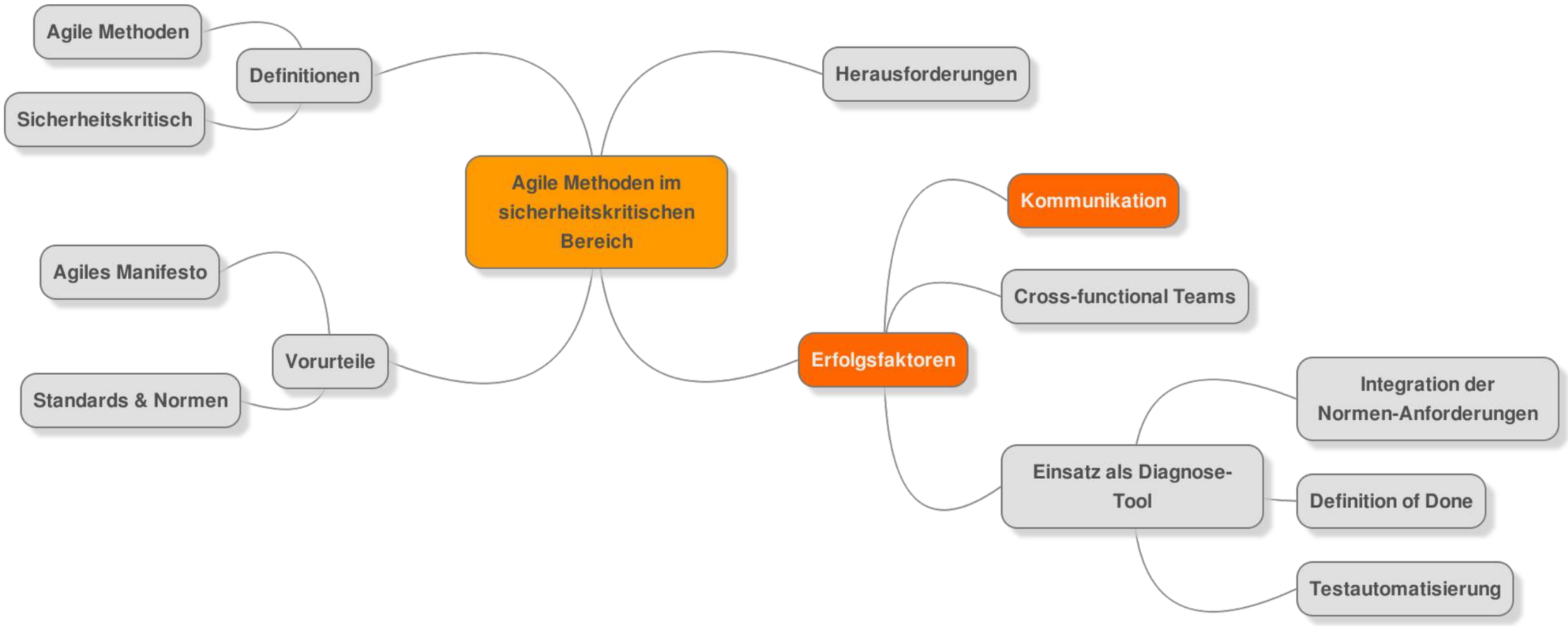
Beispiel: Mapping



Agenda

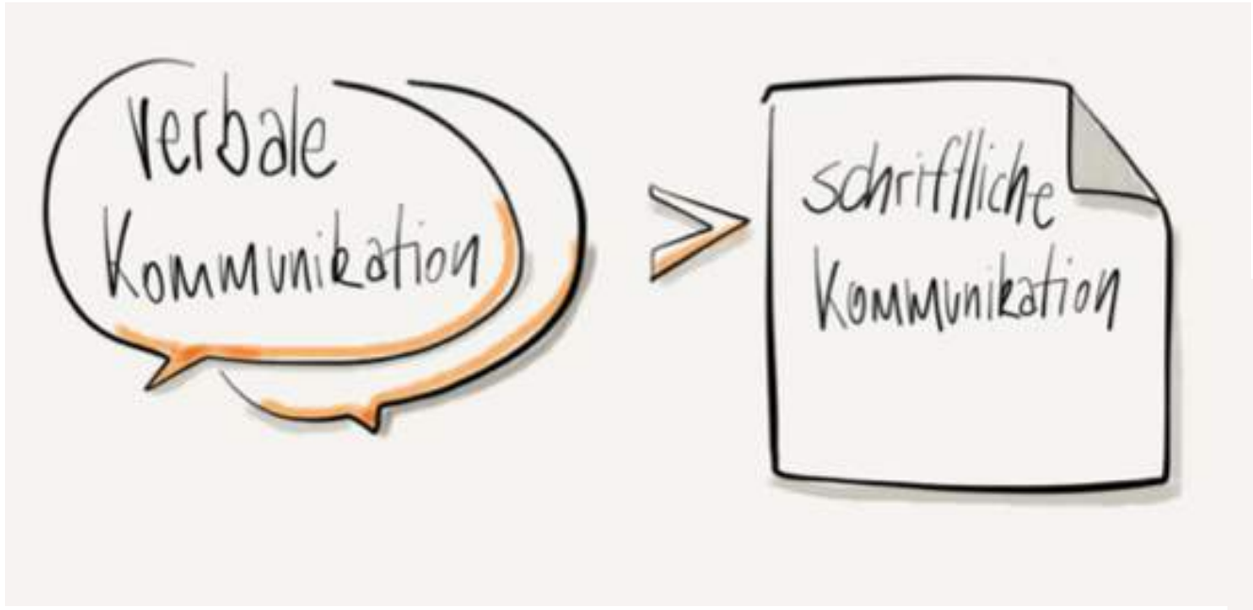

Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Agenda

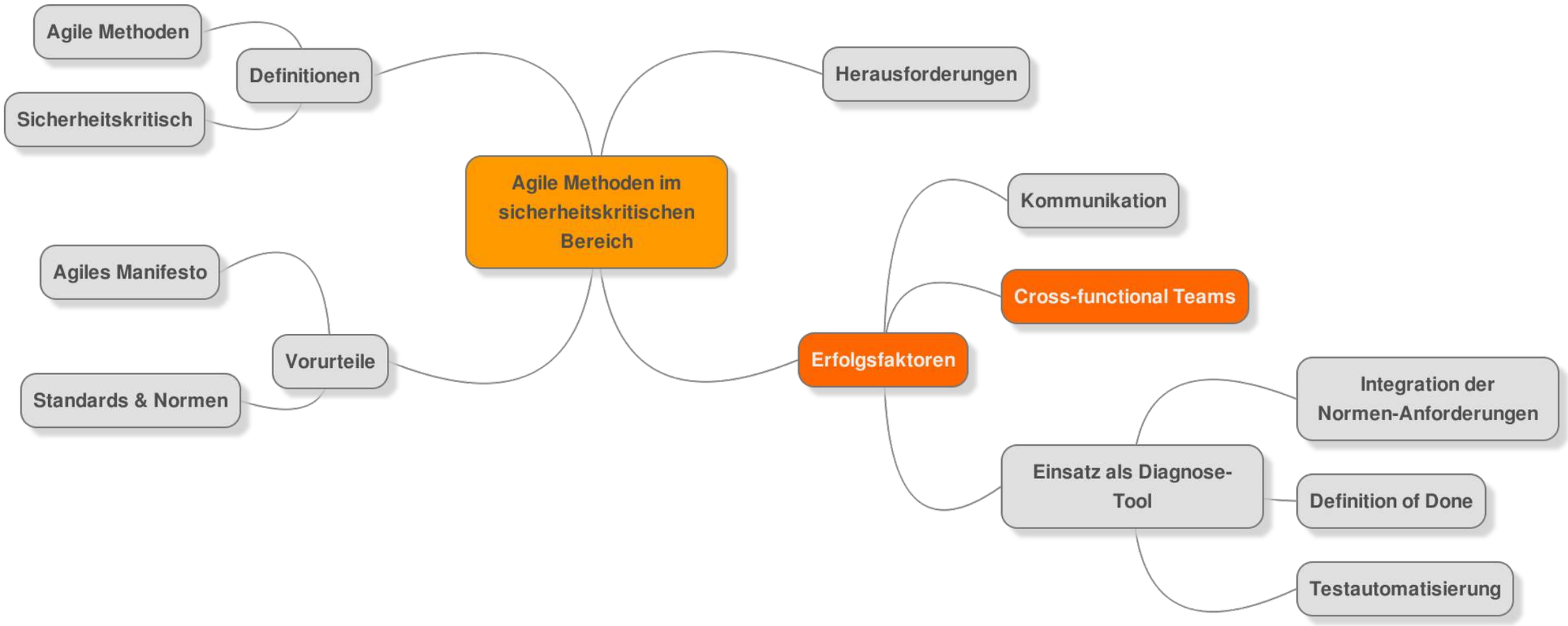

Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Agiles Manifesto
Cross-functional Teams
Vorurteile
Erfolgsfaktoren
Standards & Normen
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Individuen, Interaktion und Zusammenarbeit

Die User Story als ein Versprechen für ein Gespräch

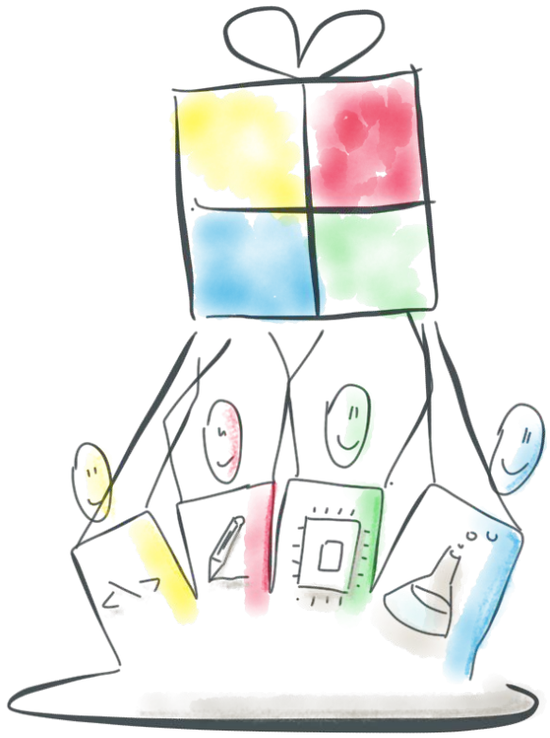


Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

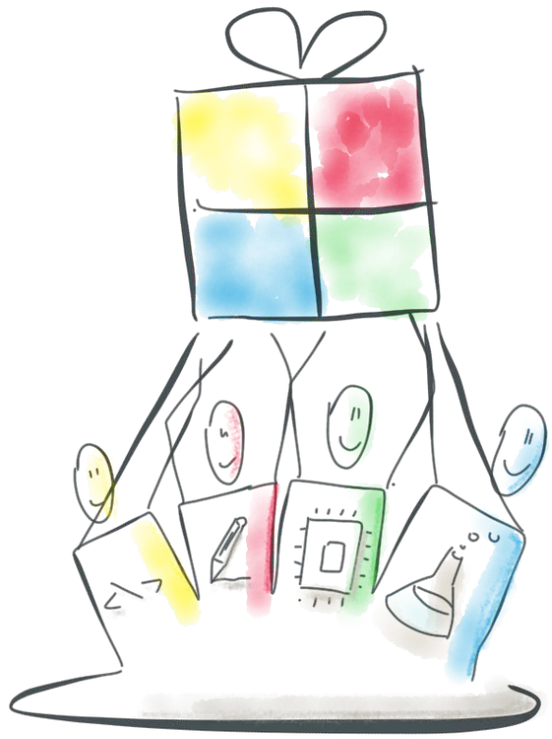
Experten in die Teams

- **Cross-funktional:** Entwicklungsteam besitzt alle für die Lieferung benötigten Skills
- Integration der Qualitäts- & Safety Experten
- Vorteile
  - Stärkere Identifizierung mit dem Produkt
  - Schaffen eines Sicherheitsbewusstseins im ganzen Team

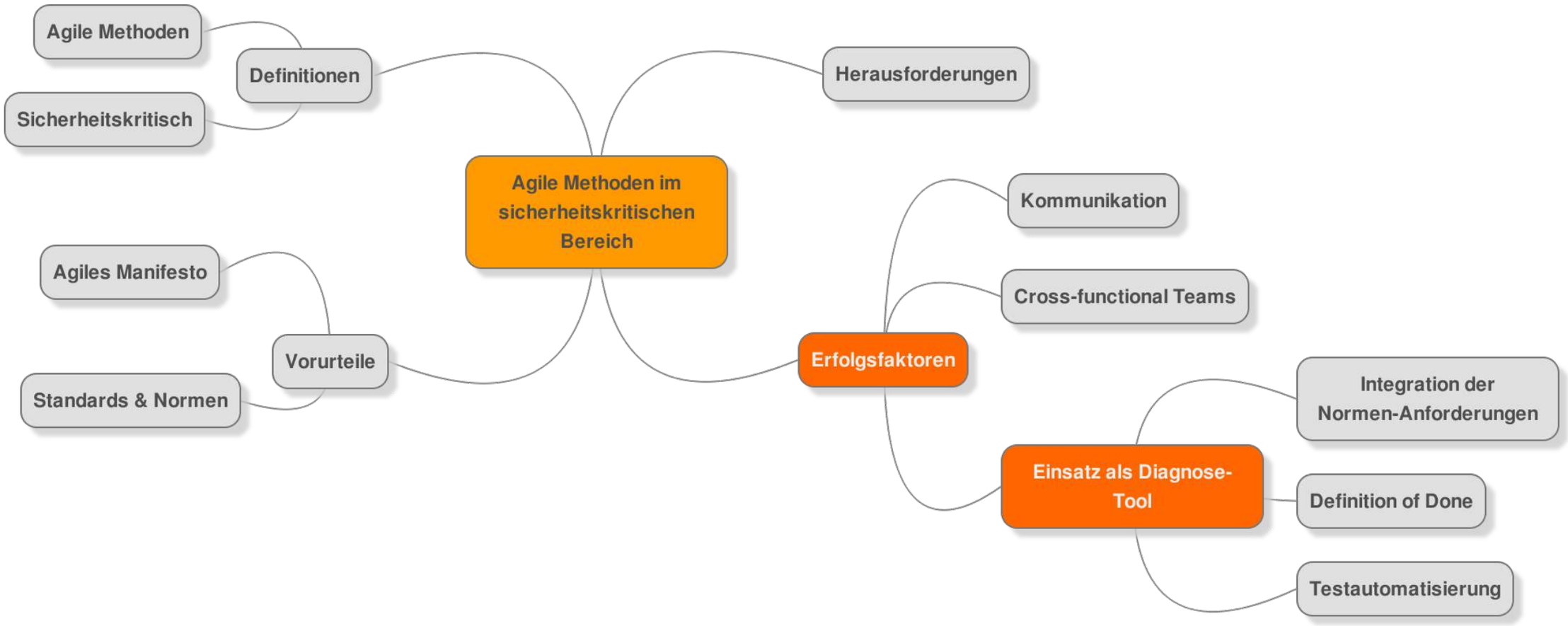


Motivation der Betroffenen

- Verstehen der Anforderungen
  - Warum werden diverse Analysen benötigt?
- Leben eines Qualitäts- und Sicherheitsbewusstseins
- anstatt sturer Abarbeitung der Vorschriften

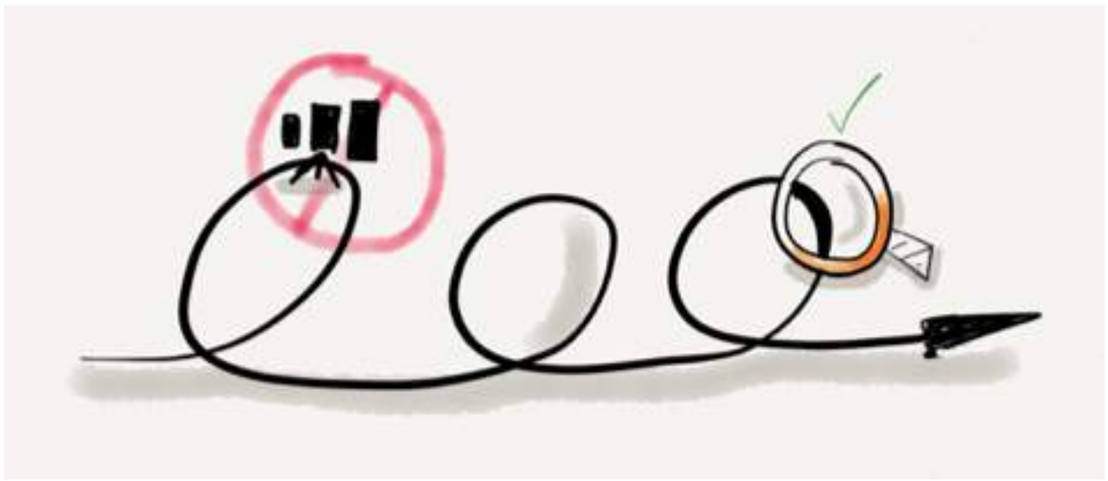


Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Integration in Sprintzyklen

- Integration der Anforderungen sicherheitskritischer Systeme in die Sprintzyklen
  - Fokus auf kontinuierliche Aktualisierung
  - Auswirkung auf die „Velocity“

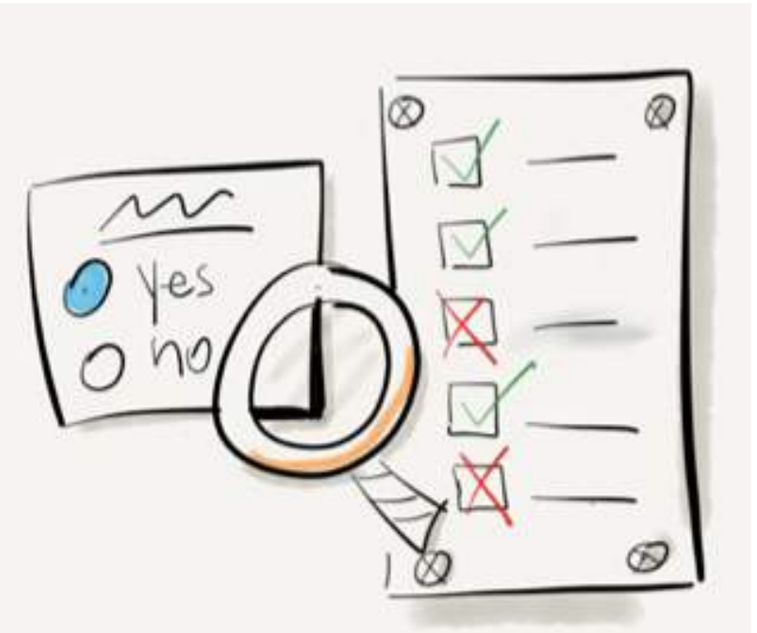


Diagnose-Tool

- Sicherung von geprüften Lieferungen
  - durch eine geeignete Definition of Done

Definition of Done

- Kriterien für abgeschlossene User Stories
  - Nachhaltige Sicherung der Qualität
- Inhalt: Vorgaben und freiwillige Zusagen
  - Vorgaben: Unternehmensrichtlinien, Kundenanforderungen, rechtliche Aspekte, …
  - Freiwillige Zusagen sind vom Entwicklungsteam
- Überprüfte Lieferung am Ende eines Sprints
  - Nur „fertige“ User Stories werden im Review vorgestellt



Beispiel: Definition of Done

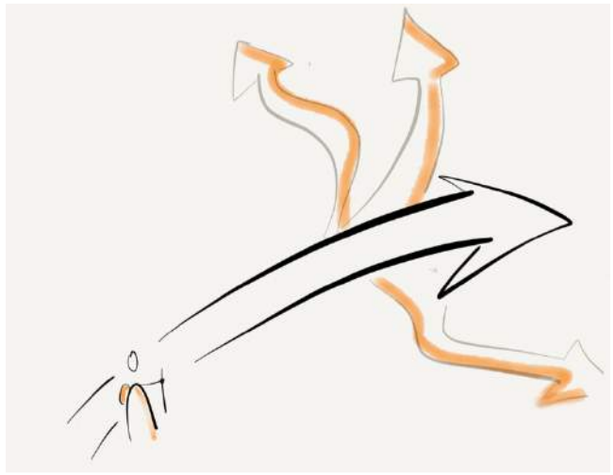
› Software für Flugsicherung

Dokumentation der User Stories (Requirements) in Tool XY
Durchführung und Dokumentation der Impact Analyse
Durchführung und Dokumentation der Software Hazard Analyse
Durchführung und Dokumentation der Fault Tree Analyse auf betroffenen Modulen
Aktualisierung des System Design Dokuments
(Optionale) Aktualisierung des Interface Design Dokuments
Implementierung der Unit Tests und Sicherstellung Traceability zu User Story
Implementierung des Quellcodes und Sicherstellung Traceability zu User Story
(Optionale) Aktualisierung der Installationsroutinen
Identifizierung von geeigneten Akzeptanztests und Überprüfung auf Automatisierbarkeit
Durchführung und Dokumentation der Akzeptanztests plus Freetests („Brechen der Software“)
Dokumentation der Änderungen für die Benutzerdokumentation

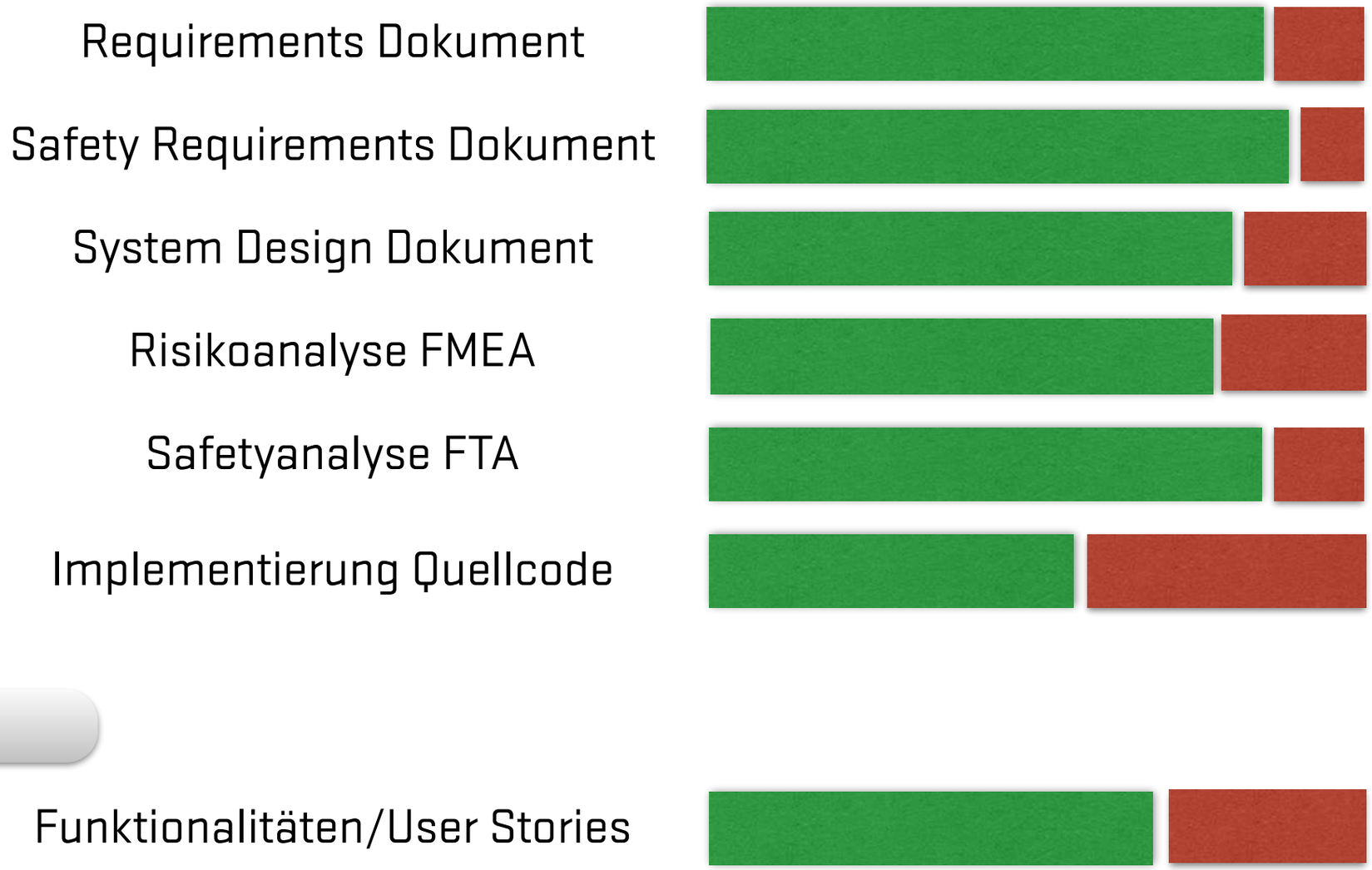
Diagnose-Tool

- Sicherung von geprüften Lieferungen
  - durch eine geeignete Definition of Done
- Verbesserte Fortschrittsmessung des Projektes
  - durch Konsolidierung der diversen Arbeitsprodukte auf Funktionalitäten

Fortschrittsmessung



Traditionell



Agil

Diagnose-Tool

- Sicherung von geprüften Lieferungen
  - durch eine geeignete Definition of Done

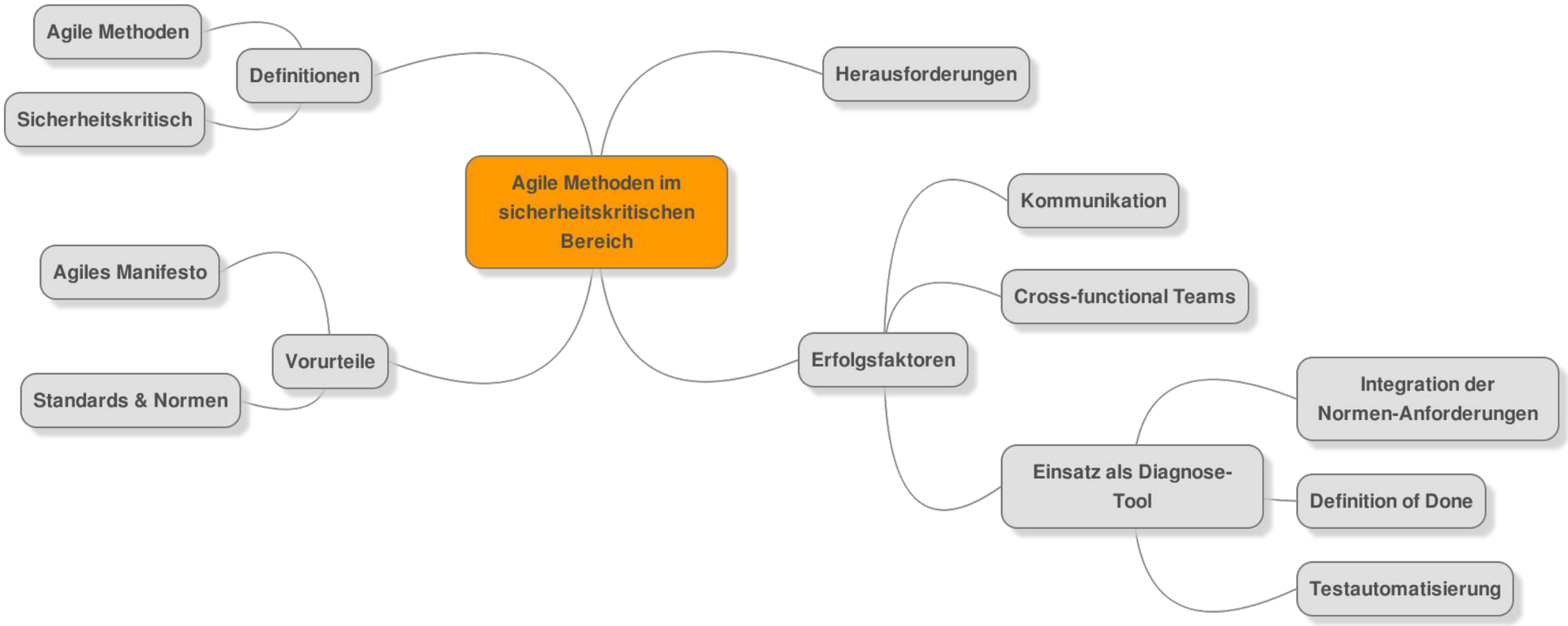
- Verbesserte Fortschrittsmessung des Projektes
  - durch Konsolidierung der diversen Arbeitsprodukte auf Funktionalitäten

- Kontinuierliche Verifikation der Funktionstüchtigkeit
  - durch flächendeckende automatisierte Tests

Testautomatisierung

- „Absicherung“ der Software
  - Ermöglichung kontinuierlicher Weiterentwicklung
- Agile Software Engineering Praktiken
  - Test-Driven Development
  - Automatisierte Acceptance Tests
  - Continuous Integration
- Reduzierung des manuellen Aufwands für umfassende Tests vor Auslieferung

Agenda


Agile Methoden
Definitionen
Sicherheitskritisch
Herausforderungen
Agile Methoden im sicherheitskritischen Bereich
Kommunikation
Cross-functional Teams
Agiles Manifesto
Vorurteile
Standards & Normen
Erfolgsfaktoren
Integration der Normen-Anforderungen
Einsatz als Diagnose-Tool
Definition of Done
Testautomatisierung

Conclusio

- Agile Methoden im sicherheitskritischen Bereich sind möglich & sinnvoll
- Voraussetzung sind ein definierter Entwicklungsprozess und Disziplin
- Alle Experten müssen in das Entwicklungsteam eingebunden werden
- Jeder Sprint dient als Diagnose für den Fortschritt der geprüften Lieferung

BORIS GLOGER®

www.borisgloger.com