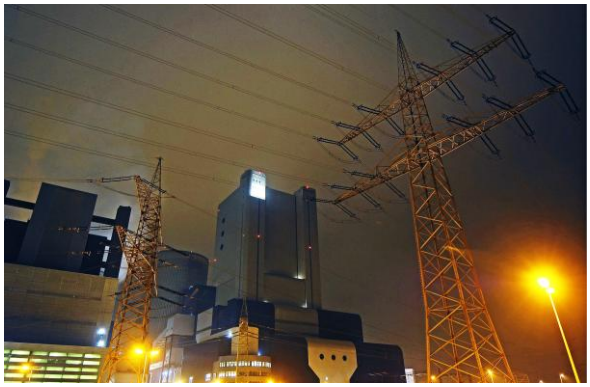
CritInfr – Schutz von kritischen Infrastrukturen

Kritische Infrastrukturen sind in unterschiedlicher Weise gefährdet. Die Erkennung sowie Klassifikation von Anomalien und Bedrohungen mittels geeigneter technischer Verfahren, Methoden und Systeme ist Ziel des Projekts. Automatische bzw. unterstützende Systeme werden konzipiert und vorgeschlagen.



Die deutsche Bundesregierung definiert Kritische Infrastrukturen (KRITIS) als Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Neben dem Ausfall dieser Einrichtungen sind Gefährdungen der Bevölkerung durch die Anbindung der Kunden und Haushalte an die zentralen Versorgungseinrichtungen, und die damit mögliche breit gestreute Verteilung von Schadstoffen, möglich.

Angreifbar sind die Einrichtungen in den Bereichen Informations- und Kommunikationstechnik, funktionale Technik, Logistik, Personal, in der Produktion und in der Qualitätssicherung. Die Kontamination der Lieferprodukte ist eine Gefahr für alle Abnehmer.

Verursacher können von außen, aber auch innerhalb der Einrichtungen agieren und unterschiedliche Wirkmittel einsetzen. Es muss berücksichtigt werden, dass Prognosen zur Art und Ausführung des Angriffs grundsätzlich nur sehr eingeschränkt möglich sind.

Ziel des Projekts ist einführend eine Aufstellung der Gefährdungen, Risiken, Wirkweisen und der bestehenden Abwehrmechanismen. Hauptziel ist die Erarbeitung von Konzepten für technische Unterstützungs- und Assistenzsysteme, um damit Anomalien, Gefährdungen und Angriffe möglichst frühzeitig zu erkennen. Die laufende Überwachung des Betriebs, der Prozesse und der Qualität der Lieferprodukte mittels technischer Sensoren, Signalverarbeitung, Klassifikation und der Analyse von Fallbeispielen sind Bestandteil von Lösungen, um zu warnen und geeignete Gegenmaßnahmen einleiten zu können.

Das Projekt umfasst die folgenden Arbeiten zur Analyse und Konzepterstellung.

Gefährdung - Bedrohung
- Analyse unterschiedlicher Gefährdungspotenziale
- Risiken, Motive, Angriffsszenarien, Gefährdungspotenzial.

Fähigkeiten in der Erkennung und Abwehr
- Fähigkeiten und Maßnahmen der Betreiber
- Fähigkeiten der Sicherheitsbehörden.

Fähigkeitslücken
- Bedarf, Wirtschaftlichkeit
- marktverfügbare Produkte, Sensoren etc.
- Auswertung, Analyse, Klassifikation
- Datenbanken, auch übergreifend vernetzt (Fallanalysen)
- Bedarf, Forschung und Entwicklung.

Recht und Gesetz
- gesetzliche Rahmenbedingungen.

Maßnahmen und Schwerpunkte
- Möglichkeiten zur Erkennung und Abwehr mit technischen Mitteln
- Sensorik, Klassifikation, Erkennung von Anomalien
- Geschäftsprozesse
- Checklisten
- Schulungsbedarf
- Technik & Mitarbeiter - Assistenzsysteme.

Produkte und Markt
- Markt für erweiterte Lösungen
- Potenzial für innovative Produkte.

Ziel ist nicht die Analyse von Schwachstellen in einer speziellen Einrichtung sondern vielmehr eine übergreifende Betrachtung im Hinblick auf technische Unterstützungsmittel. Die enge Zusammenarbeit mit Partnern aus dem einschlägigen Umfeld ist wichtig, um die Fachexpertise aus der Praxis einzubringen. Erfolgversprechende technische Lösungsvorschläge, bestehend aus Sensorik, Signalverarbeitung, Klassifikation und Mustererkennung, werden erarbeitet und auf ihre Realisierbarkeit und breite Einsatzmöglichkeit untersucht.

Technologie	Sensorik, Signalverarbeitung Mustererkennung, Klassifikation, KI (künstliche Intelligenz) Fallbasiertes Schließen (case-based reasoning), Datenbanken
Märkte	Versorger, Stadtwerke, Verkehrsbetriebe
Anmerkungen	Für deutsche Bedarfsträger sind die Richtlinien zur Fördermaßnahme "Anwender – Innovativ: Forschung für die zivile Sicherheit" (Bundesanzeiger vom 11.05.2016), interessant.