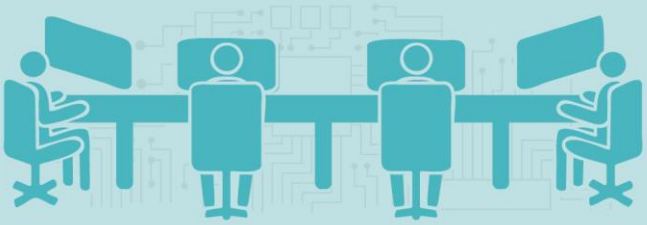
Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE

NEWSLETTER

Issue nr. 2 / February 2014



EDITORIAL

With the recent conclusion of the second year of work in PRECYSE we are glad to share with the community the outcomes of the project.

The main focus during this phase of the project has been on finalising the **methodology to iteratively increase the cyber protection of Critical Infrastructures (CI)** and the **reference architecture** to actively implement the needed security controls and mechanisms in ICT infrastructures supporting CI.

Parallel to this work, the PRECYSE consortium has established two **pilot sites** in order to assess the tools, methods and techniques developed so far. For this reason two virtual environments have been set up, emulating realistic conditions, one focused on the area of **energy and SCADA systems**, and another one on the area of **transportation and supervisor systems**.

This integration and setting up of the two demonstrators will be the main tool for validation of the PRECYSE outcomes, this will be done through two iterations of work, following this flow: design, integration and validation phases. With the first iteration already in the testing and validation phase, the enhancement and integration of further work for the second iteration will start very soon.

And finally, on March 2014 the project has held its End User Group Workshop with more than 20 attendees, getting feedback directly from experts and interest stakeholders.

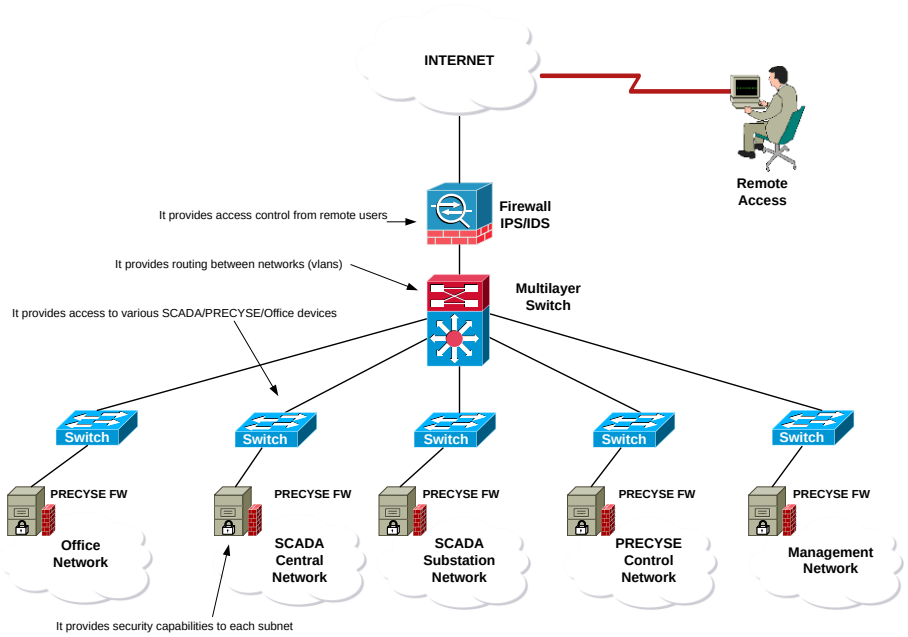
SUMMARY

PRECYSE Pilot sites

Instantiation of an integrated prototype of the methodologies, technologies and tools developed by PRECYSE project have been deployed at two test sites.

PRECYSE results are being evaluated in realistic conditions within two demonstrations in the fields of Energy and Transport.

The specific features of Linz Energy Grid Control Network and of the Traffic Control System of Valencia have been taken into account, together with the standard representation of SCADA networks, for the definition of the "Playground" network of each demonstrator.

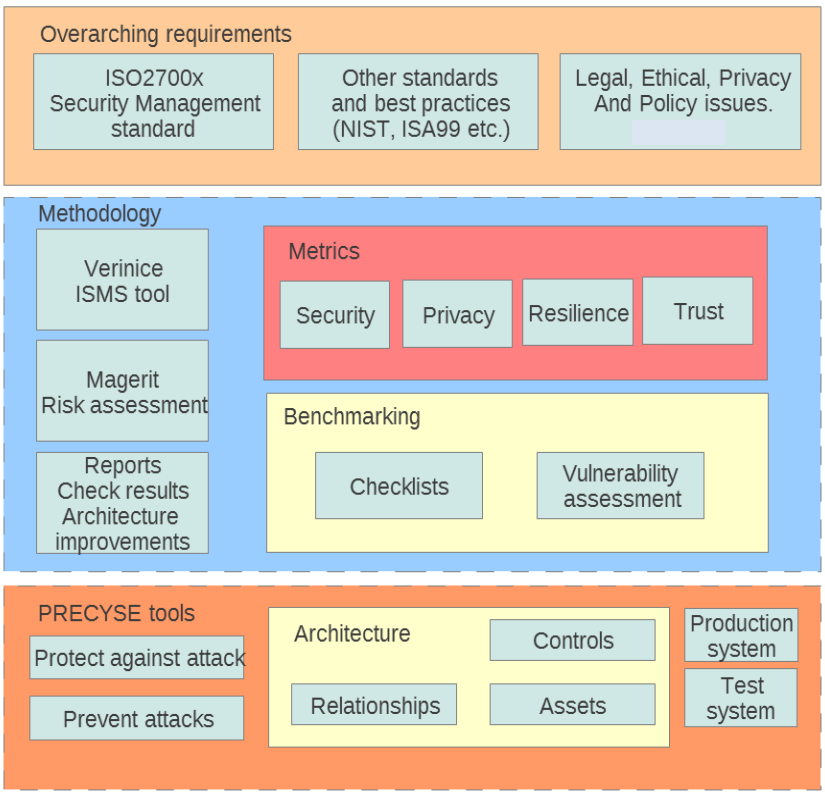


Methodology for Critical Infrastructures

The work for developing a «Methodology to Identify Assets and Associated Threats and Vulnerabilities» is now finished, and the PRECYSE Methodology will now be applied to the PRECYSE demonstrator networks in Linz and Valencia.

The main objective of the PRECYSE Methodology was to develop an open methodology for identifying assets, related threats and vulnerabilities based on existing best practice solutions. This includes to improve the level of security for critical infrastructures by bridging the gap between high-level generic methodologies for information technology security evaluation and low level or proprietary methods for security assessments provided by commercial vendors. The methodology provides a model of cyber security that is based on risk awareness to a greater extent than existing methods, and it aims at supporting a multi-objective optimisation process where decision makers get overview over alternative security improvement solutions and can choose the solution that best suits the organisation.

The PRECYSE methodology integrates high-level Information Security Management methodologies like the ISO 27k set of standards, with the MAGERIT risk assessment standard and also to support a benchmarking test suite. The test suite consists of automatic tests based on the Open Vulnerability Assessment Language (OVAL), and manual tests described in the Open Checklist Initiative Language (OCIL). The Methodology defines a set of quantitative risk metrics that can be used to support a multi-objective risk assessment process based on different metrics like cost, information leakage or downtime where not only security, but also other objectives like privacy/confidentiality or availability are considered.



Events

Selected Past Events Where PRECYSE Outcomes Were Presented

4th World Cyber Security Summit
The PRECYSE End User Group Workshop this year took place the 13th March as part of the 4th World Cyber Security Summit organised by CSIT – QUB

CRITIS 2013
was held in Amsterdam, Netherlands, on September, 2013. PRECYSE partners from AIT presented a paper based on PRECYSE work "Determining risks from advanced multi-step attacks to critical information infrastructures"

IDIMT 2013
Was held on September 2013 a full paper was presented "Architectural Model for Information Security Analysis of Critical Infrastructure"

Future Events

Future Security
Security Research Conference

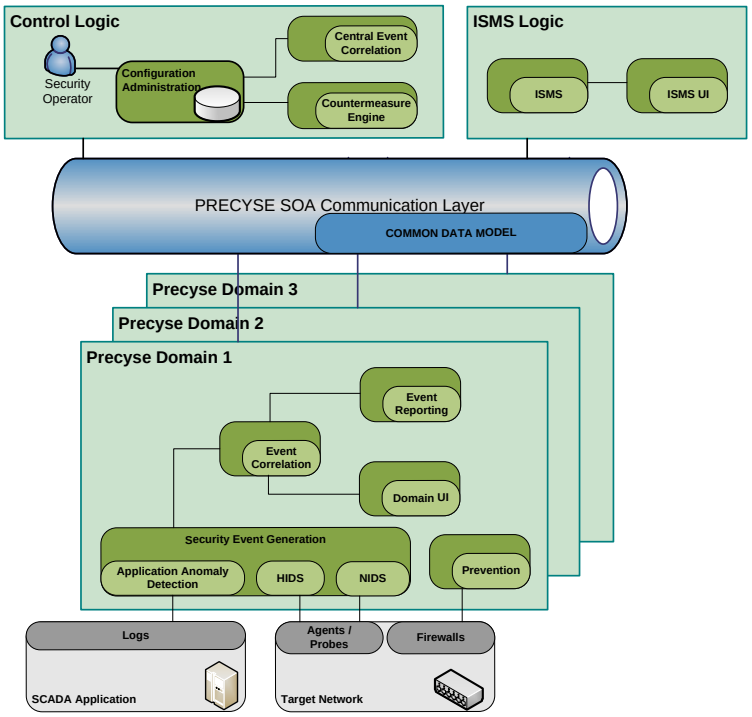
9th Security Research Conference, September 16 – 18, 2014, Berlin

CRITIS 2014
9TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY
OCTOBER 13-15, 2014, LIMASSOL, CYPRUS

PRECYSE Architecture

The target of the PRECYSE work related to the architecture was to identify the set and organization of security controls applicable to the IT assets managing a critical infrastructure. The selection of assets to be monitored as well as the association of these assets with PRECYSE security services has been addressed from a design and technology perspectives.

From the design point of view, an iterative approach has been employed to identify functional specifications and communication interfaces starting from basic logical blocks devoted to the management, processing and exchange of security information.
From the technological point of view, a set of frameworks, tools and libraries for the secure deployment of a Service Oriented Architecture has been identified and described.



The overall outcome of PRECYSE architectural work package has been the design of a distributed systems managing information related to network/hosts configuration and to security alerts both at local and at a central level.

The resulting PRECYSE Service Framework is thus a hierarchical structure built upon custom and off-the-shelf modules/tools which rely upon a well identified Web Service layer for the exchange of processed data.
A Canonical Data Model integration pattern has been employed to allow the inclusion of existing security technologies into the PRECYSE platform. Such approach allowed also the definition of a modular, tailorable model to be adapted to the specific target infrastructure, both in terms of geographical scalability and functional extensibility.

PRECYSE End User Group Workshop 2014

The PRECYSE End User Group Workshop this year took place the 13th March as part of the 4th World Cyber Security Summit organised by CSIT – QUB.

It counted with the attendance of 22 experts and end users coming from the End User group of PRECYSE.

As invited speaker, Dr. Eul Gyu Im from Hanyang University presented the research efforts of South Korea in the cyber protection of CI, and especially the Smart Grid Testbed Town in Jeju Island.

The PRECYSE partners presented the main findings after two years of research, getting valuable feedback from the audience.

Invited Project

HYRIM

The main objective of HYRIM is to identify and evaluate **'Hybrid Risk Metrics' for assessing and categorising security risks in interconnected utility infrastructure networks** in order to provide foundations for novel protection and prevention mechanisms.

The project will provide utility network providers with a risk assessment tool that – in adherence with, e.g., the BSI or ICNC recommendations – supports qualitative risk assessment based on numerical (quantitative) techniques.

For that matter, HYRIM method will explicitly account for the infrastructure's two-fold nature in terms of the utility network and the control network alongside it. The expected impact is thus a movement away from best practice only, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation.

The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

HyRiM
Hybrid Risk Management for Utility Providers

The project consortium has seven partners from across Europe. ETRA I+D, LINZ AG and AIT, the latter of which coordinates the project, are members of the HYRIM and PRECYSE consortium, and will ensure a strong connection and sharing of results between the projects.

PRECYSE at a Glance

PRECYSE

Prevention, Protection and Reaction to Cyber Attacks to Critical Infrastructures

Web site: www.precyse.eu

Project Coordinator

ETRA Investigación y Desarrollo S.A.

Santiago Cáceres / Antonio Marqués
technology-projects.etra-id@grupoetra.com

Partners:

etra I+D
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Fraunhofer IOSB
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
skytek
THALES
UNIVERSITY OF AGDER
AJUNTAMENT DE VALÈNCIA
LINZ AG STROM