SECURITY FOR SAFETY & SECURE DEVELOPMENT

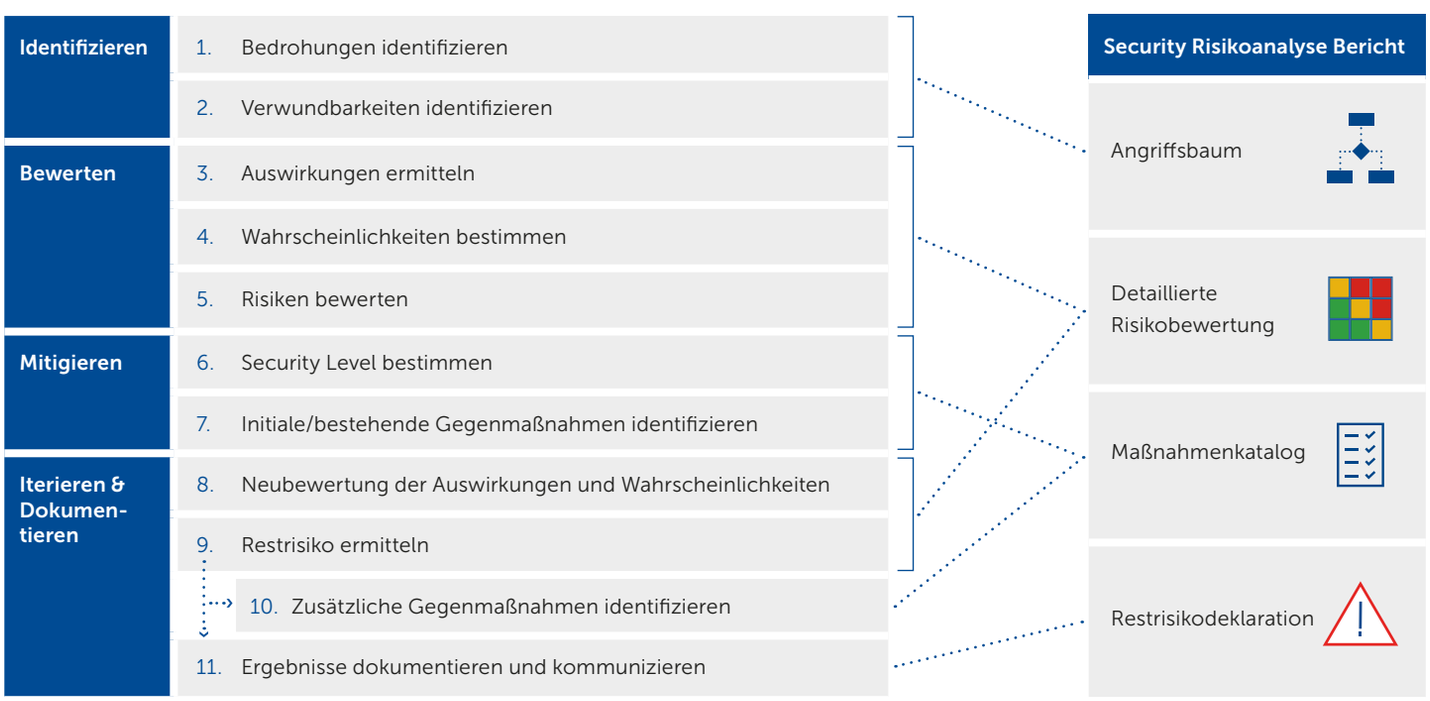
Ganzheitliche Security Risikoanalysen

Detaillierter Workflow: ISA/IEC 62443-3-2

› Identifizieren, bewerten, mitigieren und dokumentieren

Besondere Anforderungen

› Systematik und Vollständigkeit: Alle Angriffsvektoren müssen erfasst werden
› Berücksichtigung von technischen, organisatorischen und infrastrukturellen Aspekten
› Dynamik: Effiziente Erweiterungen und Anpassungen müssen möglich sein
› Übersichtlichkeit und Visualisierung: Wichtige Diskussionsgrundlage für Workshops mit Systemexperten



Arbeitspakete & Lieferobjekte

1 PLANUNG

Identifikation der **gesetzlichen und normativen Basis**
› **Beschreibung** des zu analysierenden **Systems**
› **Zieldefinition** gemeinsam mit allen Stakeholdern

› Definition der **Rollen und Verantwortlichkeiten**
› **Planung** der Inhalte weiterer Lieferobjekte
› Identifikation der **Synchronisationspunkte mit Safety**

Security Management Plan

2 RISIKOANALYSE

Identifikation von **Bedrohungen** und **Sicherheitslücken**
› **Bewertung** anhand von Eintrittswahrscheinlichkeiten und Auswirkungen
› Alle Risiken werden miteinander verglichen und in einer **Risikomatrix** kategorisiert
› Für Risiken oberhalb eines Toleranzniveaus werden **zusätzliche Schutzmaßnahmen** berücksichtigt

Security Risk Assessment Report

Arbeitspakete & Lieferobjekte

3 MASSNAHMENKATALOG

Erfüllung **Security Level Target**
› **Gap-Analyse** zum Maßnahmenkatalog der **ISA/IEC 62443** für das gewählte Security Level Target

ODER

Risikobasierter Ansatz
› Definition von Maßnahmen zur **Reduktion der größten Risiken** basierend auf **ISA/IEC 62443**
› Definition von Security-related Application Condtions

Maßnahmenkatalog & Umsetzungsplan

4 IMPLEMENTIERUNG & TEST

Beratung bei **Priorisierung und Umsetzung**
› Optimierung der Sicherheit bezüglich **Technik, Organisation und Infrastruktur** durch Implementierung der Maßnahmen basierend auf dem Maßnahmenkatalog und Umsetzungsplan
› Überwachung der Implementierungsmaßnahmen und Abschlusstest

Abnahmebericht

5 SECURITY NACHWEIS

Überblick und Verweise auf vorangegangene Security Aktivitäten
› Dokumentation der **Nachweise** aus der **Verifikation** und **Validierung**

› **Adressierung offener Punkte** mittels Security-related Application Conditions
› Übersicht über alle Restrisiken
› Abschließender **Security Anspruch**

Security Case

6 BETRIEBSFÜHRUNG

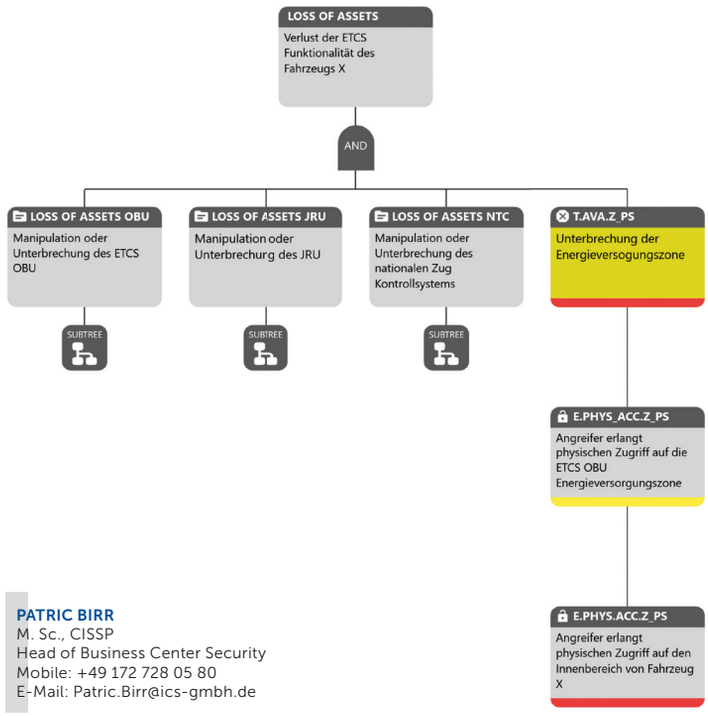
Sicherer Betrieb von **Technik, Organisation und Infrastruktur**
› Identifikation von Optimierungspotenzialen
› Kontinuierliche Verbesserung der Prozesse

› Beratung bei der Betriebsführung
› Einhaltung der Security-Vorgaben über den gesamten Lebenszyklus

Betriebsführungskonzept

Attack Tree Analysis

› Top-Down-Ansatz zur Identifizierung und Visualisierung möglicher Angriffspfade
› Grundlage für technische Diskussionen mit System- und Sicherheitsexperten
› Ganzheitliche Abbildung komplexer Angriffe durch Bewertung jedes Angriffsschrittes
› Top-Down Analyse anhand der Systemarchitektur
› Detaillierte Analysen in separaten Teilbäumen



Referenzen

› DB: Security Management iLBS (integriertes Leit- und Bediensystem), seit Q4/16, 6 BC SEC Mitarbeiter
› Deutscher Hersteller: Security Management im ETCS-OBS Entwicklungsprojekt, seit Q4/18, 5 MA
› Britischer Fahrzeugintegrator: Security Management im Retrofit Integrationsprojekt, seit Q1/20, 4 MA
› Deutscher Hersteller: Security Management im Stellwerksumfeld, seit Q2/21, 3 MA
› Siemens Mobility: Security LST Architektur Review, Q2/19 – Q1/20, 2 MA
› SBB ESTW Security Risk Assessment, Q2/18 – Q4/19, 3 MA

PATRIC BIRR
M. Sc., CISSP
Head of Business Center Security
Mobile: +49 172 728 05 80
E-Mail: Patric.Birr@ics-gmbh.de