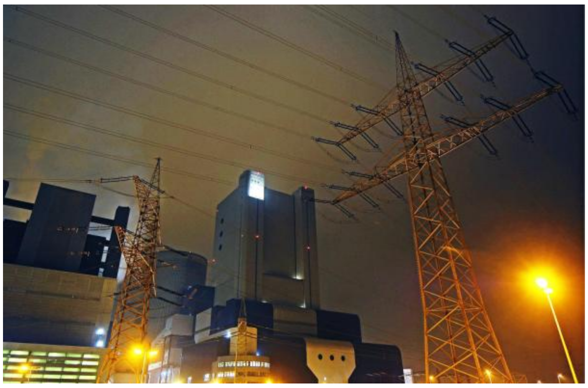
DITS.center e.V.

CritInfr – Critical infrastructures and security

Critical infrastructures are endangered in different ways. The identification and classification of anomalies and threats by means of appropriate technical procedures, methods and systems are the aim of the project. Automated or assistance systems are analyzed, designed and proposed.



The German Federal Government defines Critical Infrastructures (KRITIS) as organizations or institutions of great importance to the state community whose failure or impairment could lead to sustained shortages, serious disruption to public security or other dramatic consequences. In addition to the failure of these facilities, dangers to the population are a consequence of customers' and private households' links to the central supply facilities and the possible distribution of pollutants.

The facilities can be attacked in the areas of information and communication technology, functional technology, logistics, personnel, production and quality. The contamination of the delivery products is a threat for all customers.

Attackers can act from the outside, but also within the facilities and use different methods of attack and action. It has to be taken into account that, as a matter of principle, possibilities for the prediction of the nature and execution of the attack are very limited.

The aim of the project is to introduce a list of the threats, risks, effects and the existing defence mechanisms. The main goal is the development of concepts for technical support and assistance systems in order to detect anomalies, hazards and attacks as early as possible. The real-time monitoring of the operation, the processes and the quality of the delivery products by means of technical sensors, signal processing, classification and the analysis of cases are part of solutions to warn and to take appropriate countermeasures.

The project includes the following work packages on analysis and conceptualization.

Hazard - threat
- Analysis of different potential hazards
- Risks, motives, attack scenarios, potential hazards.

Abilities in detection and defense
- Skills and measures of operators
- Abilities of the security authorities.

Capability gaps
- Need, cost and benefit
- Marketable products, sensors, etc.
- Evaluation, analysis, classification
- Databases, also networked, case data bases
- Research and development.

Law and order
- Legal framework.

Measures and priorities
- Possibilities for detection and defense by technical means
- Sensor technology, classification, detection of anomalies
- Business Processes
- Checklists
- Requirements and needs for training
- Technology & Staff - Assistance Systems.

Products and market
- Market for advanced solutions
- Potential for innovative products.

The aim is not the analysis of weaknesses in a specific plant, but rather a general view with regard to technical support resources. The close cooperation with partners from the relevant plants and organizations is important in order to bring the practical experience into practice. Successful technical solutions, consisting of sensor technology, signal processing, classification and pattern recognition, are elaborated and examined for their feasibility and broad application possibilities.

Technology	Sensor technology, signal processing Pattern recognition, classification, AI (artificial intelligence) Case-based reasoning, databases
Markets	Utilities, municipalities, transport companies
Remarks	For German partners, the guidelines for the funding measure "Anwender – Innovativ: Forschung für die zivile Sicherheit" (Bundesanzeiger vom 11.05.2016), are of interest.