PREventivE Methodology and Tools to Protect uTIlitiEs

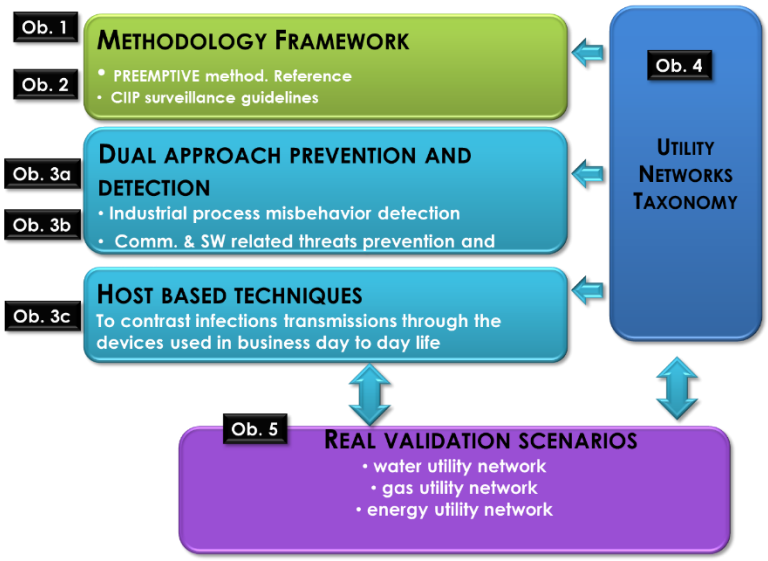
A quick overview of the Project

FP7 - Seventh Framework Programme
Grant agreement no: 607093

Project Overview

The PREEMPTIVE project seeks to prevent and detect cyber-attacks against utilities by developing innovative methods and tools in security risk assessments and intrusion detection.

Project Objectives and Main Outcomes



- Taxonomy – Report
Classifying the utility networks taking into account type and communication technology, sensibility to Cyber threats

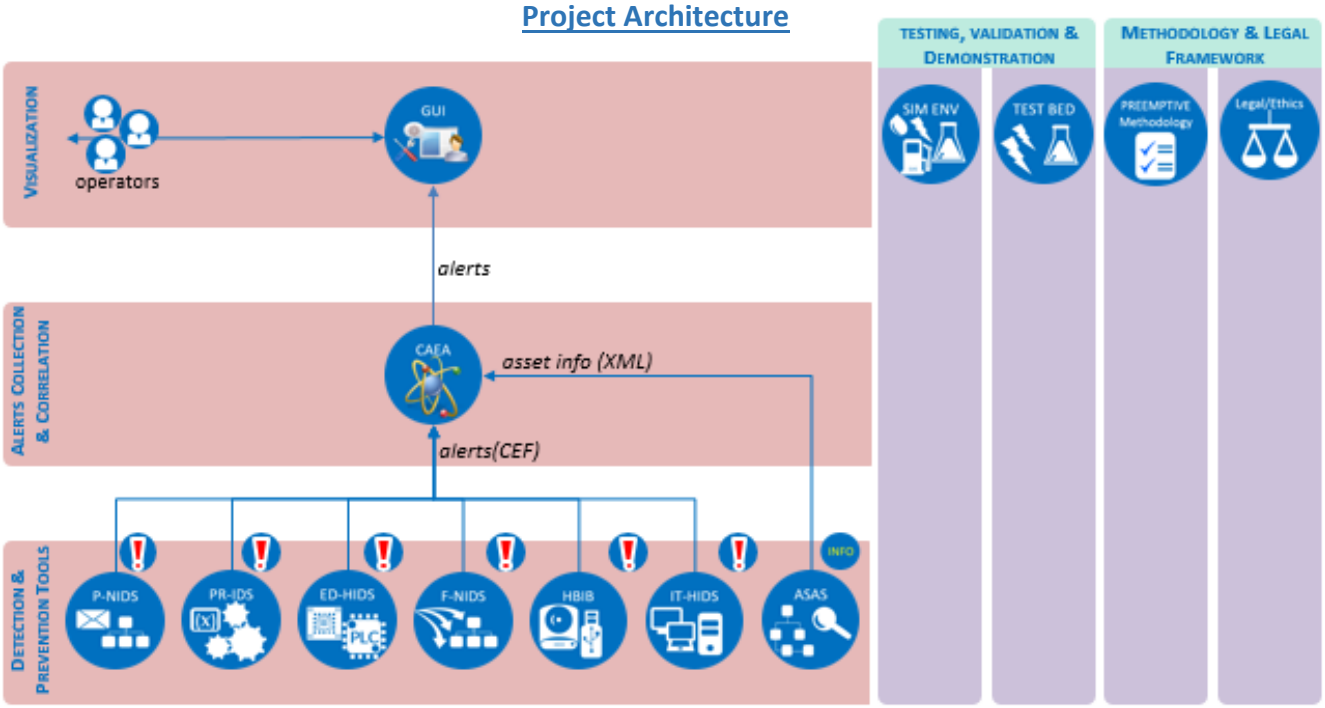
- Modelling – Software
Models and virtual environment for simulating and gathering data on cyber attacks

- Software detection (network, host and process based) and event correlation tools – Software
Prevention and detection tools to improve security on SCADA utility networks

- Cyber Defense Methodology Framework – Guidelines
* Risk and Vunerability Assessment Methods
* Standard policies, procedures and guidelines to prevent cyber attacks

- Ethics, Social Impact – Report
Legal and ethical requirements and implementation report

Project Architecture



Work Packages and their deliverables

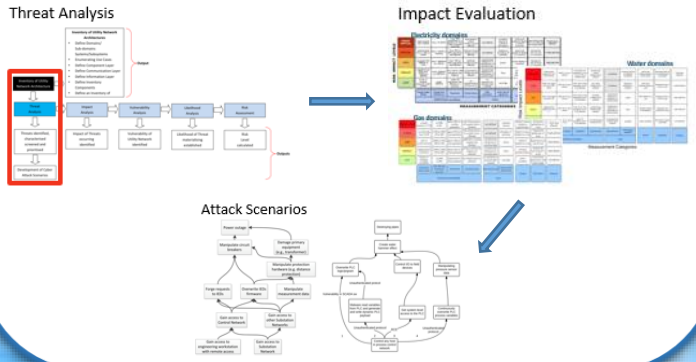
During the first two years of the PREEMPTIVE Project several objectives and milestones have been achieved. Even though the project is only at 2/3, many deliverables have been written and produced and the members are going into the final year for the finishing steps.

In the section below information is given of the most important deliverables done by each Work Package until the third year. This information is a quick overview and does not represent all of the work that has been done. Work Package 1 will not be mentioned as they perform work that is only intended for internal project use.

If more information is required about the deliverables produced in year 1 and 2, please feel free to contact us via our website: **www.preemptive.eu**.

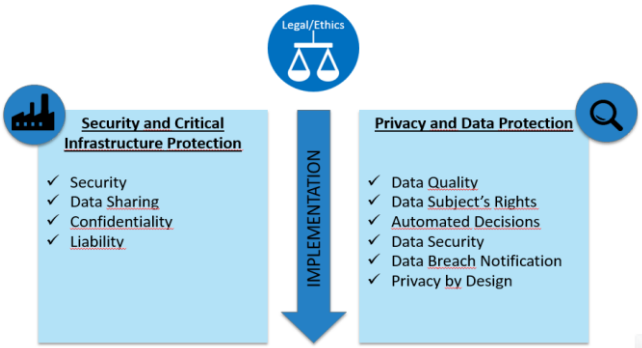
WP2: Utility Network Taxonomy

Work Package 2 created a taxonomy that provided an organized inventory of the components, communication protocols and information assets of Industrial Control Systems used by Electricity, Gas and Water Utilities.
At the same time, the taxonomy presents a number of cyber-attacks which could target these control systems, based on the peculiarities of the process and the control system in each specific domain and the results of threat characterization and domain-specific impact evaluation.



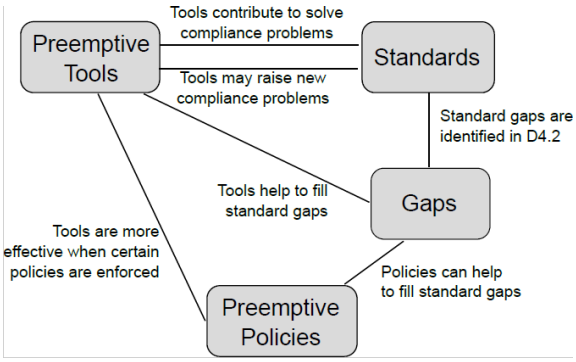
WP3: Ethics, Regulations

Work Package 3 provided guidance concerning the practical implementation of the legal requirements identified during the project's first year.
The implementation guidelines cover key legal areas such as, critical infrastructure protection and security, privacy and data protection. The guidelines aim to assist project partners during the development of the PREEMPTIVE tools, as well as end-users in their implementation of the tools into the production environment.



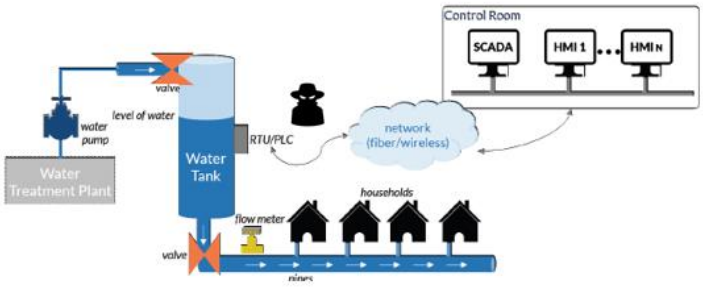
WP4: Methodology Framework

Work package 4 worked on:
- State of the art evaluation of security frameworks, standards and recommendations resulting in a gap analysis
- Development of a Risk Assessment methodology including Asset Identification, Threat Characterization and Vulnerability Assessment for securing utility networks from cyber-attacks.



WP5: Simulation & Modelling

Work Package 5 created a simulation environment for targeting analysis of cyber attacks, producing mass simulation data:
- Targeting attacks in SCADA to PLC communications from Water and Gas facilities
- Targeting attacks in electrical power grid: Line tap changer, MV breaker, AGC set-points and DER control voltage.



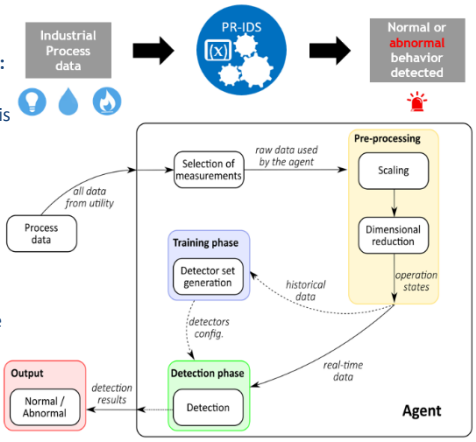
PREEMPTIVE - PREventivE Methodology and Tools to Protect uTILitiEs

WP6: Indus. Process Detection

Work Package 6 worked on:
- The Process-Related Intrusion Detection System is an anomaly-based tool that detects abnormal behaviors at the process level

- A multi-agent approach is adopted to address the complex problem of detecting anomalies in large amounts of process data.

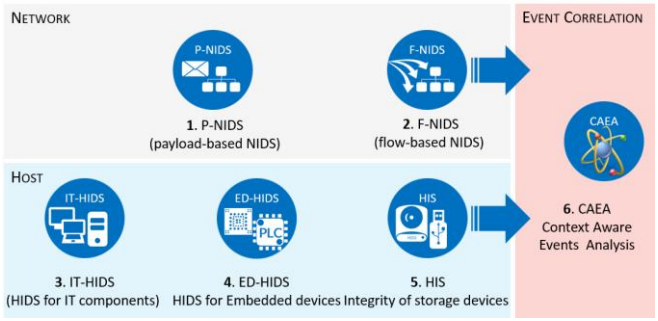
- It is built on a start-of-the-art open source distributed real time computation system Apache Storm.



- The tool operates in two phases: training and detection.
- The tool has been tested and validated with simulated data from WP5 and real data from End-Users.

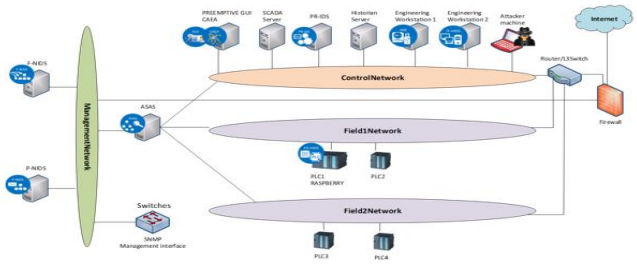
WP7: Comm. And Software Threat Detection

Work Package 7 developed a suite of tools to detect anomalous and malicious activities against critical systems. The tools in their suite aim at:
- Recognize and face new unexpected ways of intrusion;
- Focus on hosts and networks in a ICS/SCADA environment;
- Act at different levels and on different components (e.g. network, standard IT devices, embedded and storage devices) in order to guarantee protection against a wide range of attacks targeting ICS systems.



WP8: Results Validation

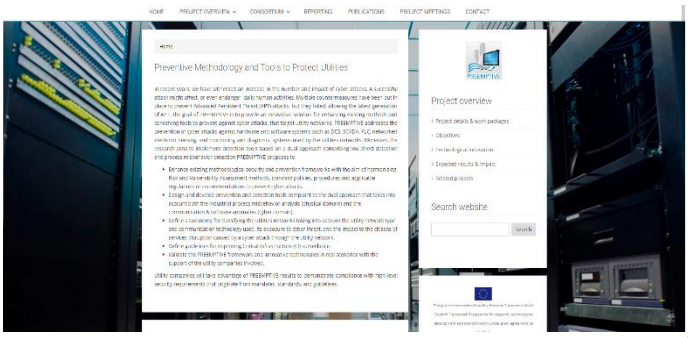
Work Package 8 made a description of the final test bed that will be used during the final live demonstrations.
It is modeled as an industrial network in a reduced configuration that can be exploited in order to running emulated cyber-attacks previously defined in the test plan.



WP9: Dissemination

Work Package 9 worked on dissemination purposes where they updated the PREEMPTIVE website with new deliverables created by the other Work Packages and scientific publications written about / for this project.

In addition to the website, there is a LinkedIn page that will aim for creating more publicity for the project.



The Consortium consists of the following members:

GRUPO AIA
harnser group
IREC
Institut de Recerca en Energia de Catalunya
Catalonia Institute for Energy Research
UNIVERSITEIT TWENTE.
SECURITY MATTERS
ISRAEL ELECTRIC CORPORATION
VITROCISET
ENCS
HWCommunications
Cyber Security and Resilience
Fraunhofer IOSB
iMinds
KU LEUVEN
ROMA TRE
UNIVERSITÀ DEGLI STUDI

End Users and related projects

End Users

The End-User Advisory Board of PREEMPTIVE consists of two partners, IEC and IREC, and five external advisors:

- Electricite de France (France)
- ENERGO (Croatia)
- CETaqua (Spain)
- GAS Natural Fenosa (Spain)
- Poste Italiane (Italy)
- CPL Concordia (Italy)

PREEMPTIVE has End Users in the **Energy**, **Water** and **Gas** domain and they are vital for this project as they give important feedback to improve and fine-tune the PREEMPTIVE methodology and tools.

In addition, the convergence of End Users and researchers will have an important impact on the research in the field: it will generate knowledge in the security research community and a better understanding of the challenges, problems and opportunities associated with critical infrastructure environments.

More Information about End User Advisory Board Meetings can be found on the PREEMPTIVE website.

Related European Projects

CRISALIS provided new means to secure critical infrastructure environments from targeted attacks, carried out by resourceful and motivated individuals. CRISALIS produced tools for network and host-based detection of targeted attacks. PREEMPTIVE will bring the results of CRISALIS one step further by:

a) Building upon the technology produced in CRISALIS (e.g., parsers, fuzzers, and core of the network-based intrusion detection system).
b) Exploring areas left uncovered in CRISALIS (e.g., host-based intrusion detection for embedded devices, industrial process anomaly detection).

More information about CRISALIS can be found on their website: www.crisalis-project.eu or contact us via the PREEEMPTIVE website: www.preemptive.eu.

EUCONCIP is a European network aiming at connecting stakeholders in the field of Critical Infrastructure Protection (CIP) and fostering cross-sector and cross-country cooperation. EUCONCIP involves public and private organizations, associations and individuals with expertise in the field of CIP through tailored activities such as working groups, workshops and conferences. PREEMPTIVE will cooperate with EUCONCIP Working Group 3 on "Advanced Topics on CII protection and resilience".

More information about EUCONCIP can be found on their website: www.euconcip.org or contact us via the PREEMPTIVE website: www.preemptive.eu.