H·I·T·S Engineering

Hoch-Integre Technische Systeme

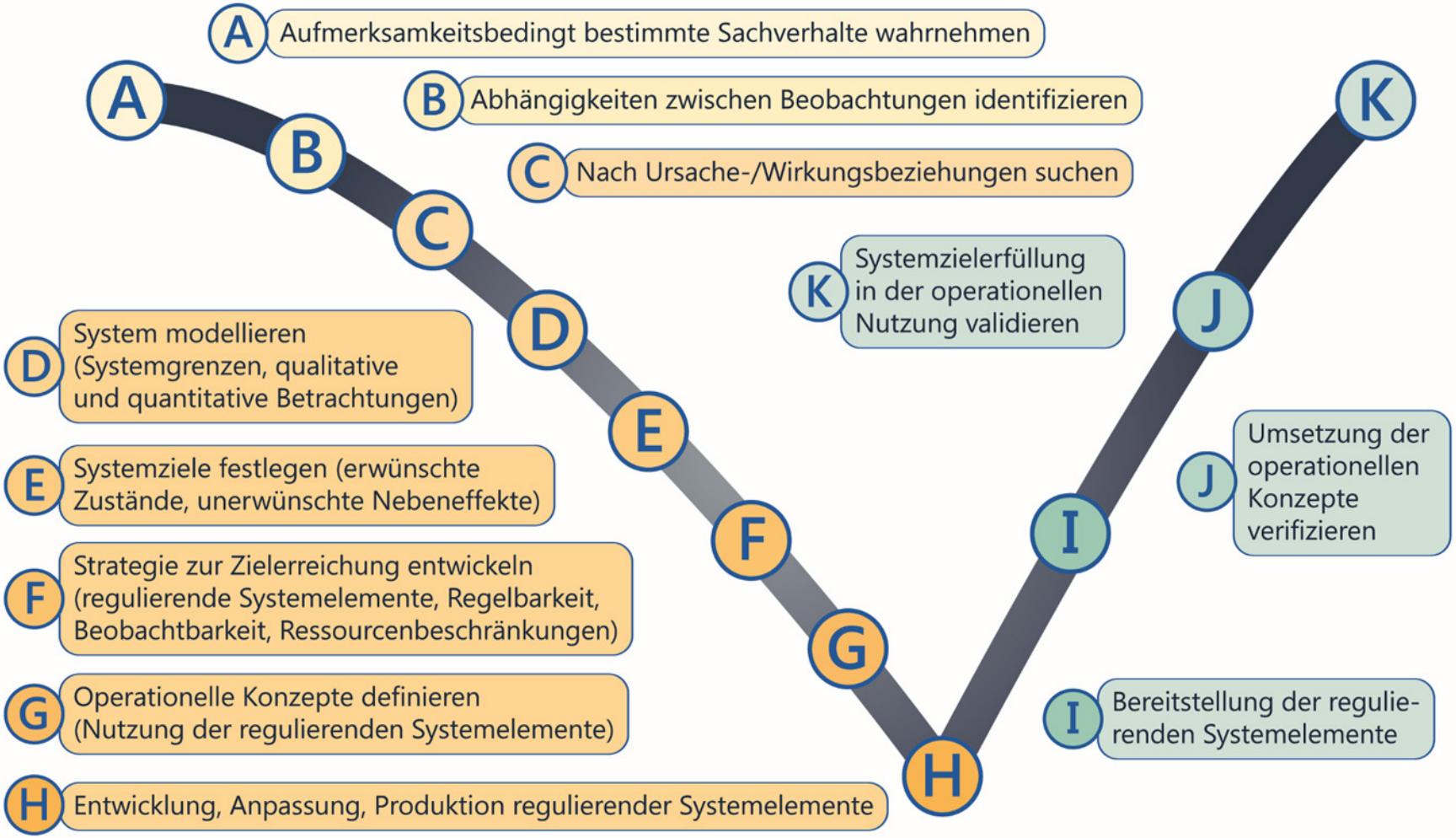
Dieter Scheithauer
Dr.-Ing., INCOSE ESEP

26.10.2016

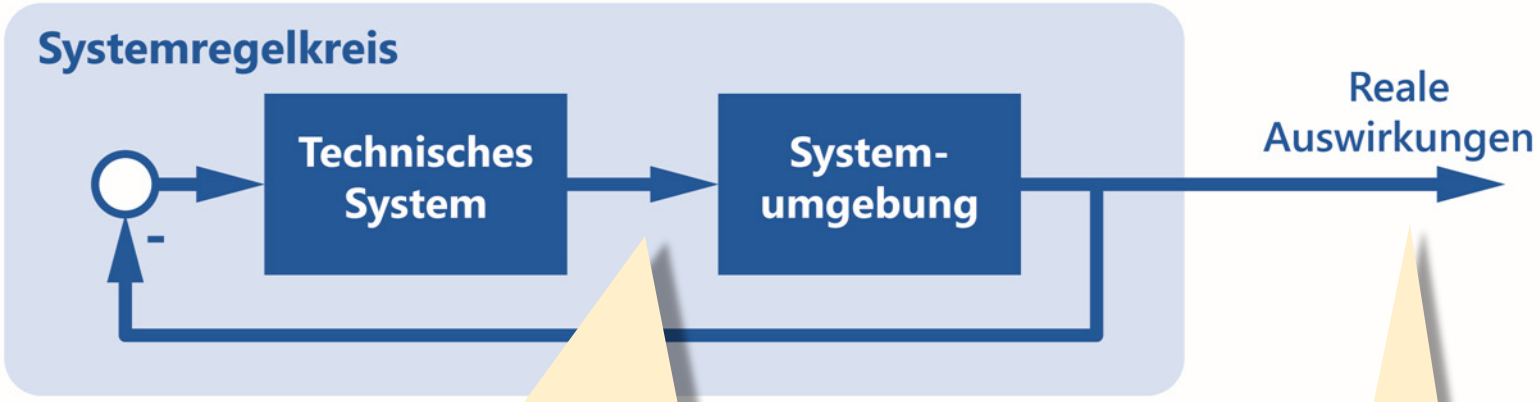
Inhalt

- Vom Problem zum System
- Der Systemregelkreis
- Systemintegrität
- Systemintegrität und Systemarchitektur
- Systemintegrität und der Systems-Engineering-Prozess
- Zusammenfassung

Systementwicklungsschritte



Der Systemregelkreis



- Haftung und funktionale Sicherheit aus Sicht des Technischen Systems
- Technisches System soll bei beabsichtigtem und vorhersehbarem Gebrauch keine Personen- oder Vermögensschäden verursachen
- Fehler im Technischen System sollen zu keinen Schäden in der Systemumgebung führen

- Systemintegrität
- Betrachtung der Systemumgebung als offenes System

Systemintegrität

Komplexität durch intendierte Globalisierung

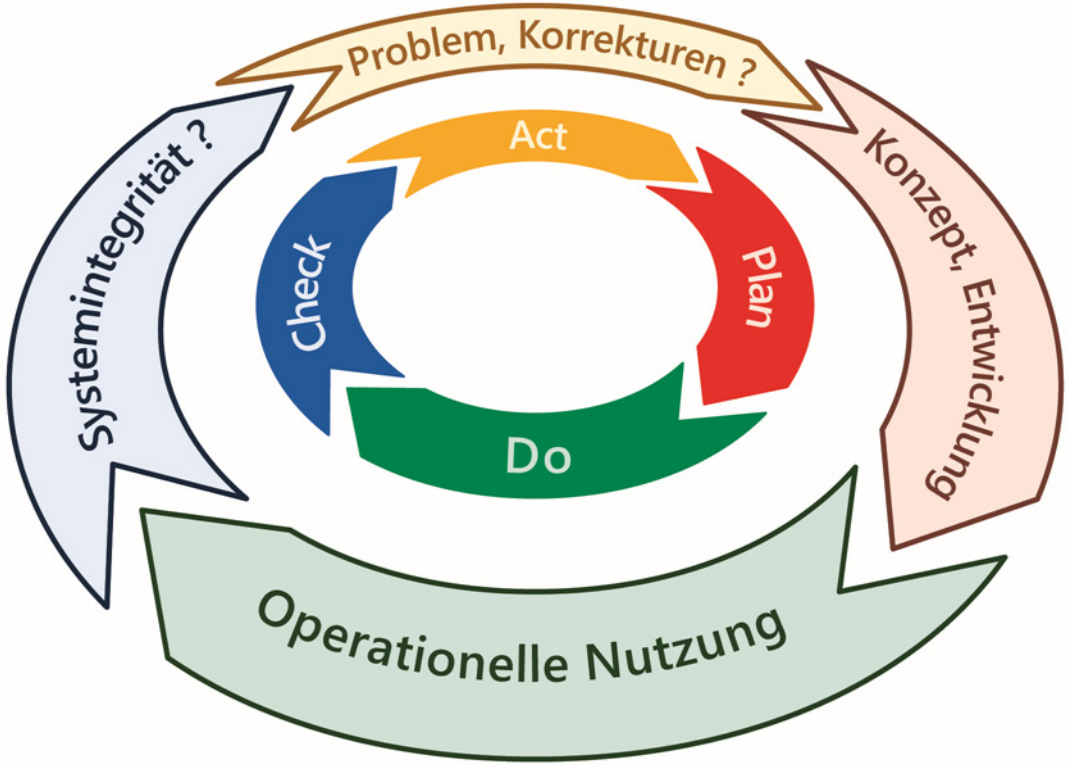
- Warenaustausch
- Finanztransaktionen
- Globale Umweltauswirkungen

Komplexität durch Ressourcennutzung am Limit

- Prinzip der kleinen Abweichung, wenn überhaupt, nur anwendbar bei Ausweitung der Systemgrenzen

Systemintegrität

- System wirkt nachhaltig
- Systemverhalten entspricht den Erwartungen unter allen Umgebungsbedingungen



Systemintegrität und Systemarchitektur

Design-Prinzipien

- Jedes Technische System in der Systemarchitektur stellt seine Integrität selbst sicher
- Jedes Technische System reagiert fehlertolerant auf unerwartete Bedingungen in der Systemumgebung
- Falls menschliche Eingriffe zur erfolgreichen Fehleridentifikation und Rekonfiguration nicht möglich sind, muss das Redundanzmanagement automatisiert erfolgen
- Die Einrichtungen des Redundanzmanagements müssen dabei die Integritätsforderungen an das Technische System erfüllen

Redundanzmanagement

- Fehleridentifikation
  - Fehler sicher erkennen
  - Temporäres Rauschen ignorieren
- Fehlerisolierung
  - Vorübergehende Begrenzung der Auswirkungen
  - Beständige Begrenzung der Auswirkungen
- Rekonfiguration des Systems
  - Aufrechterhaltung der vollen Funktionsfähigkeit
  - Begrenzte oder alternative Funktionalität (Graceful Degradation)
- Minimierung von Fehlertransienten
  - Beim Übergang zwischen Betriebszuständen bleiben alle Zustände beherrschbar

Systemintegrität und der Systems-Engineering-Prozess

- Eine hohe Qualität des Systems-Engineering-Prozesses ist unabdingbar, um
  - belastbare Voraussagen zur Systemintegrität machen zu können
  - die Systemintegrität auch bei Fehlverhalten des Technischen Systems zu gewährleisten
- Zur Beherrschung der Integrität von Software ist die Qualität der Systems-Engineering- und Software-Entwicklungsprozesse allein ausschlaggebend
  - Stochastische Prognosemodelle streuen im Vergleich zu denen für elektronische Hardware zu sehr
  - Statistisch abgesicherte Aussagen zur Systemintegrität sind in der Praxis durch keine Nachweismethode nicht hinreichend gewinnbar
  - Es gilt die Zahl der Nadeln im Heuhaufen zu minimieren

Zusammenfassung

- Technische Systeme sollen eine regulierende Wirkung auf das übergeordnete System ausüben
- Systemintegrität ist ein Maß für Nachhaltigkeit im Sinne der Erfüllung von Erwartungen
- Technische Systeme dürfen die Systemintegrität nicht gefährden, indem sie
  - die eigene Funktionsfähigkeit überwachen und
  - sich bei Teil- und Totalausfällen, ohne kritische Zustände im übergeordneten System auszulösen
- Die Entwicklung Hoch-Integrer Technischer Systeme bedarf einer hohen Prozessqualität

Danke

für Ihre Aufmerksamkeit

Dieter Scheithauer
Dr.-Ing., INCOSE ESEP

H·I·T·S Engineering

Breitensteinstraße 26
83727 Schliersee
Deutschland

Telefon: +49 (0) 80 26 - 97 68 00
Fax: +49 (0) 80 26 - 97 67 99
Mobil: +49 (0) 170 - 23 50 23 4

dieter.scheithauer@hitseng.eu
www.hitseng.eu