

Anwendungsorientierte Sicherheitsforschung für mehr Resilienz in KRITIS

Identifikation von sicherheitsrelevanten Anomalien in kritischen Infrastrukturen

Keywords

Kritische Infrastrukturen, Versorgungsunternehmen, Wasserversorgung, Sensorsignalverarbeitung, Mustererkennung, Informationsfusion, Deep-Learning, fallbasiertes Schließen, Künstliche Intelligenz, Anomalie-Erkennung.

Kurzbeschreibung

Innere und zivile Sicherheit beschäftigen unsere Gesellschaft. Kriminell motivierte Anschläge und global initiierte Terrorakte sind keine abstrakten Nachrichten mehr, sondern finden inmitten unserer Gesellschaft statt. Pläne für vielfältige und unterschiedlich motivierte Angriffe gegen kritische Infrastrukturen (KRITIS) wurden bekannt, sind Teil von Risikoanalysen und begründen Forderungen nach Reaktionen und Gegenmaßnahmen.

Die Auswirkungen materialisierter Bedrohungen und Gefährdungen für die Gesellschaft können sein:

- Störungen oder Ausfall der Versorgung, vorübergehend oder dauerhaft
- Zerstörung von Anlagenteilen, verbunden mit Stillstand, Ausfällen und/oder Personenschäden
- Kontamination der Anlage, der Umwelt oder auch der Lieferprodukte
- wirtschaftliche Schäden durch Zerstörungen und Produktionsausfall
- nachhaltiger Vertrauensverlust in die Leistungsfähigkeit des Staates, seiner Organe und der Versorgungsunternehmen verbunden mit der Bereitschaft, extreme Positionen in der Gesellschaft zu vertreten.

Die Stärkung technischer Großanlagen gegen die Auswirkungen von Angriffen, Störungen und auch menschlichem Fehlverhalten im Innenbereich muss Teil eines umfassenden Sicherheitskonzepts sein. Forschung ist notwendig, um sicherheitsrelevante Ereignisse außerhalb des Regelbetriebs identifizieren zu können. ISAKI fokussiert exemplarisch die Versorgung mit Wasser und Energie mit den Erlanger Stadtwerken als Anwender. Ziel ist die Erhöhung der Resilienz im Krisen und Katastrophenfall.

Identifikation von sicherheitsrelevanten Anomalien in kritischen Infrastrukturen (KRITIS) mit dem Schwerpunkt auf Wasser- und Energieversorgungsanlagen für die Erlanger Stadtwerke AG als Anwender



Förderung
im Rahmen
Anwender-Innovativ II

Bundesministerium
für Bildung
und Forschung

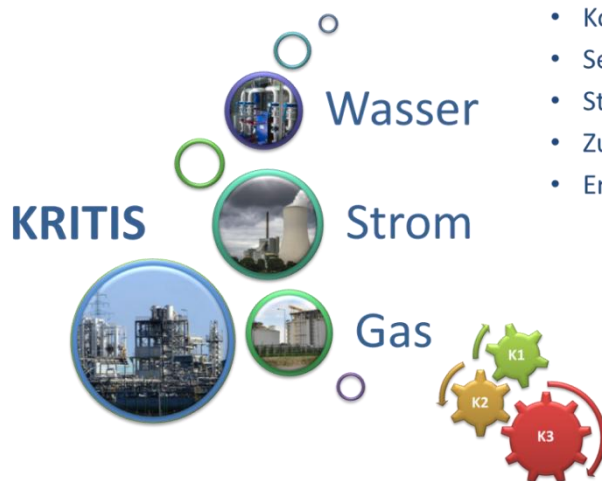
metropol
region
nürnberg

ISAKI - Identifikation von Sicherheitsrelevanten Anomalien in Kritischen Infrastrukturen

Geeignete Technik und angepasste Geschäftsprozesse sollen:

- prädiktiv und präventiv wirken
- Vorwarnzeiten erhöhen
- die Anlagenführer unterstützen
- die Zusammenarbeit mit den Sicherheitsbehörden sichern
- geeignet sein, die Zusammenarbeit der Versorgungsunternehmen untereinander zu fördern
- Gefahren und wirtschaftliche Schäden vermeiden
- die Anlagenfunktionalität und die Versorgungsfähigkeit sichern.

ISAKI ist ausgerichtet auf die möglichst frühzeitige Erkennung von seltenen und unerwarteten Anomalien, verursacht durch Kriminalität, Terrorismus oder vergleichbare Bedrohungen in komplexen, räumlich verteilten Anlagen, die mittels der Steuer-, Regelungs- und Leittechnik der technischen Subsysteme nicht oder erst (zu) spät erkannt werden. Die Komplexität der Anlage und des Umfelds begründet die besonderen Herausforderungen.



- Komponenten diverser Hersteller
- Separate Leit-, Steuer- und Kontrolltechnik
- Störfallorientierte Sicherheitstechnik
- Zusätzliche Überwachungseinrichtungen
- Erfahrung und Routine der Anlagenführer

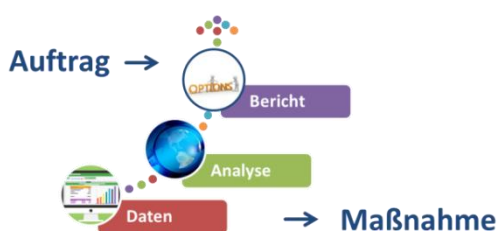


Entscheidend ist die umfassende und übergreifende Berücksichtigung, Fusion und Analyse von Daten und Informationen aus dem Prozess, offenen Quellen und Lagebildern der Sicherheitsbehörden sowie gesicherter Erkenntnisse. Ergebnis sind regelmäßige Lageberichte zur Vorlage bei der Geschäftsleitung.



- Massendatenerfassung und -speicherung
- Sensordaten und unstrukturierte Informationen
- Fusion von Daten und Informationen in Graphdatenbanken
- Statistische und semantische Verfahren
- Training von Modellen und künstliche Intelligenz

... helfen den Anlagenführern und dem KRITIS Management bei der Informationserfassung, Aufbereitung und Analyse bis hin zu Warnungen, Alarmen und Status- sowie Lageberichten.

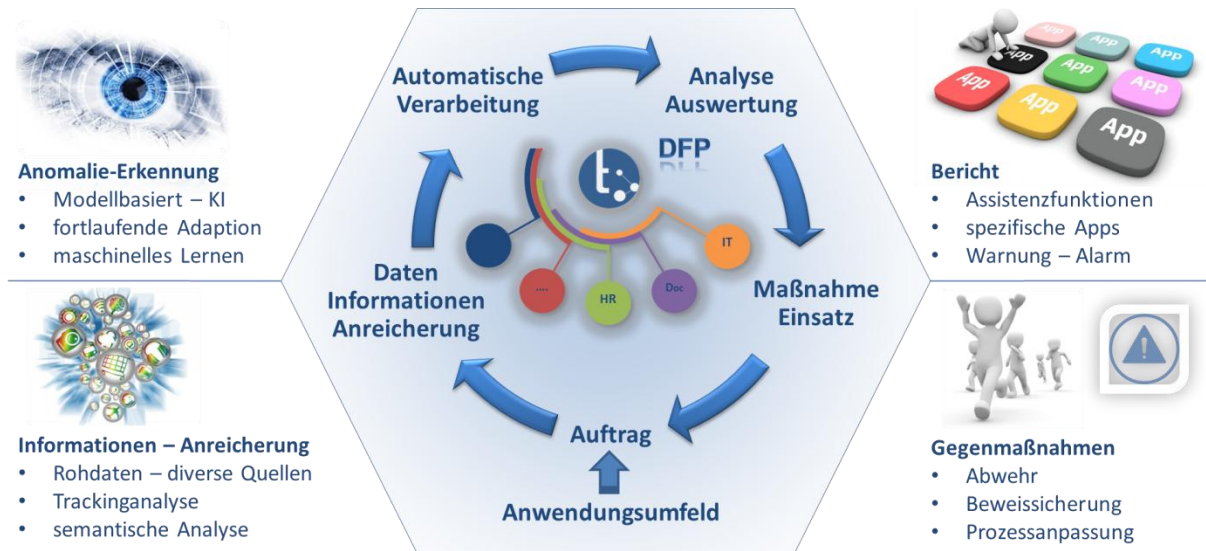


Intelligence Cycle – ein bewährtes Prozessmodell

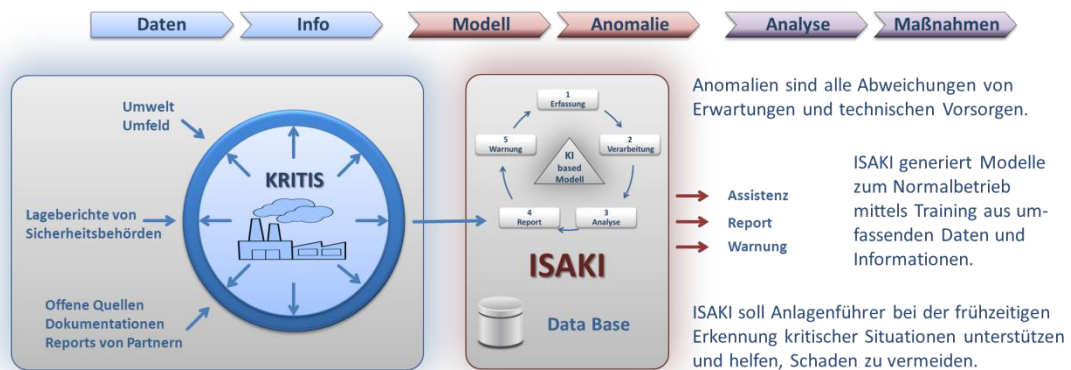
- | | |
|---|---|
| <ol style="list-style-type: none"> 1. Request 2. Planning 3. Collection 4. Processing 5. Analysis 6. Report 7. Dissemination | Assistenzsystem zur Unterstützung :
<ul style="list-style-type: none"> • Effektivität • Effizienz • Motivation. |
|---|---|

ISAKI - Identifikation von Sicherheitsrelevanten Anomalien in Kritischen Infrastrukturen

Der sogenannte „Intelligence Cycle“ beschreibt den Prozess der Informationserfassung, Verarbeitung, Analyse und Aggregation. Bewährte Verfahren kommen zur Anwendung und werden mit neuen Erkenntnissen aus der Forschung angereichert.



Modellbasierte Verfahren werden zur automatisierten Erfassung und Aggregation der Daten und Informationen eingesetzt. Diese Ansätze kennzeichnen auch das Innovationspotenzial.



Das Ziel wird durch die Erfassung, Fusion, Analyse und Klassifikation von strukturierten sowie unstrukturierten Daten und Informationen sowie deren zeitliche Abfolgen realisiert. Eingeschlossen ist auch die Berücksichtigung von Informationen aus hoheitlichen Lageberichten und offenen Quellen zu Veränderungen der Risikolage mit langer Vorwarnzeit. Aspekte der IT-Sicherheit stehen nicht im Vordergrund der Forschung; die Lösung wird aber fähig sein, Informationen auch aus IT-Sicherheitskomponenten zu berücksichtigen.

ISAKI soll mittels eines geeigneten IT-Demonstrators exemplarisch Hinweise auf mögliche sicherheitsrelevante Vorgänge und Situationen für den Wasserversorgungsbereich der Erlanger Stadtwerke AG (ESTW) als Anwender liefern. Das folgende Bild veranschaulicht den Informationsfluss und die Ziele.

ISAKI - Identifikation von Sicherheitsrelevanten Anomalien in Kritischen Infrastrukturen



Der Stand der Technik soll durch das Projekt überzeugend verbessert werden, die Grundlagen für die anschließende Nutzung der Ergebnisse schaffen sowie die Anschlussfähigkeit in den Bereichen: Wissenschaft, Lehre, wirtschaftliche Verwertung gewährleisten.

Idealerweise gelingt es im Rahmen des Projekts außerdem, Versorgungsunternehmen untereinander und mit den staatlichen Sicherheitsbehörden zu vernetzen sowie das Teilen von sicherheitsrelevanten Informationen anzustoßen.

Das Projekt ISAKI bietet mit einem interdisziplinären Team beste Voraussetzungen dafür, entscheidende Fortschritte und Erkenntnisse zu gewinnen, die Grundlagen für nachfolgende Entwicklungen von Innovationen sind.



Die Arbeitsgemeinschaft verbindet den Bedarf und die Erfahrungen des Anwenders, Forschung, Erfahrungen und Interessen. Anwender sind die Erlanger Stadtwerke, mit dem Schwerpunkt Wasser und Energie. Forschungsarbeiten im Bereich der Modellbildung, Mustererkennung und Klassifikation werden von der TU Nürnberg geleistet. Das Start-Up Traversals Analytics and Intelligence kümmert sich um den Demonstrator mit einer später geplanten Überleitung in eine Innovation. Sicherheitsbehörden, deren Erfahrungen und Interessen werden von dem Polizeipräsidium Mittelfranken vertreten. DITS.center bringt sich mit einem Netzwerk und umfangreichen Erfahrungen in Sicherheitsaspekten

mit einem interdisziplinären Team ein.

ISAKI Ergebnisse sind potenziell breit anwendbar zur Erkennung von Anomalien in komplexen, räumlich verteilten Anlagen, die mittels der Steuer-, Regelungs- und Leittechnik der technischen Subsysteme nicht oder erst (zu) spät erkannt werden.

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Wir danken dem BMBF für die Förderung des Vorhabens im Rahmen des Programms „Anwender – Innovativ: Forschung für die zivile Sicherheit II“.