Sicherheitsmanagement Ordnungsrahmen (Synopse)

Gunnar Heyn

08.02.2011

CME
Projekt GmbH

Consulting Management Engineering

Zielstellung der Synopse

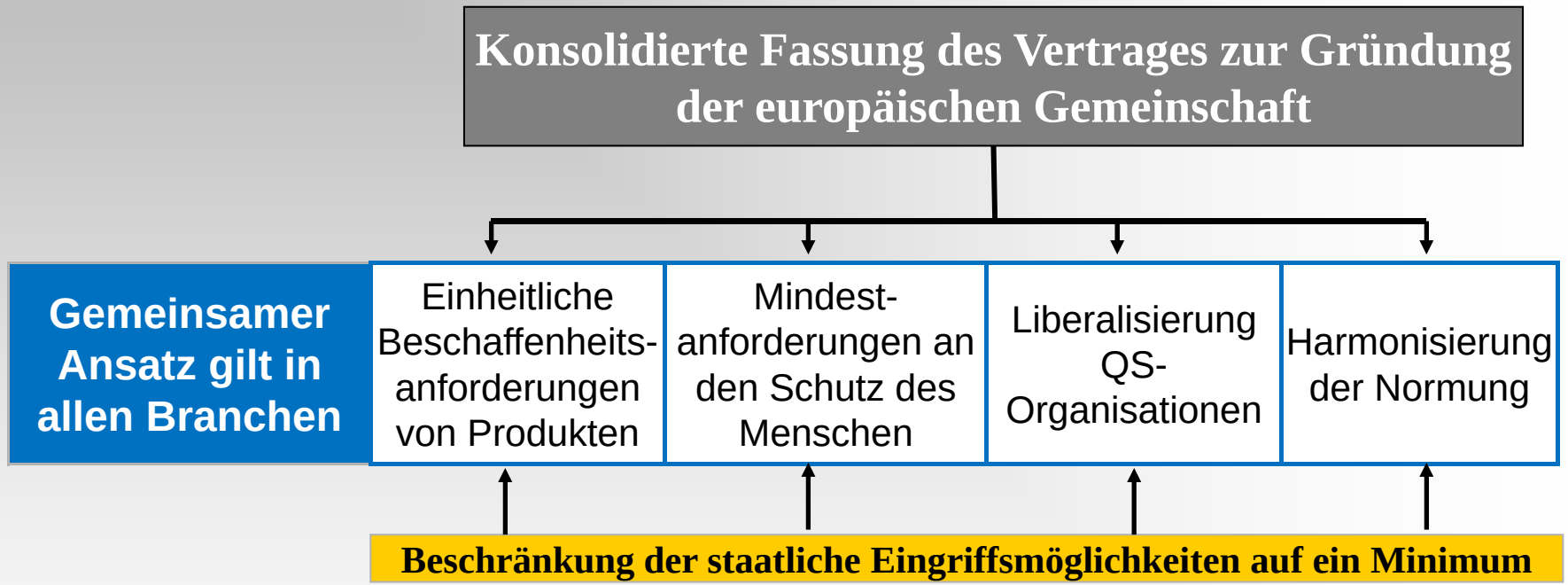
- Eine **Synopse oder Synopsis** (altgr *sýnopsis* aus *syn*- ‚zusammen' und *opsis* ‚das Sehen') ist eine zusammenfassende und vergleichende Übersicht und Gegenüberstellung gleichartiger Daten und Texte. Praktische Anwendung findet die Synopse in der Organisationslehre (zum Beispiel der Problemanalyse).
- Über die hier dargestellte Synopse wird der Ordnungsrahmen des Sicherheits-management im Anlagenbau und der Schienenfahrzeugtechnik über Grafiken, in Spaltenform bzw. über Tabellen nebeneinander dargestellt und analysiert.
- Über die Synopse soll herausgearbeitet werden, worin Gemeinsamkeiten und Unterschiede bestehen, und ob trotz der unterschiedlichen Gesetze, Verordnungen und Richtlinien in den Sicherheitsmanagement - Kernthemen Synergien bestehen und genutzt werden können.
  Vorteile:
  - Mit dem Blick über den „Branchen – Tellerrand" können qualitätssichernd sinnvolle Methoden, Prozesse und Tools im Wissenstransfer ausgetauscht werden.
  - Da die Industrie unterschiedliche Branchen bedient, könnten infolge der Vereinfachungen und Angleichungen von Sicherheitsmanagementabläufen beim Hersteller, diese wirtschaftlichen Effekte auch anteilig an die Betreiber durchgestellt werden.
- CME (i.G.) wird darlegen, dass das im Anlagenbau erworbene Sicherheitsmanagement – Fachwissen unter Berücksichtigung der branchenspezifischen Vorschriften auch in der Schienenfahrzeugtechnik eingesetzt werden kann.

Ausgangssituation Ordnungsrahmen

- Ein Ordnungsrahmen strukturiert die Planung und Realisierung zur Gestaltung eines Systems und erleichtert durch die transparente Darstellung ihre Kommunikation. Somit stellt ein Ordnungsrahmen ein Modell mit hohem Abstraktionsgrad dar, welches den Zusammenhang der Bestandteile und Beziehungen eines Systems aufzeigt. Dadurch kann auf eingängige Weise ein Überblick selbst über komplexe Zusammenhänge gewährt werden.

- Als „New Approach“ wurde mit der Konsolidierten Fassung des Vertrages zur Gründung der Europäischen Gemeinschaft ein neuer Ordnungsrahmen eingeführt, um ohne Beschränkung Produkte mit eindeutigen Beschaffenheitsanforderungen für eine Interoperabilität im Europäischen Wirtschaftsraum sicher in Verkehr bringen zu können.

new approach („neues Konzept“)

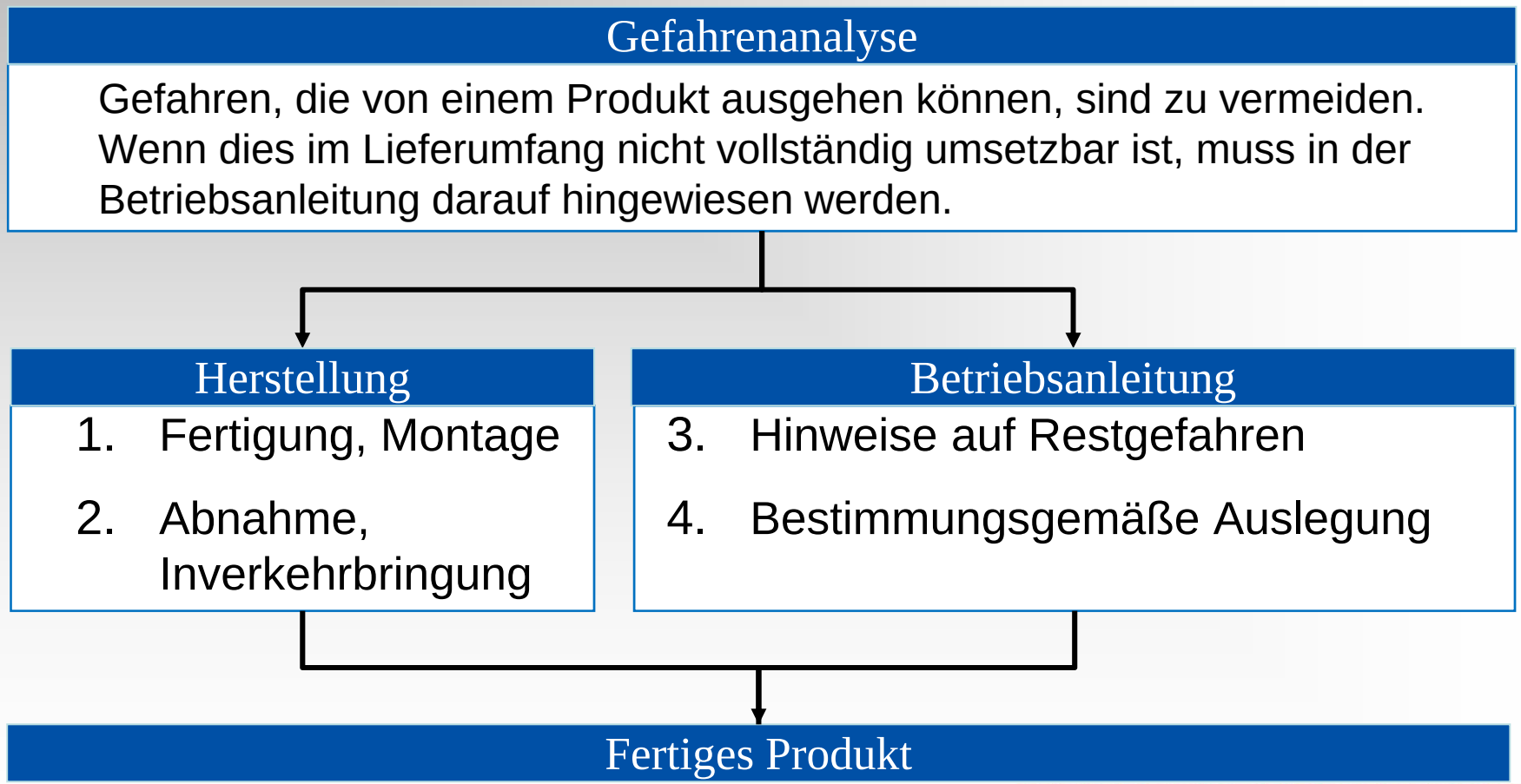


Fazit:

Die Aufgaben- und somit die Verantwortungsverteilung wurde neu definiert, wobei die Beschaffenheitsanforderung und somit die Herstellerverantwortung gestärkt wurde:

- Hersteller: Fertigung, Montage, Inverkehrbringung
- Betreiber: Inbetriebsetzung, Betrieb, Wartung, Außerbetriebnahme

Pflichten der Hersteller im „New Approach“



Pflichten des Betreibers im „New Approach“

Gefährdungsbeurteilung / Sicherheitstechnische Bewertung

- Bestimmungsgemäßen Betrieb definieren ⇒ Spezifikation
- Prüf- und Instandhaltungskonzept definieren ⇒ Spezifikation
- Gefährdungen des Betriebes ermitteln
- Betriebsanweisungen erstellen
- Prüfart, Prüfumfang und Prüffristen festlegen
- Prüfanforderungen sicherstellen

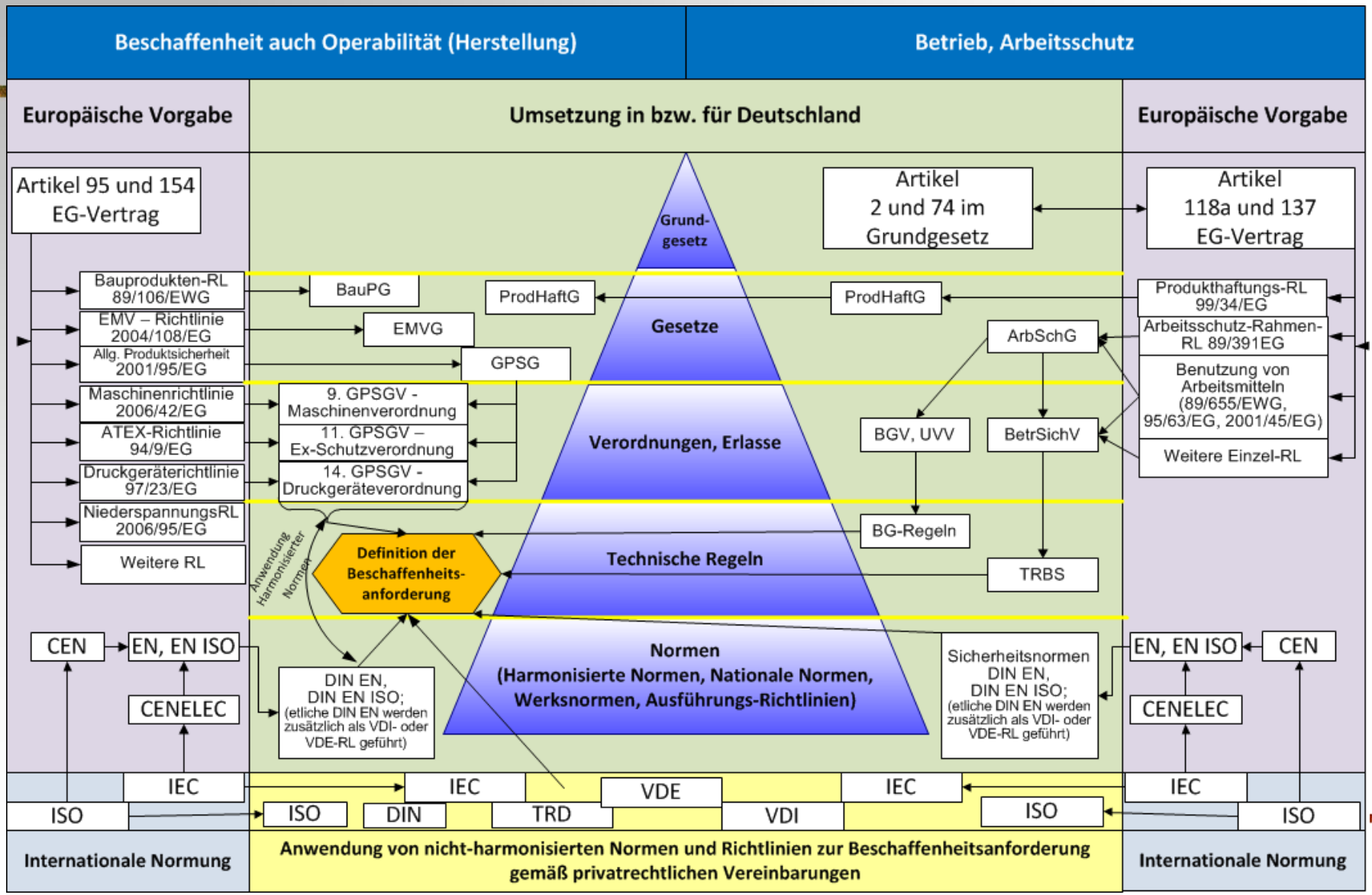
Sicheres Inbetriebsetzung der Anlage (Inbetriebnahmeanforderungen sicherstellen)

- Montageendkontrolle (Mechanical Completion)
- Produkt inkl. Betriebsanleitung und Konformitätserklärung prüfen
- Freigabe zur Heißen Inbetriebnahme;
- Ausführung vorgeschriebener Prüfungen innerhalb der Inbetriebnahme
- Abnahme durch den Betreiber

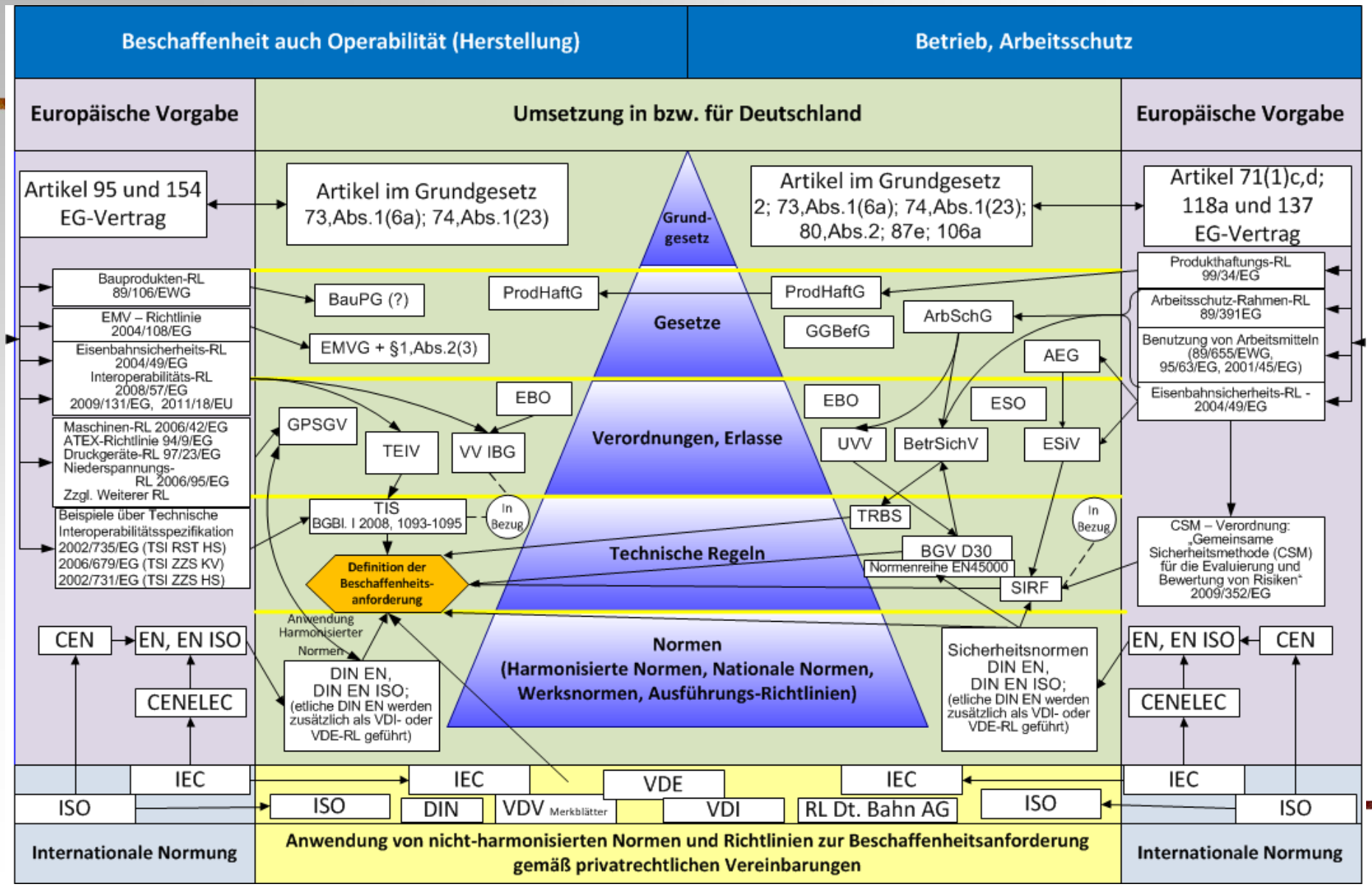
Umsetzung des „New Approach“

Ansatz	Europäische Rechtsetzung	Umsetzung im Anlagenbau und Güterwagen	Umsetzung im Bereich der Vollbahnen
Einheitliche Beschaffenheits-Anforderungen von Produkten	EU – Herstellungs- Richtlinien	GPSGV, EMVG, BauPG, etc.	AEG, Bundesgesetzblatt zur Umsetzung der TEIV einschließlich TSI (BGBl. I 2008, 1093 – 1095), EBO, BoStrab
Mindestanforderungen an Schutz des Menschen	Richtlinie Produktsicherheit, Arbeitsmittel-Benutzungsrichtlinie, Eisenbahnsicherheit	ArbSchG, GPSG, BetrSichV	ESiV, EBO, ESO, EVO, CSM-VO, BoStrab, ArbSchG, GPSG, BetrSichV
Liberalisierung, QS-Organisationen	EU – Herstellungs-Richtlinien	Notified Body (NoBo) – Regelung im GPSG	Notified Body (NoBo)
Nationale Prüfstellen zur Inbetriebsetzung überwachungs-bedürftiger Systeme	Liegt im Ermessen des Errichterlandes	Zugelassene Überwachungsstelle (ZÜS) Regelung über BetrSichV	Eisenbahn Bundesamt (EBA)
Harmonisierung der Normen	Veröffentlichte EN - Normen	Umsetzung in DIN EN, (z.B. 13445; 12952)	Umsetzung in DIN EN

Ordnungsrahmen im Anlagenbau



Ordnungsrahmen für Schienenfahrzeuge



Synopse zum „Ordnungsrahmen“

Ansatz	Umsetzung im Bereich der Vollbahnen	Umsetzung im Bereich Anlagenbau und Energieversorgung
Grundgesetz und EG-Vertrag	Eisenbahnen bestehen ab dem 2. Kondratjew-Zyklus (1830). Entsprechend der Historie insbesondere der Eigenschaft als Staatsbetrieb wird die Eisenbahn noch explizit im Grundgesetz erwähnt. Die staatliche Aufsicht ist deshalb auch präsenter als in der Energiewirtschaft. Der EG-Vertrag verpflichtet sich zum Ausbau und zur Sicherheit der Verkehrsnetze.	Energieerzeugungsanlagen bestehen ab dem 3. Kondratjew-Zyklus (ca. 1885) und werden im Grundgesetz explizit nicht erwähnt, obwohl deren ökonom. Bedeutung und ökol. Auswirkung einem immer größeren gesellschaftlichen Interesse unterliegen. Der EG-Vertrag verpflichtet sich zum Ausbau der Energienetze aber nicht zu deren Sicherheit, und nicht zur ökologischen Energieerzeugung.
Besicherung von Qualität und/oder Sicherheit (Inverkehr-bringung) im EU-Binnenmarkt	TSI-Zertifizierung dokumentieren die Umsetzung von Interoperabilitätsspezifikationen (Beschaffenheitsanforderungen); Es ist nicht erkennbar, dass EG-Richtlinien eine Harmonisierung von Herstellernachweisen im Schienenfahrzeugbau fordern. Der Prozess wird mit DIN EN 15085 empfehlend beschrieben. Keine EG Forderung nach Herstellergefahrenanalysen besteht.	EG Richtlinien definieren bereits detailliert Beschaffenheitsanforderungen, die mit nationalen Gesetzen harmonisiert wurden. CE-Zertifizierungen dokumentieren die Umsetzung. Mit der Anwendung von harmonisierten Normen besteht bereits eine Konformitätsvermutung. Seitens der Hersteller besteht die Pflicht zur Erstellung von Gefährdungsanalysen.
Betriebliche Sicherheit	Unterschiedliche Gesetze, Verordnungen und Regelwerke greifen. Die BetrSichV und deren sinnvolle Grundanforderungen, werden nur beschränkt umgesetzt. (Wie verhält es sich mit der Gleichstellung von Sicherheiten für Arbeitnehmern und für Fahrgäste?) Sektorenspezifische Sicherheitsrichtlinien bestehen	Das ArbSchG wird komplett durch die BetrSichV umgesetzt. Der verpflichtenden Gefährdungsbeur-teilung läuft ein Sicherheitsmanagementprozess zur Abwehr bzw. Minimierung von Risiken voraus, welcher in der Betreiberverantwortung für Spezifikationserstellung, Procurement und QM liegt. Sektorenspezifische Sicherheitsrichtlinien bestehen.

Treiber zur Anwendung und Verbesserung des Sicherheitsmanagements

- Die Umsetzung des „New Approach“ der Europäischen Gemeinschaft schreitet voran. Die Erfahrungen der Behörden sowie der ZÜS führen zu detaillierten Forderungen
  z.B. nach Sicherheitsgesprächen oder HAZOP vor Erstellung von Gefährdungsbeurteilung (überwachungspflichtige Anlagen)
- Abgleich von unterschiedlichen Forderungen im Hinblick auf gleiche Beschaffenheitsanforderungen (Interoperabilität) und Entwicklung von möglichst identischen Aktivitäten innerhalb internationaler Projekte → Hebung von Synergien auch in Richtung Inbetriebnahme und Betrieb
- Stand der Sicherheits-Technik ist im Wandel der Zeit → Änderungen von harmonisierenden technischen Normen sowie deren zwingende Anwendung sind die Folge.

Der allgemeine Bedarf an Normen

Normen gewährleisten, dass Produkte und Dienstleistungen für den vorgesehenen Zweck geeignet sind

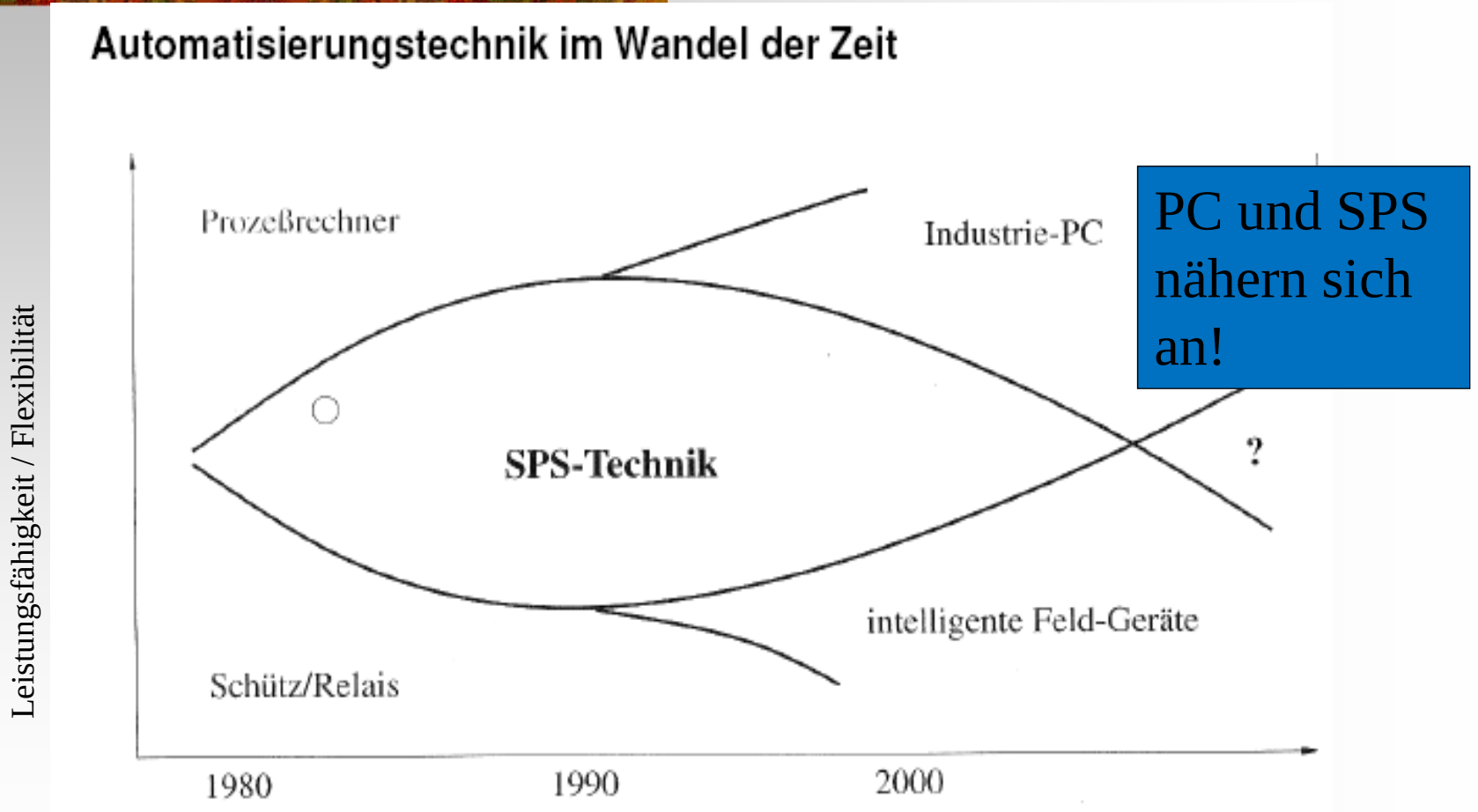
Normen sind dokumentierte, i. d. R. freiwillige Vereinbarungen, in denen Kriterien für Produkte, Dienstleistungen und Verfahren festgelegt werden.
Mit Hilfe von Normen kann gewährleistet werden, dass Produkte und Dienstleistungen für den vorgesehenen Zweck geeignet, vergleichbar und kompatibel sind.
Normen werden durch wichtige Wirtschaftssektoren bzw. von Seiten des Marktes bedarfsorientiert entwickelt oder es liegt ein öffentliches Interesse vor.

Normen sind sinnvoll ...

... für Interoperabilität von Produkten und Dienstleistungen
Beispielsweise besteht in der Industrie der Bedarf an einer Norm benötigt, um die Interoperabilität eines Produkts oder einer Dienstleistung zu gewährleisten.

... für Fairness am Markt und mehr Qualität und/oder Sicherheit
Der Markt nutzt Normen, um einen fairen Wettbewerb zu ermöglichen und über Standards die Qualität und Sicherheit von Produkten oder Dienstleistungen zu verbessern.

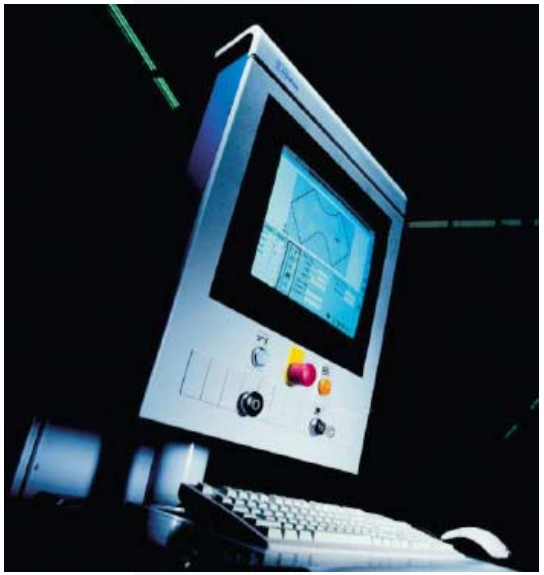
Prozessanpassungen durch Entwicklung der Sicherheits-Technik



Regelwerksentwicklung entsprechend dem Stand der Sicherheits-Technik

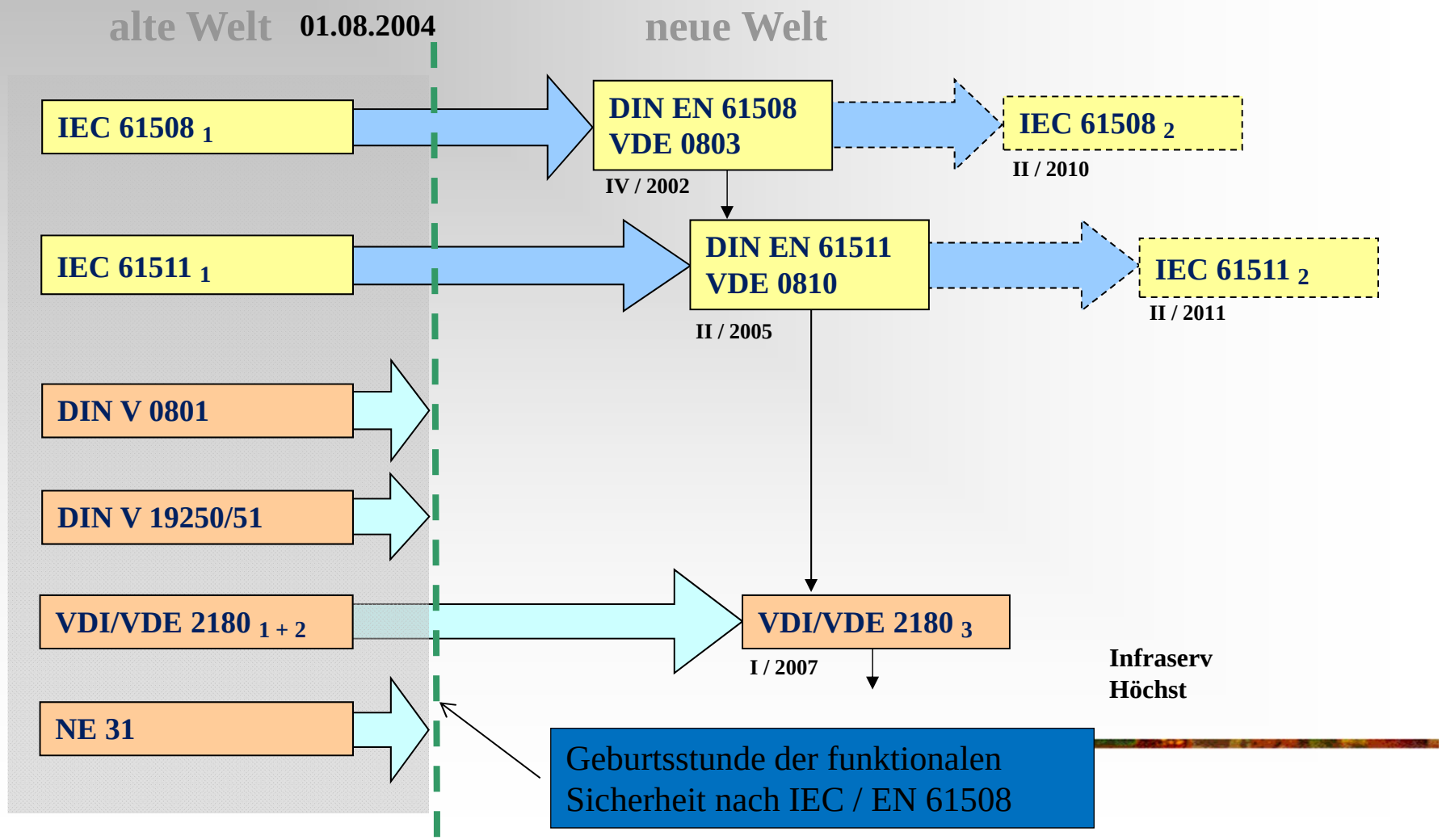
PLT- Schutzeinrichtungen
Entwicklung

1980	elektromechanische, fest verdrahtete Schutzeinrichtungen
1984	VDI/VDE 2180 „Anlagensicherung mit Mitteln der MSR“
	„Microcomputer in der Sicherheitstechnik“ (Hölscher/Rader)
1989	DIN V 19250 „Grundlegende Sicherheitsbetrachtungen“
1990	VDE 0801 „Rechner in Sicherheits-Systemen“
1998	VDI/VDE 2180 (Überarbeitung)
2000	VDI/VDE 2180, Blatt 5 „Anwendersoftware“
2003	NE 93 “Stördatenerfassung“
2004	IEC 61508, IEC 61511 als VDI-RL („SIL- Problematik“)
2007	VDI/VDE 2180 (2. Überarbeitung)
2008	VDI/VDE 2180, Blatt 5
…	…
...?..	Normung zu komplexen PLT- Schutzeinrichtungen ??

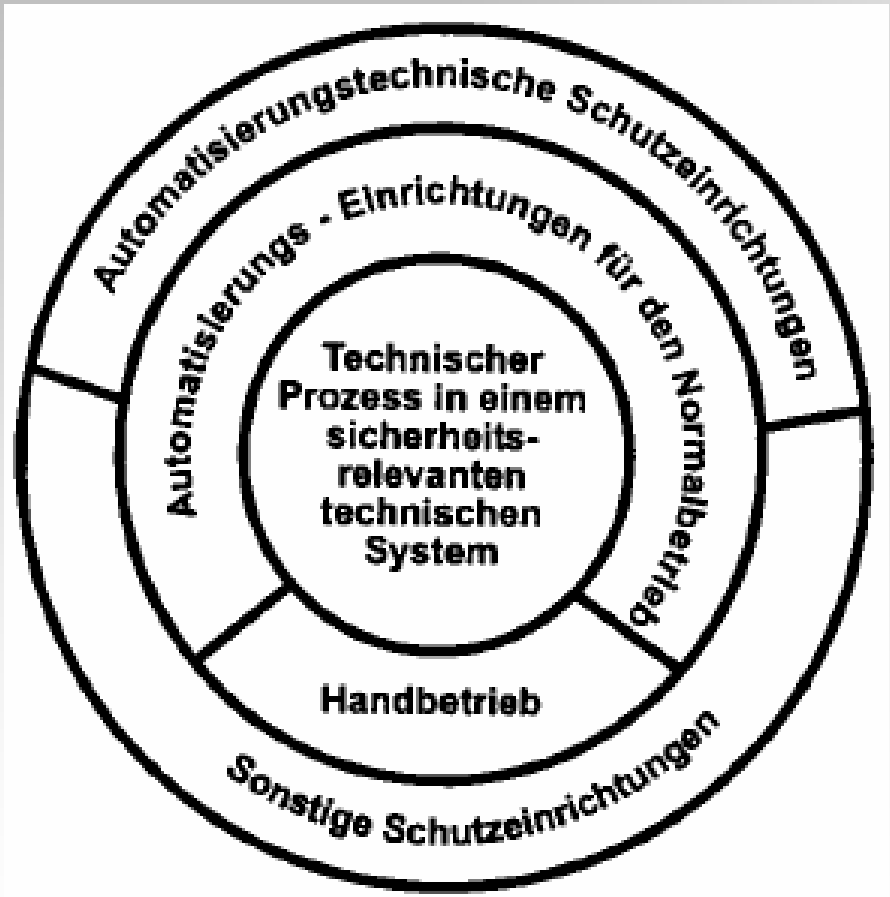


Euteneuer; lanuv NRW

Regelwerksentwicklung entsprechend dem Stand der Sicherheits-Technik



Darstellung der Schutzebenen in Schalenmodellen



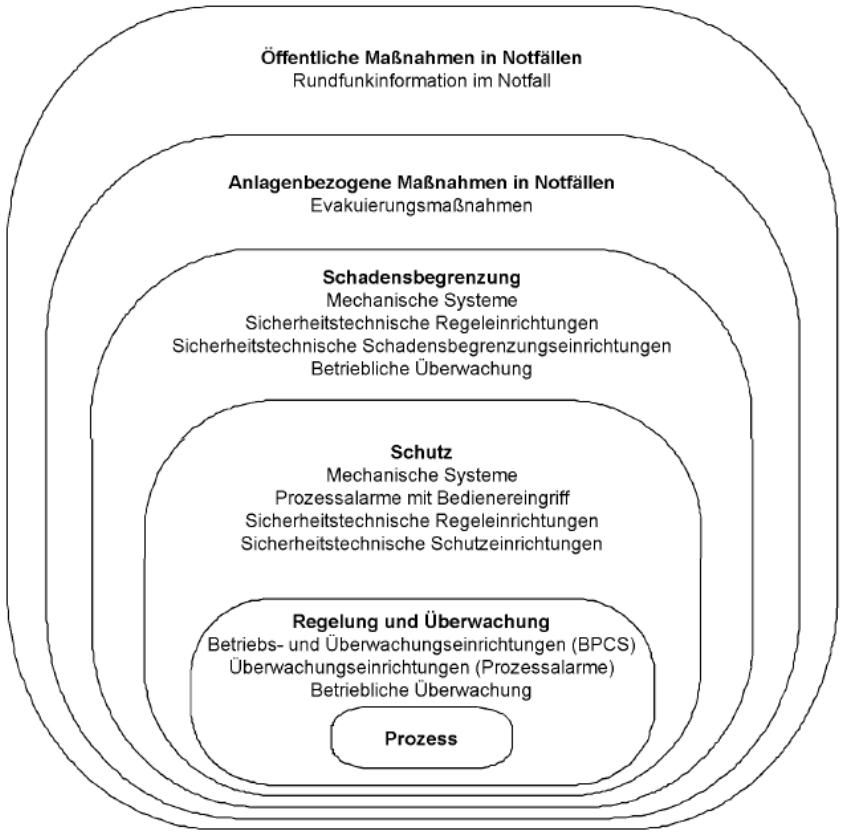
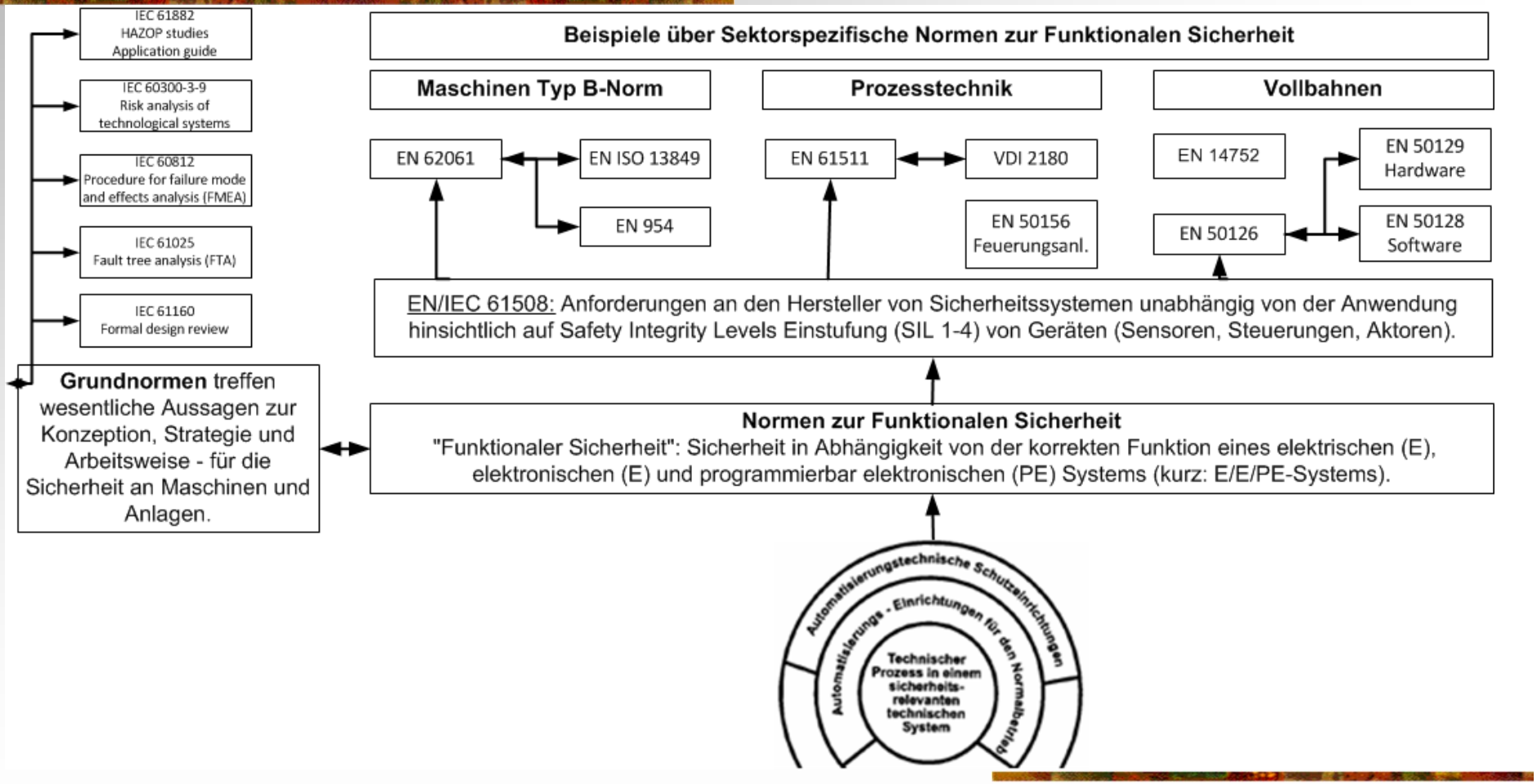


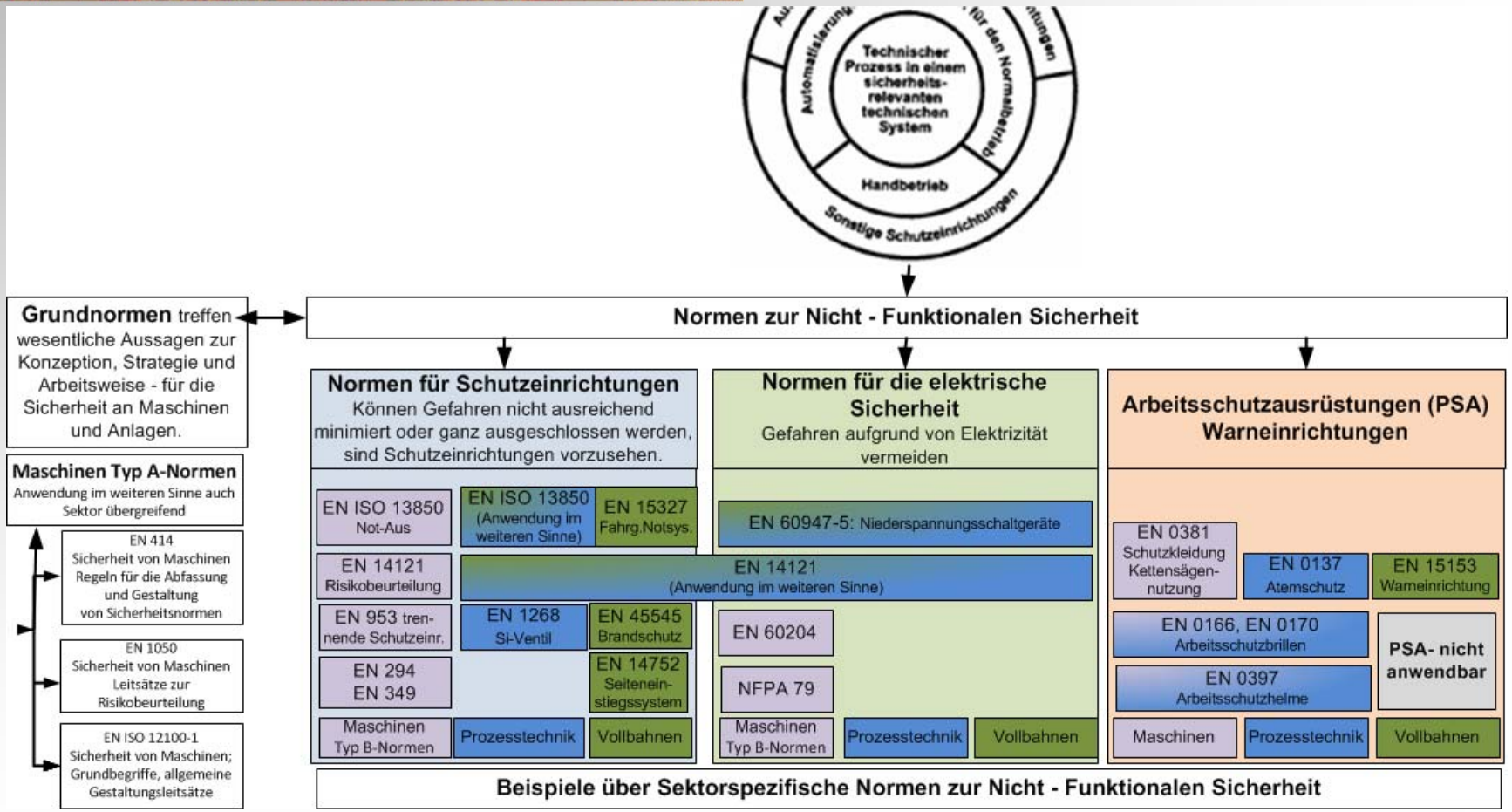
Bild 9 – Typische Methoden der Risikominderung in prozesstechnischen Anlagen

IEC 61511-1

Normensynopse zur Funktionalen Sicherheit



Normensynopse zur Nicht-Funktionalen Sicherheit



Fazit zur Normen – Synopse (Teil 1)

- Es existieren keine sektorenübergreifenden Grundnormen zur *Nicht-Funktionalen Sicherheit*, die generelle Aussagen zur Konzeption, Strategie und Arbeitsweise für die Sicherheit an Vollbahnen, Maschinen und Anlagen liefern. Der Anlagenbau orientiert sich an den Sicherheitsgrundnormen für Maschinen (Typ-A Normen), da neben Prozesstechnik auch Maschinen verbaut werden.
- Die englischsprachigen IEC Grundnormen für die Planung der *Funktionalen Sicherheit* werden weitestgehend sektorenübergreifend berücksichtigt.
  Dies erfolgt auch zum Teil über sektorspezifischen Normen zur *Funktionalen Sicherheit*, die somit mehr Gemeinsamkeiten als Unterschiede ausweisen (insbesondere über das RAMS-Management).
  Leider gehen über die fehlende generelle Standardisierung branchenübergreifende Neuerungen und Erfahrungsrückflüsse verloren bzw. erfolgen zeitverzögert.

Fazit zur Normen – Synopse (Teil 2)

- Die EN/IEC 61508 mit Spezifikationsanforderungen an den Hersteller von Sicherheitssystemen ist in allen Branchen die Basisnorm. (Herstellerstandards und Interoperabilität von Sicherheitssystemen über alle Branchen)

- Die Festlegung der SIL-Klassen ist Aufgabe des Betreibers im Anlagenbau, da dieser die Verantwortung zur Abwehr der Gefährdungen im Betrieb hat und somit eine Einschätzung über Risiken im Betrieb vornehmen muss. Im Bahnsektor wurde diese Aufgabe auf den Hersteller delegiert.

- Die Vermutung liegt nahe, dass sich die Vollbahnen infolge des sektorenspezifischen Risikos einen anderen Ordnungsrahmen gegeben haben und nicht unter der BetrSichV aufgehängt sind. Allerdings ist es dann nicht nachvollziehbar, weshalb andere Branchen spezielle sektorenspezifische Risiko-Graphen aus weiterführenden Normen verwenden und die Vollbahnen sich auf den SIL Risiko-Graph aus der Basisnorm EN 61508 beschränken.

Empfehlung (Teil 1)

Erstellung von **eigenen** einfachen und verständlichen Sicherheitsmanagement - Prozessen zur Befriedigung der Gesetze, nur in Anlehnung an Normen und Richtlinien, welche ja i. d. R. freiwillige Vereinbarungen sind.

Folgende Anforderungen sind dabei zu berücksichtigen:

- Prüffähige Anlagentechnik
- Prüffähigkeit für ZÜS bzw. EBA
- Beanstandungslose Gefährdungsbeurteilung
- Umsetzung Sicherheitsphilosophie des Betreibers
- Bereitstellung der erforderlichen Dokumentation

Empfehlung (Teil 2)

Kernstück zur Umsetzung vorstehender Anforderungen:

Organisation und Durchführung von Sicherheitsgesprächen

1. Nach ordnungsgemäßer Systemdefinition erfolgt die Gefährdungs- und Risikoidentifizierung des jeweiligen Systems und seiner Schnittstellen. Verifizierung von Gefährdungen anhand von Fragelisten und Aktionsprotokollen über Schlüsselwörter
2. Halbquantitatives Bewertung der identifizierten Gefahren und Risikobeurteilung mit Hilfe einer **Risiko - Matrix.**
   (Hier noch keine Anwendung des Risiko - Graphen!)
3. Entwurf und Planung von Maßnahmen zur Risikoreduzierung: Zuordnung von z.B. verfahrenstechnischen bzw. leittechnischen Schutzebene gemäß den identifizierter Risiken
4. Falls eine Schutz Prozessleittechnik (funktionale Sicherheit) erforderlich wird, sind Anforderungen an die Schutz PLT gemäß dem Risiko-Graph entsprechend der zu beachtenden Normen festzulegen

Lieferanten-Sicherheitsgespräche Ziele (1)

- Bewertung der im Rahmen der Lieferanten-Gefährdungsanalysen gemäß EU-Herstellungsrichtlinien identifizierten Restgefahren hinsichtlich ihrer Wirkung(en) auf benachbarte Systeme
- Bewertung, ob aufgrund der geplanten Ausführung des Systems besondere organisatorische Maßnahmen seitens des Betreibers erforderlich sind
- Beurteilung der Wirkung von Stoff- und Energieströmen über die Schnittstellen des zu betrachtenden Systems hinaus
- Dokumentation der Schnittstellen aus sicherheitstechnischer Sicht
- Beurteilung, ob diese Schnittstellen zu denen der benachbarten Systeme passen

Lieferanten-Sicherheitsgespräche Ziele (2)

- Bewertung, ob die Lieferantensysteme in ihrer Umsetzung die sicherheitstechnische Spezifikation erfüllen
- Bewertung der durch die Lieferanten erstellten Entwürfe zur Klassifizierung von PLT-Einrichtungen durch Überprüfung der ermittelten Risikoparameter
  (→ SIL)
- Abgleich der SIL-Klassifizierungen
  ... gemäß Planung des Lieferanten
  ... oder durch Festlegung im Sicherheitsgespräch
  mit den Empfehlungen des Betreibers;
  Gegebenenfalls Bewertung von Abweichungen.

Ihre Unterstützung im Sicherheitsmanagement

Für Rückfragen steht Ihnen gern zur Verfügung:

Gunnar Heyn
CME Projekt GmbH
Paulinerweg 39
04299 Leipzig
Tel.: 0174 4088091
Fax: 0341 8621145
g.heyn@cme-projekt.de

Vielen Dank für Ihre Aufmerksamkeit