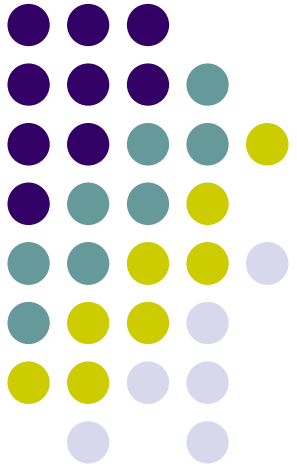
Das Qualitätsmerkmal „Technische Sicherheit“

Diskurs zwischen Risikovermeidung und Sicherheitsmanagement



Dr. Bernd Schulz-Forberg, VDI, Berlin

Die VDI-Publikation

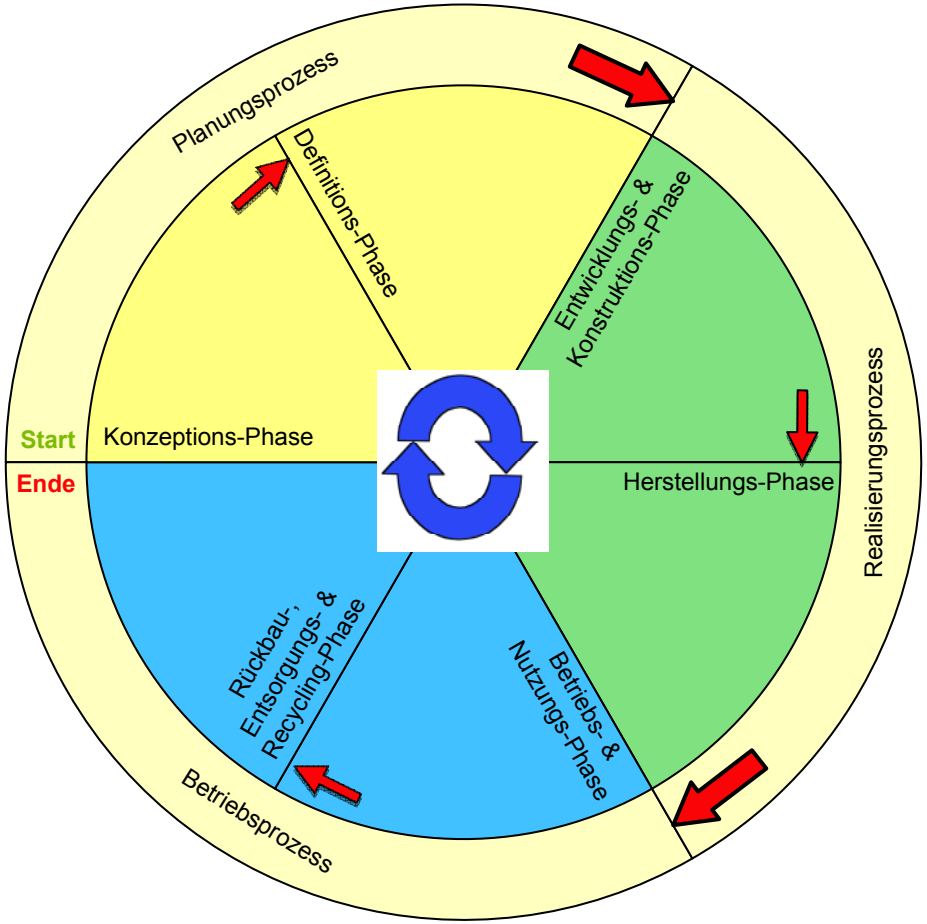
Das Qualitätsmerkmal „Technische Sicherheit“ - Denkansatz und Leitfaden -

1. Auflage 2016, Herausgeber VDI, Beuth Verlag, ISBN 978-3-410-26196-4

Das Qualitätsmerkmal „Technische Sicherheit“, Bernd Schulz-Forberg, Technische Sicherheit Bd.6 (2016) Nr. 5 - Mai

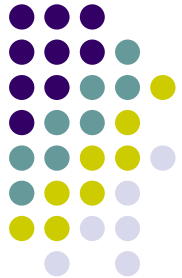
- Erzeugung der Technischen Sicherheit
- Die Grenzen der Sicherheit
- Überprüfbarkeit der Sicherheit
- Gesellschaftliche Betrachtungen
- Empfehlungen
- Schlussbemerkungen

Denkansatz; Das Phasenkonzept



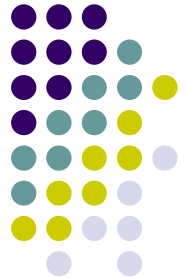
**In den ersten drei Phasen wird am Schreibtisch gearbeitet,
Hardware wird noch nicht eingesetzt**

Denkansatz



- Erwartung der Märkte
- Rechtsgrundlagen
- Technologische Weiterentwicklung
- *Technologische Innovationen*
- Unterschiedliche Regelungen
- Menschlicher Einfluss in allen Phasen
- *Risikosteuerung als gesellschaftlicher Prozess*
- *Kommunikation*
- Interdisziplinäres Vorgehen
- Bestandteile des Vorgehenskonzepts
- Aufgabe

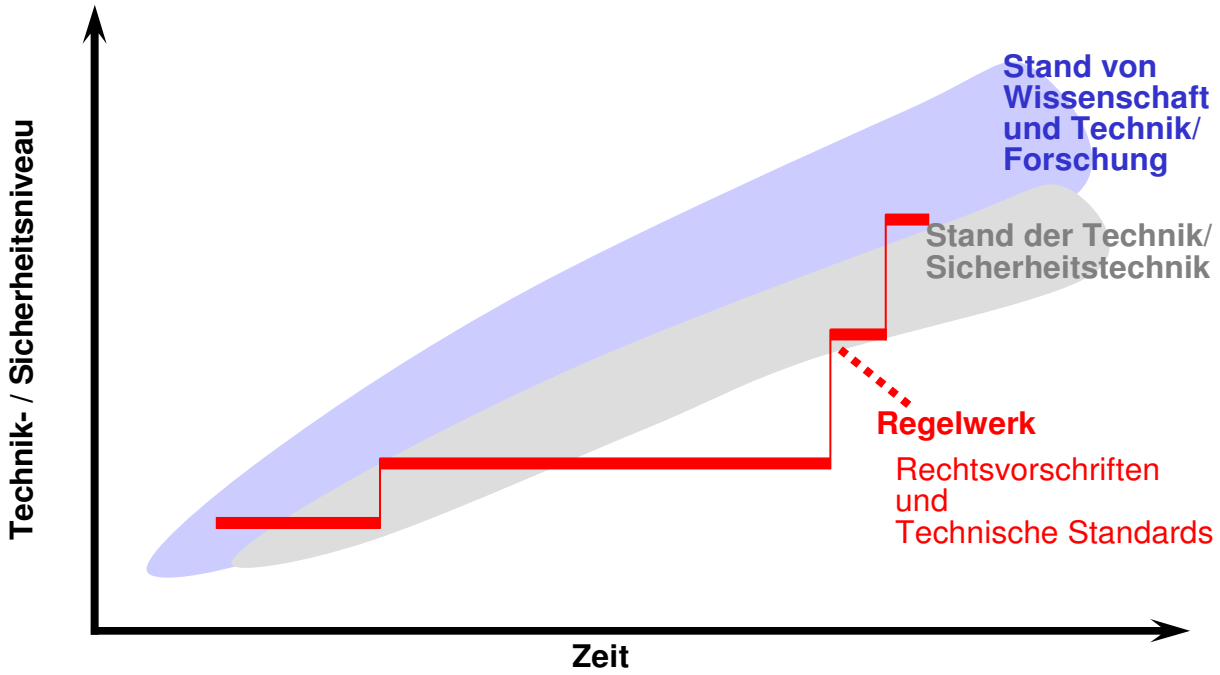
Technologische Innovationen



- Das Kunststück Innovation ist erlernbar!
- Verbinden sich Fantasie, Wissen und Erfahrung, dann gelingen Innovationen.
- Normen sollten hierbei optimal in Form von Wirkstandards eingesetzt werden. (Positive Wirkung)
- Sie dürfen auf keinen Fall in einer Institutionenmatrix zum Erstarren des dynamischen Innovationsprozesses führen. (Negative Wirkung)

– schreiben Warnecke und Bullinger aus der Fraunhofer Gesellschaft (aus: Kunststück Innovation, 2003).

Stand der Technik



Qualitativer Zusammenhang des Standes der Technik mit dem Stand von Wissenschaft und den allgemein anerkannten Regeln der Technik

Risikosteuerung

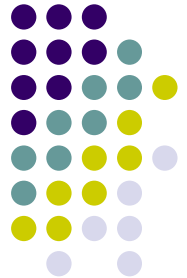
Aaron B. Wildavsky, Sozialwissenschaftler aus Berkley, schrieb:
„No risk ist he highest risk of all“. Wenn wir versuchen,
gar kein Risiko einzugehen, dann gehen wir das größte Risiko überhaupt ein.
Denn dann entscheiden wir nicht mehr, dann sind wir nur noch gelähmt.

Zur Kommunikation

- All we have to do get the numbers right.
- All we have to do is tell our audience the numbers.
- All we have to do is explain what we mean by the numbers.
- All we have to do is show our audience that we have accepted similar risks in the past.
- All we have to do is show our audience it`s a good deal for them.
- All we have to do treat our audience nicely.
- All we have to do is make our audience partners.

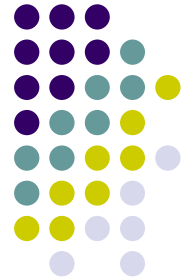
Morgan, G. et. al. (2002): Risk communication: A mental models approach, Cambridge University Press; Cambridge, New York,

Aufgabe



- **Harmonisierung der Sicherheitstechnik als interdisziplinäre Aufgabe,**
- **Entwicklung auf dem Gebiet der Sicherheitstechnik zur Verbesserung sicherheitsmethodischer Vorgehenskonzepte und**
- **Rückkopplung in die einzelnen Technikfelder.**

Leitfaden; Motiv und Nutzen

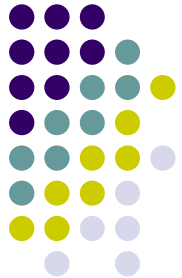


- Nach öffentlichkeitswirksamen Unfällen wird in den Medien und häufig auch in der Politik reflexartig spekuliert, dass die Regeln nicht ausreichen und schleunigst verbessert werden müssten.
- Dabei spielt es keine Rolle, ob tatsächlich die Regeln nicht ausreichen oder es sich nur um ein Vollzugsdefizit handelt.
- Aus einer Alarmierungsstimmung heraus neigt die Gesellschaft dann dazu, sogar „Verschlimmbesserungen“ ins Auge zu fassen.

Leitfaden; Motiv und Nutzen

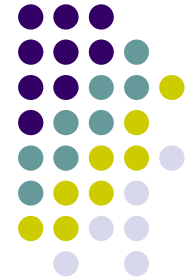
- Bei innovativen Technologien wirkt sich das bisherige Verhalten besonders nachteilig aus, da aus jedem Technikbereich heraus der Stand der Technik bzw. der Stand von Wissenschaft und Technik für das innovative Vorhaben gesondert ermittelt wird und eine Verallgemeinerung für andere Bereiche kaum je vorgenommen wird.
- Diese Schwachstelle in Technikrecht muss überwunden werden.
- Eine fachgebietsübergreifende Vorgehensweise zur Generierung und zum Erhalt von Sicherheit ist geboten.

Leitfaden, Überlegungen



- Emissionsverhalten
- Passive Beschaffenheitsmerkmale
- Aktive Funktionsmerkmale
  - „fail-safe“
  - „fail operational“
- Managementsysteme
  - Konfigurationsmanagement
  - Sicherheitsmanagementsystem

Leitfaden, Überlegungen; Safety Case



- In allen Phasen müssen die technischen Vorgaben eindeutig, klar verständlich und nachvollziehbar sein.
- Die Randbedingungen, unter denen die Antworten zur Bildung des „safety case“ gegeben werden, müssen für jede Phase von den zuständigen und verantwortlich handelnden Personen eindeutig beschrieben und auch begründet werden.
- Die herangezogenen Bewertungsmaßstäbe müssen nachvollziehbar dargestellt werden, wobei das zu Grunde gelegte Regelwerk aus gesetzlichen und technischen Bestimmungen konkret zu benennen ist. Die ggf. notwendige Bezugnahme auf den Stand der Technik oder den Stand von Wissenschaft und Technik ist zu integrieren.
- Die Antworten auf die phasenspezifischen Fragestellungen müssen klar zwischen Tatsachen, Angaben der handelnden Personen, Berechnungen, Annahmen, Prüfergebnissen und Schlussfolgerungen unterscheiden. Darüber hinaus ist die Bewertung getrennt zu führen.

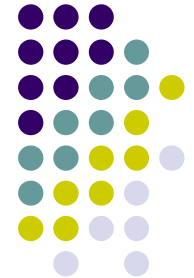
Leitfaden, Überlegungen; Safety Case

- Unterschiede in den Bewertungen in den Phasen sind von den verantwortlich handelnden Personen deutlich hervorzuheben und zu begründen.
- Schlussfolgerungen müssen transparent und vollständig nachvollziehbar sowie in sich schlüssig sein.
- Der „safety case“ ergibt sich aus den einzelnen Phasen des Produkt-Lebenszyklus und muss aus sich heraus verständlich und nachvollziehbar sein.
- Die Dokumentation muss vollständig sein und insbesondere alle rekursiven Iterationsschritte enthalten. Die Transparenz über alle drei Prozesse muss durchgehend gewährleistet sein. Der Interessenschutz kann besondere organisatorische Maßnahmen notwendig machen, ohne jedoch das Interesse „Öffentlich-Technischer Sicherheit“ unzumutbar zu beeinträchtigen.

Leitfaden, Systematik

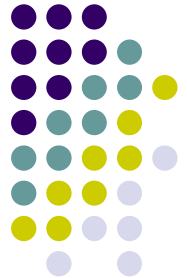
- DIN 31004-1:1982-11 „Begriffe der Sicherheitstechnik – Grundbegriffe”
- Risiko: probabilistische Sicht auf stochastische Versagensformen
- Das „größte noch vertretbare Risiko“ (Betrachtung des Grenzrisikos)
- Maßnahmen zur Reduzierung eines Risikos können weitere, anders geartete Risiken induzieren,die ihrerseits zur Erhöhung des Gesamtrisikos führen.
- Die deterministische Betrachtung geht von einer maximalen Einwirkung beim Belastungsfall aus („worst case“)
- Beide Betrachtungsweisen (**Grenzrisiko und worst-case**) sind anerkannte Grundlagen der Ingenieurswissenschaften und enthalten in Teilen Elemente der jeweils anderen Betrachtungsweise

Leitfaden, Ziele der Sicherheitstechnik

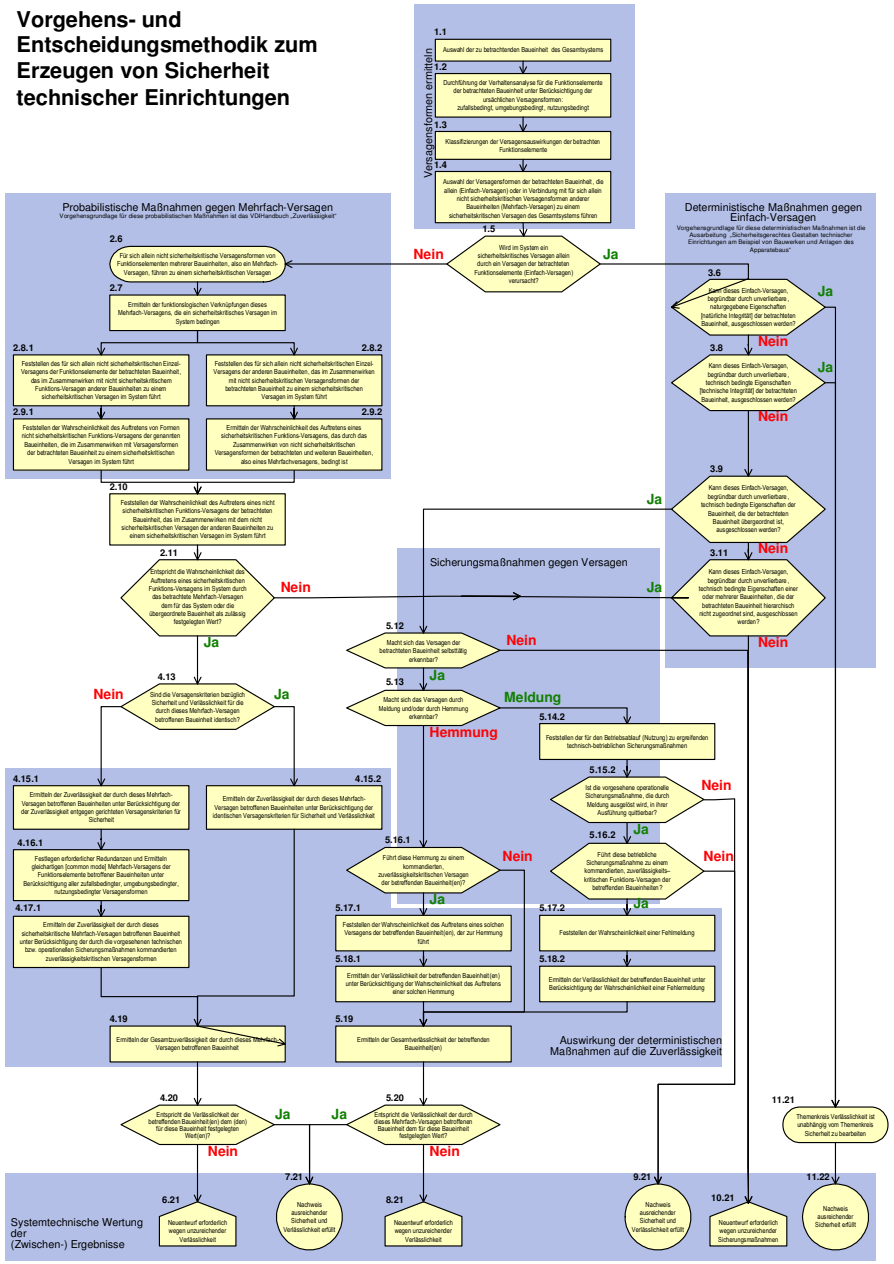


- Für die Sicherheit von technischen Systemen müssen die Systeme in ihrer Gesamtheit analysiert werden, z.B mit Hilfe der FMEA: Technische Regel - DGQ-Band 13-11:2012 „FMEA – Fehlermöglichkeits- und Einflussanalyse“
- Sicherheitstechnische Rahmenspezifikation
- Methodik, Konzept, Anforderungen und Nachweisführung
- Ausschluss von sicherheitskritischen Versagensfällen
- Ausschluss der Folgen sicherheitskritischer Versagensfällen
- Begrenzung der Wahrscheinlichkeit sicherheitskritischer Versagensfällen (Zuverlässigkeitstechnik)

Leitfaden, Herausforderungen



- Software-basierte Funktionalität
  - Software ist wie ein Produkt zu behandeln
  - Sicherheit ist als zweiseitige Eigenschaft überlebenswichtig, nämlich als Betriebssicherheit wie auch als Informationssicherheit.
- Human Factors
  - Integriertes Modell
  - Intermittierendes Modell
  - Post hoc Beteiligungsmodell
- Unterstützendes Management
  - Grundlegendes
  - Im Planungsprozess
  - Im Realisierungsprozess
  - Im Betrieb



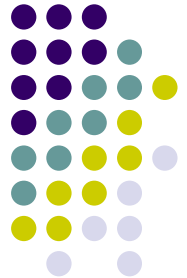
Das Handlungsschema im Überblick

Das Handlungsschema (1)

- Das Handlungsschema ist ein sicherheitsmethodisches Ablaufdiagramm für die ersten drei Phasen eines Lebenszyklus
- Ähnliches und Gleichlautendes kann damit vereinheitlicht werden

  - Deterministik: Zunächst werden die Versagensformen ermittelt, wobei die Handlungsschritte 1.1-1.4 (Auswahl der Baueinheit, Versagensanalyse, Klassifizierung der Auswirkungen und sicherheitskritisches Versagen durch Einfach-Versagen oder Mehrfach-Versagen) betrachtet werden müssen

Das Handlungsschema (2)

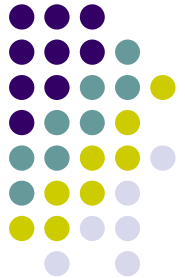


- Einfach-Versagen ?
- Bei positiver Antwort befindet man sich im Bereich der Deterministik
- Nehmen wir den klassischen Fall einer Baueinheit aus dem Brückenbau und betrachten wir ein Auflager
- Die Masse ergibt gemäß der unverlierbaren Schwerkraft die Auflagekraft, die es abzufangen gilt
- Bei sachgemäßer Ausführung ist der Nachweis ausreichender Sicherheit erbracht, d.h. die Phasen 1-3 sind erfolgreich durchlaufen

Das Handlungsschema (3)

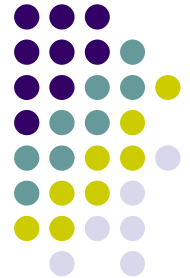
- Typ B-Behältern werden nach dem Prinzip des „worst case“ ausgelegt
- Einfach-Versagen ist damit begründbar durch unverlierbare, technisch bedingte Eigenschaften ausgeschlossen
- Zur Überzeugung aufsichtführender Institutionen / Öffentlichkeit kann ein Prototyptest hilfreich sein
  - In der Vergangenheit sind mehrfach Belege dafür erbracht worden, dass die Beanspruchung mit dem 9 m Fall auf ein unnachgiebiges Fundament alle stoßartigen Beanspruchungen bei realen Transportbedingungen mit Sicherheit abdeckt

Das Handlungsschema (4)



- Probabilistik:Je komplexer eine technische Einrichtung bzw. je anspruchsvoller der jeweilige Einsatzzweck (Missionsprofil) ist, desto notwendiger ist es, dass auf Beschaffenheit (passive Eigenschaftsmerkmale) **und** Funktionsverhalten (aktive Eigenschaftsmerkmale) Verlass besteht
- Probabilistische Vorgehensweisen ersetzen keinesfalls die bewährten deterministischen Vorgehensweisen, sondern ergänzen sie bei entsprechendem Bedarf
  - Beispiel: Brand eines Zuges im Tunnel: Die Zielbremsung nutzt die kinetische Energie des Zuges, um ihn mittels einer elektronischen Regelungseinrichtung so abzubremsen, dass er an einer Stelle zum Stehen kommt, die für Rettungskräfte zugänglich ist. Für diese Regelungseinrichtung kommt die probabilistische Vorgehensweise (Zuverlässigkeitstechnik) zur Anwendung.

Das Handlungsschema (5)



- Übergang von automatisiertem auf personalgeführten Betrieb technischer Einrichtungen (Notwendig, aber …)
- Der Eisenbahnunfall vor der Einfahrt in den Bahnhof von Santiago de Compostela am 24. Juli 2013 zeigt, was passiert, wenn ein Lokomotivführer diese Übergangsstelle übersieht. An dieser Stelle hätte der Zug durch eine zuverlässig wirkende elektronische Einrichtung automatisch abgebremst werden müssen. Eine Zielbremsung, die nicht bis zum Stillstand hätte führen müssen, hätte hier den Unfall verhindert

Das Handlungsschema (6)

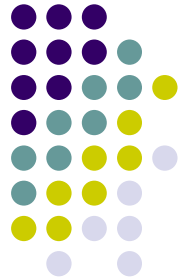
- Das Handlungsschema bringt sämtliche Fachgebiete zusammen in der Aufgabe, Sicherheit zu erzeugen und zu erhalten
- Es ist damit erreicht, dass alle Vorgehensweisen von der deterministischen über die semi-probabilistische bis hin zur probabilistischen für die ersten drei Phasen des Lebenszyklus zusammengestellt wurden
- Da alle Vorgehensweisen in einem Schema dargestellt werden, ist das Schema zwangsweise recht kompliziert, aber vollständig

Deep Water Horizon

Fehlende Redundanz des Blowout Preventers

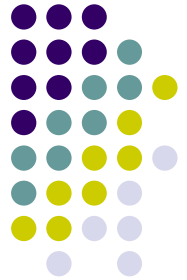
Engineering Failure Analysis

Special issue: A Tribute to Prof. A. Martens, Elsevier 2014, Volume 43



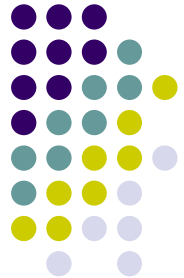
- 1992 Northeim train crash – A root cause analysis,
- Partial collapse of the Berlin Congress Hall on May 21st, 1980
- Investigations on the breakdown of a heat recovery steamgenerator during the initial operation run
- Failure of a pressure vessel for rail transport of fluid carbon Dioxide
- Failures of cranes due to wind induced vibrations
- Damage investigation on the explosive destruction of a tank at a chlorine liquefaction plant
- ‘‘Stolt Rotterdam’’ – The sinking of an acid freighter
- Root cause analysis of cracks in old steel viaducts and retrofitting
- Fatigue cracks in railway bridge hangers due to wind induced vibrations – Failure analysis, measures and remaining servicelife estimation
- Investigations for indications of deliberate blastingon the front bulkhead of the ro-ro ferry MV ESTONIA
- Breakdown of heat exchangers due to erosion corrosionand fretting caused by inappropriate operating conditions
- Explosion of a hardening vessel for AAC (autoclaved aerated concrete)

Anwendung des Handlungsschemas ?



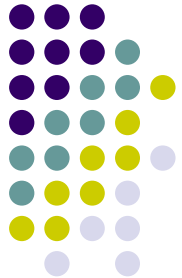
- Failures of cranes due to wind induced vibrations
- “Stolt Rotterdam” – The sinking of an acid freighter
- Investigations for indications of deliberate blasting on the front bulkhead of the ro-ro ferry MV ESTONIA

Zur Erinnerung: Aufgabe



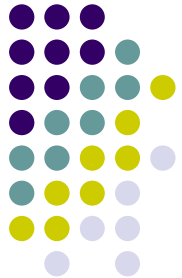
- **Harmonisierung der Sicherheitstechnik als interdisziplinäre Aufgabe,**
- **Entwicklung auf dem Gebiet der Sicherheitstechnik zur Verbesserung sicherheitsmethodischer Vorgehenskonzepte und**
- **Rückkopplung in die einzelnen Technikfelder.**

Fazit



- Übertragung der systematisch erarbeiteten Sicherheitskonzepte in Projekt- und Systemspezifikationen
- Systembezogenen Anforderungen an die Gestaltung des gesamten Systems und seiner Baueinheiten bzw. Funktionselemente müssen übernommen werden
- Festlegung von Sicherheitsanforderungen für die Nachweisführung und zur Erlangung von Betriebs-genehmigungen

Fazit

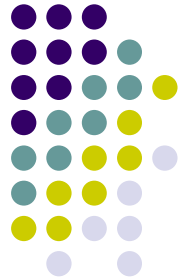


- **Die Vorgehens- und Entscheidungsmethodik (Handlungsschema) bildet die geeignete Arbeitsgrundlage, um Entscheidungen zur Angemessenheit sicherheitstechnischer Gestaltungsmerkmale systematisch zu entwickeln und zu beurteilen**

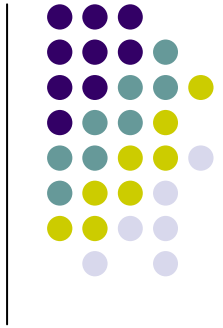
- **Unterschiedlichen Vorgehensweisen in verschiedenen Fachdisziplinen können damit überwunden werden.**

- **Erfassung und Auswertung aller auftretenden sicherheitskritischen Versagensformen für den gesamten Produkt-Lebenszyklus als „lessons learned“ zur Erfahrungsrückführung**

Botschaft



- ***Das Handlungsschema zur Erzeugung von Sicherheit in allen Fachbereichen der Technik ist grundsätzlich universell anwendbar***
- ***Die Wirtschaft muss sich die Technik des Handlungsschemas erarbeiten, da die Sicherheitsverantwortung oft ganz, aber sicher zum Teil beim Hersteller / Betreiber verbleibt***
- ***Die VDI-Richtlinien beschreiben im Regelungsraum einen möglichen Weg; Innovationsprozesse dürfen nicht in einer Institutionenmatrix erstarren***



Vielen Dank für Ihre Aufmerksamkeit