Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH

RTR

Branchenrisikoanalyse Telekommunikation

Ulrich Latzenhofer

RTR-GmbH

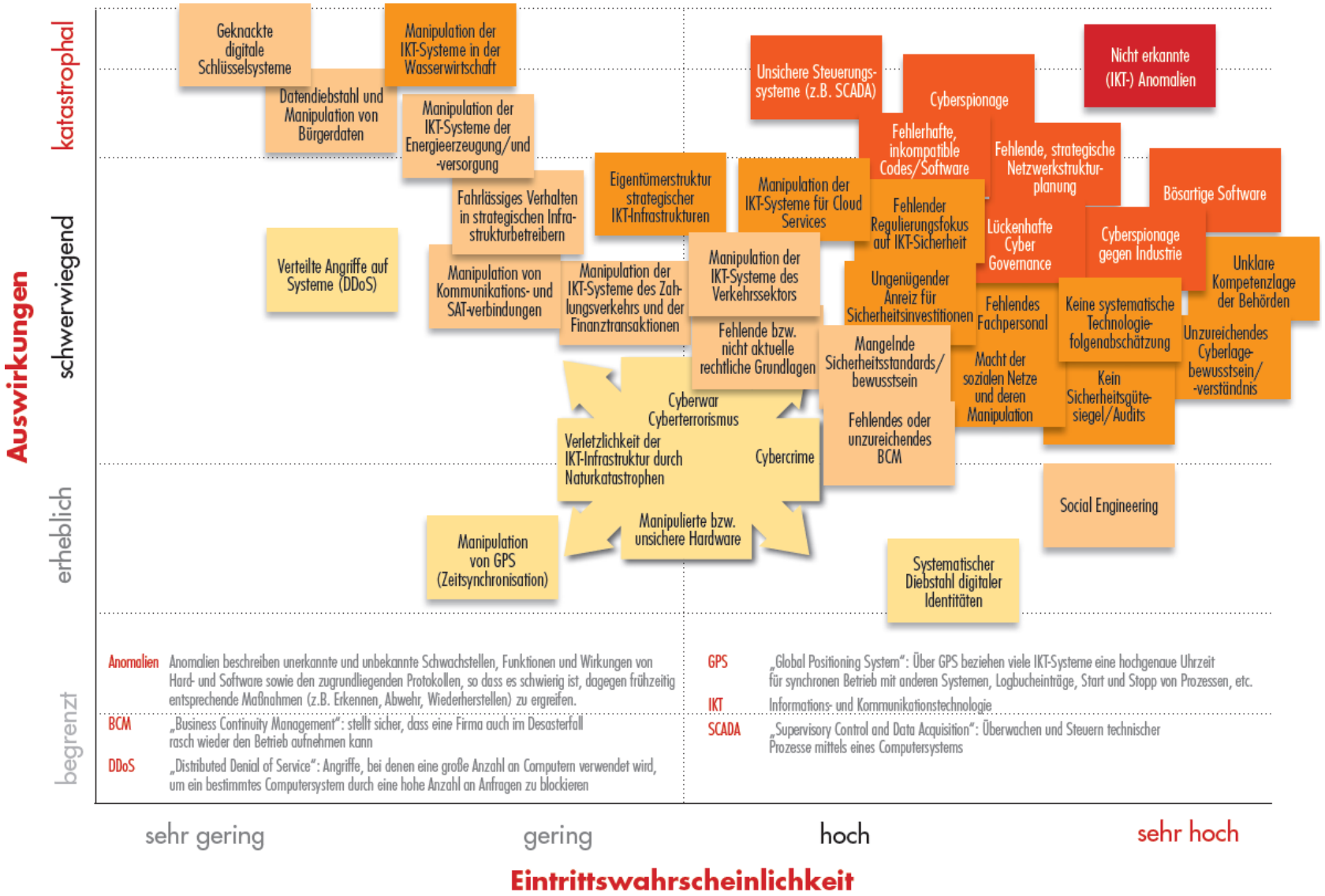
17.10.2016

Inhalt

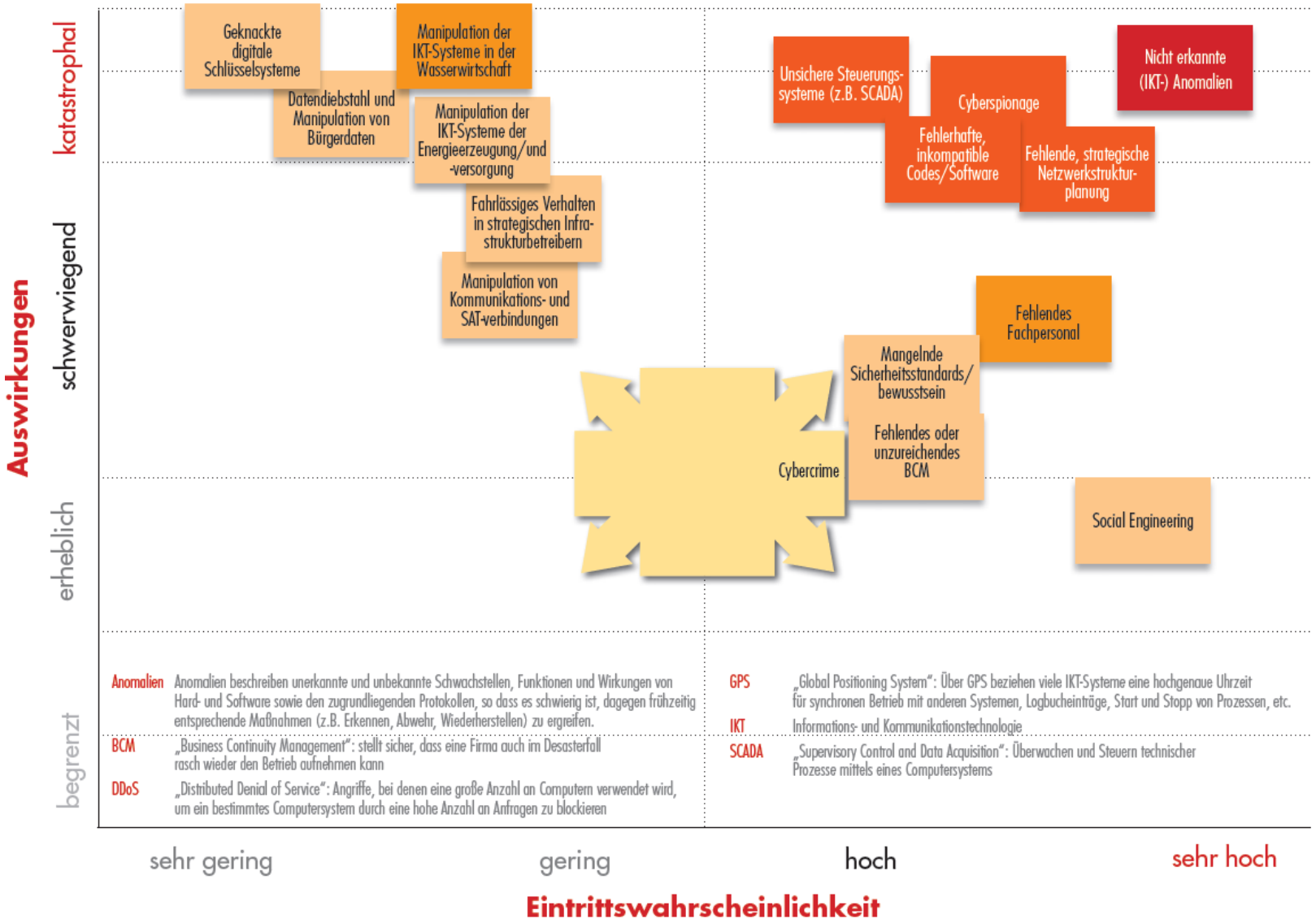
- Kontext
- Standards
- Arbeitsprogramm
- Organisatorische Struktur

Kontext

KSÖ Cyber-Risikomatrix 2011: „Bandbreite“ der Risiken



KSÖ Cyber-Risikomatrix 2011: Top 15 im Bereich IKT



Österreichische Strategie für Cyber-Sicherheit 2013

Risikoanalysen für sektorspezifische Cyber-Bedrohungen

- Basis von Krisen- und Kontinuitätsmanagementplänen
- Teil der integrierten Cyber-Sicherheitspolitik: Zusammenarbeit von öffentlichen Einrichtungen, Wirtschaft (insbesondere Betreibern kritischer Infrastrukturen), Wissenschaft und Zivilgesellschaft
- Ausarbeitung und laufende Aktualisierung

Risikomanagement

- Umfassende Sicherheitsarchitektur (Risiko- und Krisenmanagement) für Betreiber kritischer Infrastrukturen
- Branchentypische Risikomanagementpläne auch für KMU in Abstimmung mit staatlichen Krisen- und Kontinuitätsmanagementplänen
- Maßnahmen zur Erhöhung des Schutzniveaus in ausgeglichenem Verhältnis zum jeweiligen Risiko

Österreichisches Programm zum Schutz kritischer Infrastrukturen 2014

Risikomanagement für strategische Unternehmen

- Risikoanalyse
- Maßnahmen zum Umgang mit Risiken

Staatliche Risikoanalysen

- Durchführung von Risikoanalysen branchenweise
- Abstimmung mit Methoden und Verfahren der Nationalen Risikoanalyse
- Orientierung an internationalen Standards
- Grundlage für Festlegung von Schutzstandards für strategische Unternehmen und Planung weiterer Maßnahmen (Lagebilder etc.)
- Grundlage für Information und Beratung strategischer Unternehmen durch Sicherheitsbehörden
- Grundlage für Entwicklung generischer Maßnahmen zur Reduzierung identifizierter Risiken

Risikoanalyse für Systeme der Elektrizitätswirtschaft 2014

Risikoanalyse für Systeme der Elektrizitätswirtschaft 2014: Methodik

- **Gefahrenidentifikation:** Identifikation von Gefahren infolge Störung von Verfügbarkeit, Vertraulichkeit und Integrität von Kommunikation
- **Gefahrenfelder:** Gliederung der Kommunikationsbeziehungen in 15 Bereiche
- **Gefahrenanalyse:** Identifikation, Zuordnung und Analyse von 114 Einzelgefahren
- **Bewertung von Risiken:** Festlegung von Bewertungskriterien, Bewertung der 114 Gefahren zu 73 Einzelrisiken, Aggregation zu 19 Aggregationsrisiken
- **Erarbeitung von Maßnahmen** prioritär zur Verringerung von Risiken, die im worst case über einer formal definierten Toleranzgrenze liegen
- **Risiken überprüfen** durch iterative Abstimmung in der Projektgruppe
- **Risikobericht** als Zusammenfassung des abgestimmten Sachstands
- **Periodische Revision** für kontinuierlichen Verbesserungsprozess

Standards

ISO 31000 – Risikomanagement

Familie von Normen im Zusammenhang mit Risikomanagement

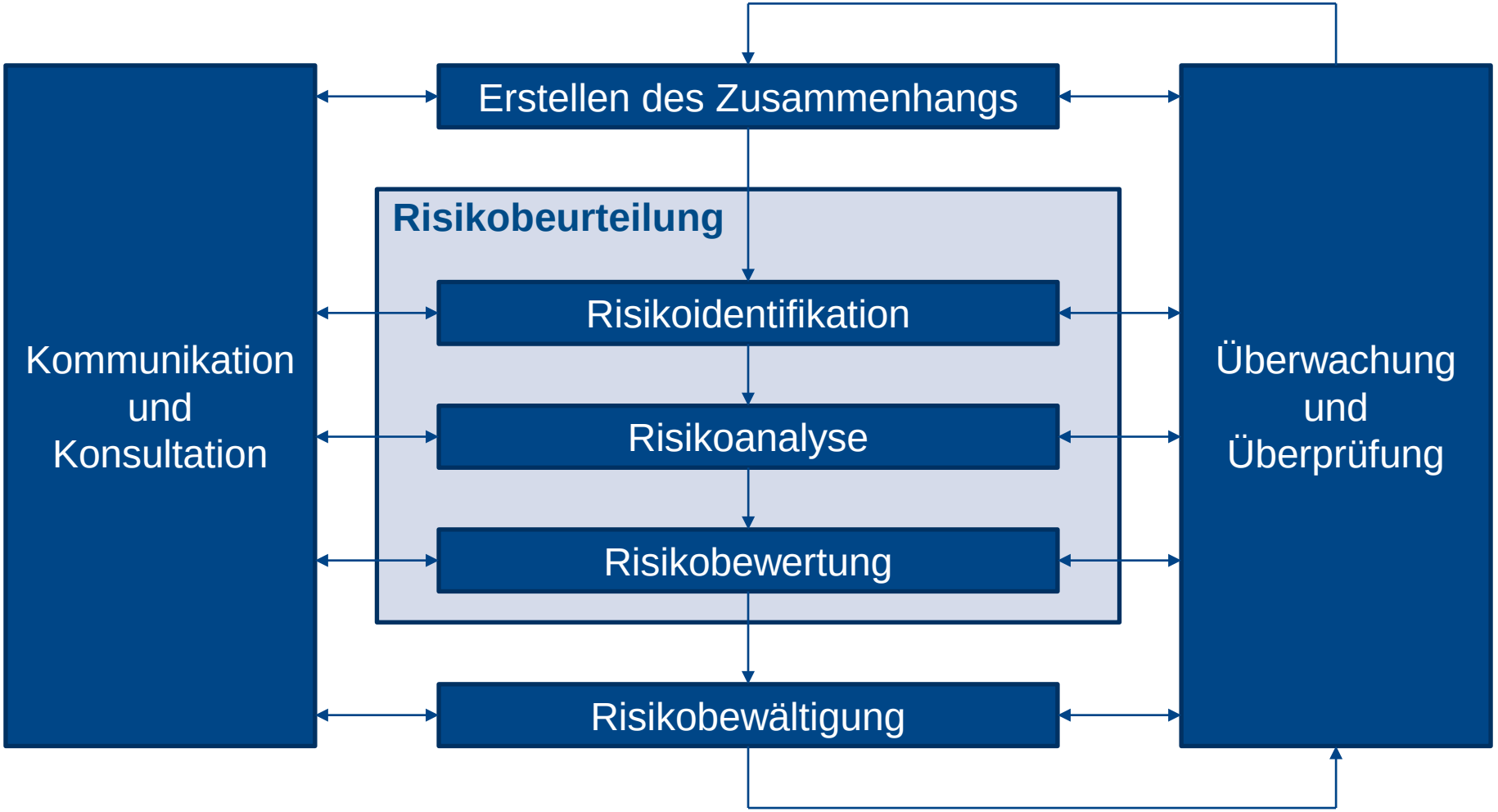
- ISO 31000:2009 – Risk management – Principles and guidelines
- IEC 31010:2009 – Risk management – Risk assessment techniques
- ISO Guide 73:2009 – Risk management – Vocabulary

Managementsystem für Design, Implementierung, Wartung und Verbesserung von Risikomanagementprozessen

Universeller, aber generischer Ansatz: für jede „Zielgruppe“, für alle Gegenstände von Risikoanalysen

Begriff Risiko: nicht mehr „Wahrscheinlichkeit des Verlusts“, sondern „Auswirkung von Unsicherheit auf Ziele, Tätigkeiten und Anforderungen“

Risikomanagement nach Grundsätzen von ISO 31000



IEC 31010 – Verfahren zur Risikobeurteilung

- Brainstorming
- Strukturierte und semi-strukturierte Befragungen
- Delphi-Methode
- Prüflisten
- Vorläufige Untersuchung von Gefährdungen (PHA)
- Gefährdungs- und Betreibbarkeits-untersuchung (HAZOP)
- Gefährdungsanalyse mit Kontrollen an kritischen Stellen (HACCP)
- Toxikologische Risikobeurteilung
- Strukturiertes „Was-Wenn“-Verfahren
- Szenariumsanalyse

- Analyse der geschäftlichen Auswirkungen
- Ursachenanalyse
- Fehlzustandsart- und -auswirkungsanalyse (FMEA) und FMECA
- Fehlzustandsbaum-analyse (FTA)
- Ereignisbaumanalyse
- Ursache-Folgen-Analyse
- Ursache-Wirkung-Analyse
- Schutzebenenanalyse (LOPA)
- Entscheidungsbaum-analyse
- Beurteilung der menschlichen Zuverlässigkeit

- „Bow-Tie“-Analyse
- Auf die Funktionsfähigkeit bezogene Instandhaltung (RCM)
- Kriechanalyse und Kriechkreisanalyse
- Markovanalyse
- Monte-Carlo-Simulation
- Bayessche Statistik und Bayessche Netze
- FN-Kurven
- Risikoindizes
- Folgen-/ Wahrscheinlichkeits-matrix
- Kosten-/Nutzen-Analyse
- Multi-Kriterien-Entscheidungsanalyse (MCDA)

ONR 49000 – Risikomanagement für Organisationen und Systeme

Familie von ON-Regeln zur Umsetzung von ISO 31000 in die Praxis

- ONR 49000 – Begriffe und Grundlagen
- ONR 49001 – Risikomanagement
  (systemischer Ansatz, Risikomanagement-System, Risikomanagement-Prozess)
- ONR 49002-1 – Leitfaden für die Einbettung des Risikomanagements ins Managementsystem
  (Wechselwirkung mit Kernprozessen der Organisation, Nahtstellen zu anderen Management-Teilsystemen)
- ONR 49002-2 – Leitfaden für die Methoden der Risikobeurteilungen
- ONR 49002-3 – Leitfaden für Notfall-, Krisen- und Kontinuitätsmanagement
  (Notfall- und Krisen-Szenarien, Krisenstab und Krisenmanagement-Prozess, Kontinuitätsmanagement)
- ONR 49003 – Anforderungen an die Qualifikation des Risikomanagers

ONR 49002-2 – Methoden der Risikobeurteilung

Einteilung von Methoden der Risikobeurteilung in fünf Gruppen

- Kreativitätstechniken (Brainstorming, Delphi-Technik, World Cafe)
- Szenario-Analysen (Schadensfall-Analyse, Fehlerbaum- und Ablaufanalyse, Szenario-Analyse),
- Indikatoren-Analysen (Critical Incidents Reporting, Change Based Risk Management),
- Funktions-Analysen (FMEA, Gefährdungsanalysen, HAZOP, HACCP)
- Statistische Methoden (Standardabweichung, Konfidenzintervall und Monte-Carlo-Simulation)

Unterschiedliche Eignung für verschiedene Prozessphasen

- Risikoidentifikation
- Risikobewertung (Auswirkungen, Wahrscheinlichkeit, Risikohöhe)
- Risikobewältigung

IEC 61508 - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

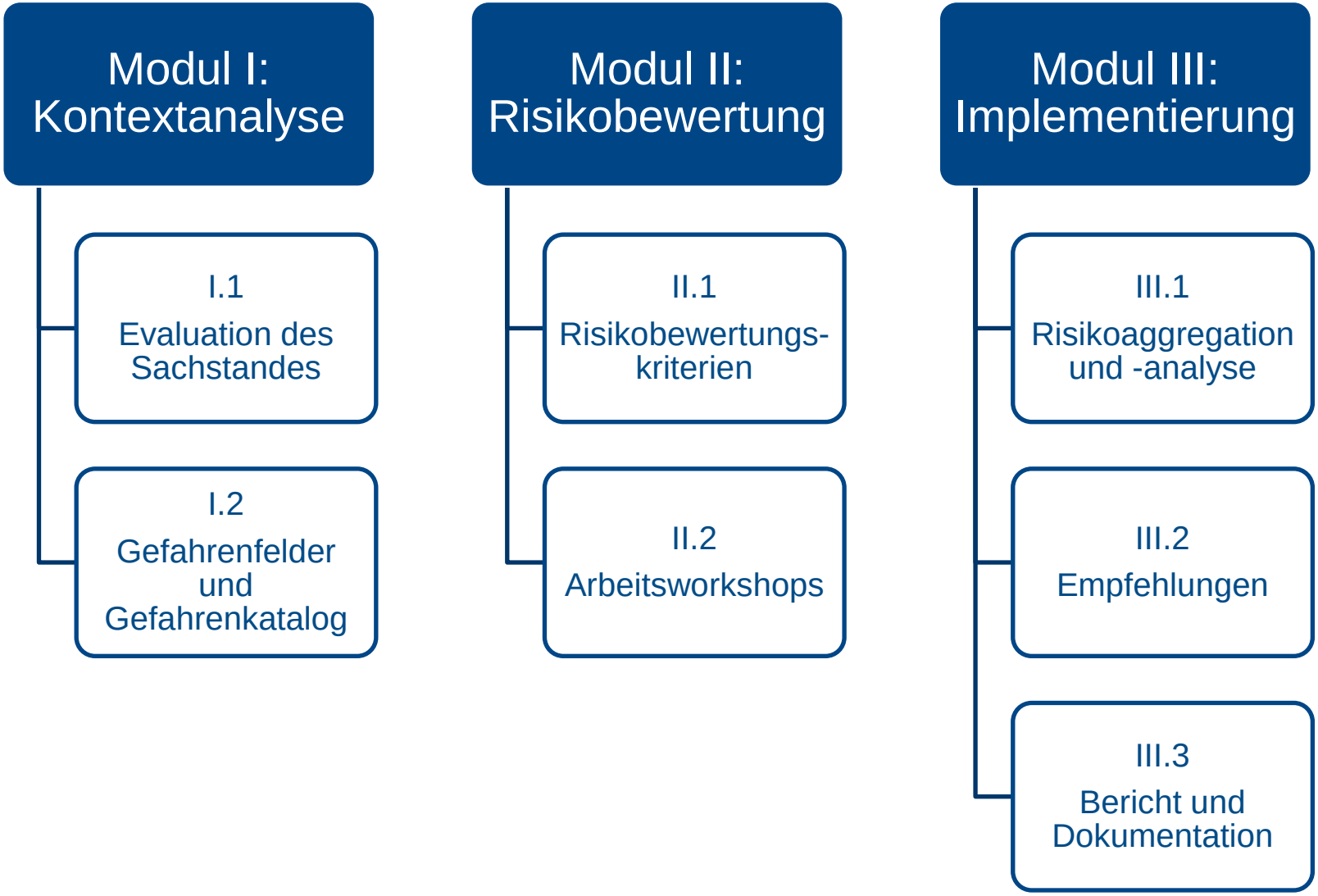
Mehrteilige Norm primär zur Herstellung ungefährlicher Produkte

- IEC 61508-1:2010 – Allgemeine Anforderungen
- IEC 61508-2:2010 – Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme
- IEC 61508-3:2010 – Anforderungen an Software
- IEC 61508-4:2010 – Begriffe und Abkürzungen
- IEC 61508-5:2010 – Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)
- IEC 61508-6:2010 – Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
- IEC 61508-7:2010 – Anwendungshinweise über Verfahren und Maßnahmen

Relevanz für Konformität von Prozessen (z. B. V-Modell)

Arbeitsprogramm

„Projektstrukturplan“ Branchenrisikoanalyse Telekommunikation



Allgemeine Grundsätze

Anwendung bewährter Methoden auf Basis von Standards

- Risiko-, Kritikalitäts-, Verwundbarkeitsanalysemethoden
- Nationale/internationale, zivile/militärische Standards

Modularisierung der zu erstellenden Dokumente

- Bessere Wartbarkeit der Dokumente
- Aufbereitung für verschiedene Leserkreise

Verfahrensweisen des Projektmanagements

- Strukturierung in Teilvorhaben
- Vermeidung bzw. Minimierung von Projektrisiken

I.1 Evaluation des Sachstandes

Erfassung und Strukturierung wesentlicher Einflussfaktoren als Basis für weitere Arbeitspakete

Ziel

- Umfassender Überblick über technische, organisatorische und personelle Anforderungen

Methodik

- Literaturrecherche
- Delphi-Methode

Ergebnis

- Strukturierte Zusammenstellung von Literatur

I.2 Gefahrenfelder und Gefahrenkatalog

Strukturierte Zusammenstellung möglicher Gefahren für Akteure, Komponenten und Systeme in Anlehnung an bekannte Critical Incident Reporting Systems, „Near-Miss“-Analysen aus Luft- und Raumfahrt und ONR 49.002

Ziel

- Aggregierter Gefahrenkatalog auf Basis bestehender Kataloge und Erfahrungen beteiligter Organisationen

Methodik

- Delphi-Methode
- Gefahrenfelder nach ONR 49002
- Prozessanalyse nach IEC 61508

Ergebnis

- Zusammenstellung systemrelevanter Gefahren

II.1 Risikobewertungskriterien

Identifikation relevanter Interessensgruppen, Schaffung eines harmonisierten Verständnisses relevanter Risikobewertungskriterien
(Eintrittswahrscheinlichkeit/Machbarkeit, Auswirkungsdimension)

Ziel

- Zusammenstellung von Gefahrengebieten und Risikobewertungskriterien

Methodik

- Delphi-Methode
- Methodenmix aus ONR 49002-2, IEC 31010 und IEC 61508

Ergebnis

- Abgestimmte Kriterien zur Bewertung von Risiko- und Gefahrenlisten bzw. -gebieten

II.2 Arbeitsworkshops

Ermittlung von Einzelrisiken aus identifizierten Gefahren (Erfassung aller Risiken, Evaluierung der Einzelrisiken, Evaluierung möglicher Risikominimierungsmaßnahmen)

Ziel

- Bewertung von Einzelrisiken und Abstimmung der Bewertung unter Experten

Methodik

- Drei jeweils vier- bis sechsstündige Workshops
- Visualisierung mittels Software

Ergebnis

- Gemeinsam bewertete Einzelrisiken auf Basis des Gefahrenkatalogs

III.1 Risikoaggregation und -analyse

Zusammenfassung der Einzelrisiken zu Aggregationsrisiken, Abstimmung unter beteiligten Organisationen, Aufbereitung von Maßnahmen zur Risikosteuerung

Ziel

- Zusammenstellung einer aggregierten Risikolandschaft

Methodik

- Workshop
- Risikolandschaft nach ONR 49002 bzw. IEC 31010

Ergebnis

- Aggregierte und kommentierte Risikomatrix für alle Einzelrisiken in allen zuvor identifizierten Gefahrenfeldern und eine Aggregationsrisikomatrix

III.2 Empfehlungen

Ausarbeitung und Abstimmung empfohlener Maßnahmen auf Basis der Ergebnisse aus Arbeitspaket III.1

Ziel

- Vorlage eines abgestimmten Vorschlags über die im Rahmen der Risikoanalyse erörterten Maßnahmen und Vorgehensweisen

Methodik

- Workshop

Ergebnis

- Abgestimmte und priorisierte Handlungsempfehlungen zu den identifizierten Risiken

III.3 Bericht und Dokumentation

Strukturierte Zusammenfassung aller Ergebnisse in einem Bericht, Dokumentation der Workshops

Ziel

- Zusammenstellung eines abgestimmten Berichts zu den identifizierten Risiken und den akkordierten Empfehlungen

Methodik

- Bericht

Ergebnis

- Abgestimmter Bericht inklusive Dokumentation aller Zwischenschritte

Organisatorische Struktur

Beteiligte Organisationen

Betreiber öffentlicher Kommunikationsnetze und -dienste

Einrichtungen der öffentlichen Verwaltung

- Sicherheitsressorts
- Computer Security Incident Response Teams
- Regulierungsbehörden

Interessensgruppen

- Konsumenten
- Wirtschaft
- Forschung
- Weitere nach Bedarf

Beratungsunternehmen

Projektorganisation

Lenkungsausschuss

- Schnittstelle zu ÖSCS und APCIP
- Abnahme des Ergebnisses
- 2017 voraussichtlich zwei ca. zweistündige Sitzungen

Technisches Expertengremium

- 2017 voraussichtlich fünf ca. vier- bis sechsstündige Workshops (vier im ersten Halbjahr, einer im Herbst)
- Zusätzliche Expertengespräche

Benennung der Mitglieder durch beteiligte Organisationen nach Möglichkeit bis 14.11.2016

Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH

RTR

Branchenrisikoanalyse Telekommunikation

Ulrich Latzenhofer

RTR-GmbH

17.10.2016