GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

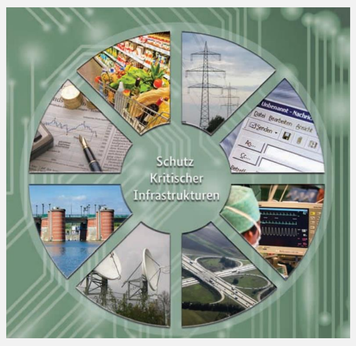
SURF Systemic Security for Critical Infrastructures

SURF-Förderkennzeichen: 16KIS0140
BMBF Förderschwerpunkt: IT-Sicherheit für Kritische Infrastrukturen" (IKT 2020)

Erste Jahreskonferenz und Auftaktveranstaltung des Förderschwerpunkts:
“IT-Sicherheit für Kritische Infrastrukturen“ ,15.-17.07.2015, SGL Arena in Augsburg

Motivation

Schutz Kritischer Infrastrukturen (KRITIS) + **Neue Anforderungen der KRITIS** → **Herausforderungen**



(Bildquelle: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Flyer.pdf?__blob=publicationFile)

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur

- Hochleistungsfähige IT-Systeme für den Betrieb notwendig
- Zunehmende Vernetzung
  - Offene Zugänge zum Internet
  - Mobile Geräte
  - Fernwartungen
- Hohe Verfügbarkeitsanforderungen
- Heterogene Systeme, teilweise Legacy-Systeme

http://www.deutsches-museum.de/ausstellungen/kommunikation/informatik/universalrechner/

- Seltene Wartungsfenster
- Sicherheitsaspekte blieben bisher hinter Safety-Anforderungen zurück
- Erschwerter Zugriff auf Informationen in Bezug auf Gerätestatus
- Hohes Schadenspotential im Fehler- bzw. Angriffsfall

Stromausfall in den USA (Bildquelle:http://beyondtheborderobserver.org/2013/08/14/)

Urananreicherungsanlage in Natanz nach Stuxnet (Bildquelle: http://www.zeit.de)

Hacking Angriff auf JP Morgan (Bildquelle: http://www.spiegel.de)

Zielsetzung

Übergeordnete Ziele + **Wissenschaftlich-technische Einzelziele**

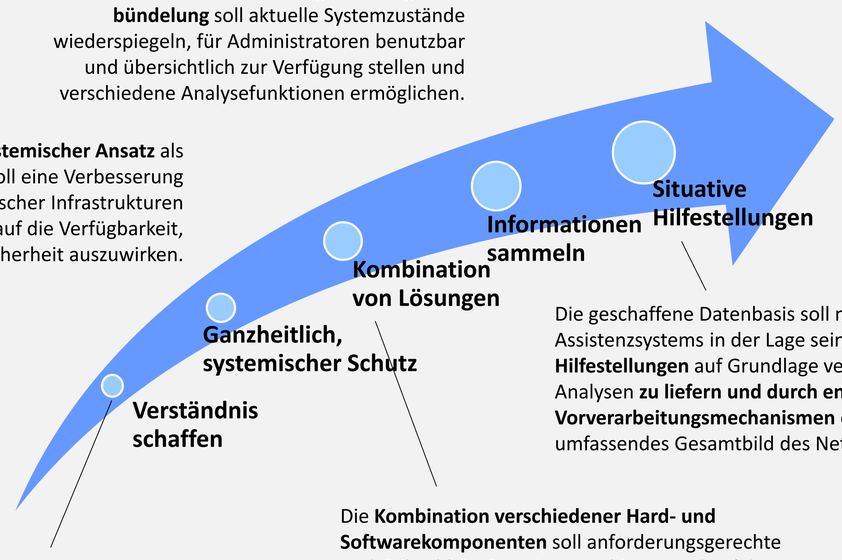
- Verbesserung der IT-Sicherheit kritischer Infrastrukturen ohne Abstriche an Verfügbarkeit, Betriebssicherheit und Personensicherheit
- Vollfunktionale Einbettung von Altsystemen, ohne Verletzung existierender Safety-Zertifizierungen
- Dezentralisierung der IT-Struktur, um fatale Angriffe auf Kontrollzentren zu vermeiden
- Assistenzsysteme zu Erkennung, Lokalisierung und Abwehr von Angriffen

- Analyse der Anforderungen kritischer Infrastrukturen und Modellierung der Infrastrukturen
- Realitätsnahe Modellierung einer komplexen kritischen Infrastruktur
- Priorisierung der Sicherheitsvorfälle
- Assistenzsystem zur Reaktionsunterstützung
- Vorschaltgerät zur Absicherung der Kommunikation zwischen den Subsystemen einer kritischen Infrastruktur
- Architektur der Sicherheitsinfrastruktur
- Messsonde zur Datenerfassung und -vorbearbeitung
- effektvolle Visualisierung der Reaktionsempfehlungen

Projektphasen

Die Verlässliche **Informationsgewinnung und -bündelung** soll aktuelle Systemzustände wiederspiegeln, für Administratoren benutzbar und übersichtlich zur Verfügung stellen und verschiedene Analysefunktionen ermöglichen.

Ein **ganzheitlicher, systemischer Ansatz** als integriertes Schutzkonzept soll eine Verbesserung der IT-Sicherheit kritischer Infrastrukturen erreichen ohne sich negativ auf die Verfügbarkeit, Betriebs- oder Personensicherheit auszuwirken.



Die Schaffung eines **gemeinsamen Verständnisses** für die Anforderungen und Besonderheiten Kritischer Infrastrukturen bildet ein wichtiges Fundament für entstehende Modelle, Analysen und Soft- sowie Hardwarekomponenten.

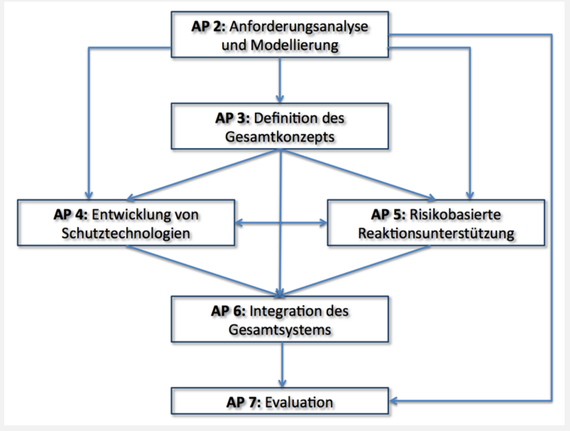
Die geschaffene Datenbasis soll mittels eines Assistenzsystems in der Lage sein, **situative Hilfestellungen** auf Grundlage verschiedener Analysen **zu liefern und durch entsprechende Vorverarbeitungsmechanismen** ein umfassendes Gesamtbild des Netzes liefern.

Die **Kombination verschiedener Hard- und Softwarekomponenten** soll anforderungsgerechte und risikoabhängige Lösungen bieten und auf dem Fundament eines *Resilient Cores* zuverlässig und kosteneffizient arbeiten.

Lösungsansatz

(Bildquelle: Infineon Technologies AG)

Projektstruktur + **Handlungsfelder** → **Rolle der Partner**



- Erfassung und Strukturierung der Anforderungen der KRITIS
- Identifikation geeigneter Modelle zur Risikoabschätzung
- Auswahl von Metriken zur Beschreibung des Systemzustands
- Architektur der Sicherheitsinfrastruktur: Resilient Core; Netzwerkmonitoring-Tools und zugehörige Analyselogik zur Erkennung/Behandeln von Angriffen bzw. Fehlkonfigurationen
- Vorschaltgerät zur Kommunikationssicherung
- Messsonden zur Vorverarbeitung von Rohdaten der Sicherheitsinfrasturktur
- Verfügbarkeitsmodellierung: Gesamtsystemverfügbarkeit, Betrachtung von möglichen Ausfällen, Laufzeitmonitoring
- Priorisierungsmechanismus für eingehende Alarmmeldungen
- Situationsbasiertes Assistenzsystem
- Visualisierung und Darstellung für Benutzer

- Auf HW-Komponenten aufbauend Daten über den Systemstatus erfassen
- Aus Konfigurationen der Netzkomponenten Metadaten sammeln
- Externe Messsonden an zentrale Infrastruktur anbinden (Fernwartungen) und Testinfrastrukturen kombinieren
- Metadaten sichtbar machen und dem Anwender bereitstellen
- Aufbau eines *Resilient Cores* für dezentralen Schutz

SURF Projekteckdaten

SURF - Systemic Security for Critical Infrastructures
Laufzeit: 01.09.2014 – 31.08.2016 , 24 Monate
Budget / Förderung: ca. 4 Mio€ / ca. 3.1 Mio€
Koordinator: Infineon Technologies AG
TU München, Lehrstuhl für Netzarchitekturen und Netzdienste
Web page: https://www.net.in.tum.de/html/surf

Konsortium

Anwender | **Unternehmen** | **Forschungseinrichtungen**

AIRBUS GROUP, Infineon, Fraunhofer SIT, THD Technische Hochschule Deggendorf, M, HIRSCHMANN A BELDEN BRAND, TUM Technische Universität München

Koordination

Dr.-Ing. Florian Schreiner
+49 89 234 21833
Florian.schreiner@infineon.com

Madeleine Meier
+49 89 234 21516
Madeleine.meier@infineon.com

Prof. Dr.-Ing. Georg Carle
+49 89 289 18030
carle@net.in.tum.de

Nadine Herold
+49 89 289 18038
herold@net.in.tum.de