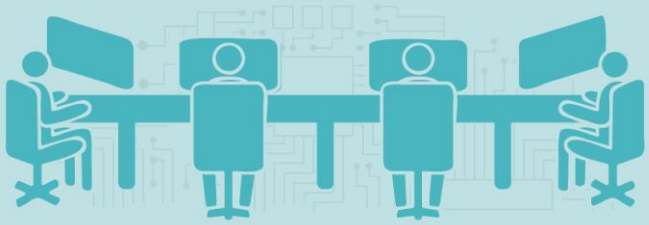
Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE

NEWSLETTER

Issue nr. 1 / February 2013



EDITORIAL

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

The main focus during the initial phase of the project has been on the clear **identification of the scenarios** to be tackled by our research, negotiating the different responsibilities within the group of institutions cooperating in the project, and analysing the requirements to achieve the final goals of the project. Requirements coming from the outside end-user community have been taken into account thanks to our PRECYSE Users Group.

This initial effort has led to the first draft version of the **PRECYSE reference architecture** where the different components and concepts to be developed in the next months are specified and their relationships described. This common understanding of the project boundaries and expected route map has been key to building a strong team capable of obtaining breakthrough results in the short lifetime of the project.

Parallel to this work, the PRECYSE consortium has established the basics of its **methodology to improve the cyber security** of any ICT systems supporting Critical Infrastructures (CI).

SUMMARY

Pilot sites

An integrated prototype of the methodologies, technologies and tools developed by the PRECYSE project will be implemented and deployed at two test sites.

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

ENERGY DEMONSTRATOR

The energy demonstrator will be deployed in **the Energy Management Control Centre** of the region of **Linz** (Austria). It provides power supply and related services for **400.000 inhabitants** in an area of 2.000 km^2.

TRANSPORT DEMONSTRATOR

The demonstrator will be deployed at the **Traffic Control Centre** in Valencia (Spain), which has a metropolitan area with more than **1.500.000 inhabitants** and an average of more than **500.000 vehicles** running every day.

Scenarios and Use Cases

The first year of PRECYSE was predominately based upon a thorough Requirements Analysis and the development of comprehensive Use Cases. This work was considered critical for the success of the project, as it clearly sets the scene for the remaining activities to ensure that all the consortium members are working towards a common understanding.

The initial activity focused on the collection of requirements, which was achieved by using the **Volere tool** as a template. The process was a combination of internet interaction supported by several telephone conferences and **meetings in Valencia, Linz and Kristiansand**, where, in addition to producing the necessary deliverables, the consortium team members learned about their colleagues environments and forged some excellent working relationships for the future.

The Requirements Definition stage led on to the **Use Case Specifications and then to the Methodology and Architectural Framework** in a logical fashion. As a result we now have a well documented definition of the programme going forward, which informs the other work packages. The documents produced also enable non-consortium members to understand in detail the objectives and goals of the PRECYSE project.

In particular the descriptions of the Linz and Valencia demonstrators and their use cases describe the ways that PRECYSE will be used to demonstrate its potential for the future.

Pictured above, the **PRECYSE Consortium meets with Aker Solutions**, a member of our User Group, during the Requirements and Use Cases workshop held at Kristiansand (Norway). **Aker Solutions** are a company who provide oilfield products, systems and services for customers in the oil and gas industry world-wide.

Events

Past Events where PRECYSE was Presented

Chip-to-cloud security forum
PRECYSE was succesfully presented at the Chip-to-cloud Security Forum on 19th September 2012, PRECYSE was presented in the slot "End to end security solutions for critical infrastructures and the cloud". The presentation was given by Santiago Cáceres and can be downloaded directly in the download section of the PRECYSE Web site.

ITS Spain
The PRECYSE Valencia Demonstrator was presented at the Spanish National Intelligent Transportation Systems (ITS) in Spain, held in Madrid on 24th – 26th April 2012.

Future Events

IEEE INDIN'2013
11th IEEE International Conference on Industrial Informatics. Bochum, Germany, July 29-31, 2013

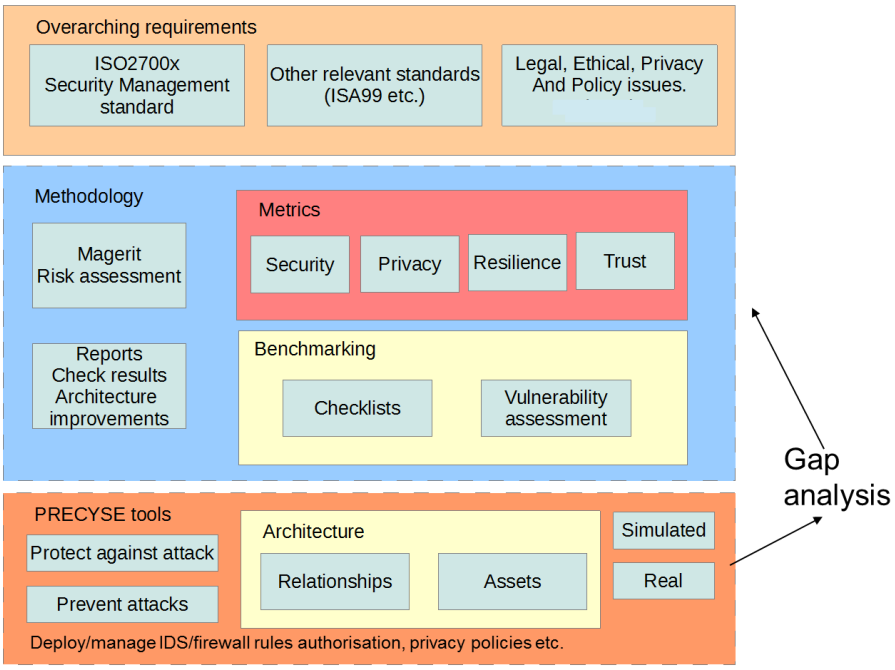
Future Security
Security Research Conference

8th Security Research Conference, Berlin, September 17th-19th, 2013.

PRECYSE Methodology

Approach

The primary goal of the PRECYSE methodology is to support an improvement process for the security management of a Critical Infrastructure, through **risk assessment, benchmarking and gap analysis**. The PRECYSE methodology will also help to bridge the gap between operational and strategic security management.



The previous figure shows the different aspects of the PRECYSE methodology, with various standards and legal, ethical, privacy and policy issues as overarching requirements. A core element of the methodology is risk assessment based on an adaptation of the MAGERIT methodology. Another important part of the methodology is benchmarking based on vulnerability assessment, checklists and metrics for security, privacy, resilience and trust. Based on this, reports are generated that propose improvements to the Critical Infrastructure being tested. PRECYSE tools for preventing and protecting against attacks provide input to a gap analysis that also is part of the methodology.

Going Beyond

Current status

The first methodology specification has already been delivered and submitted to the EU commission at the beginning of December 2012. The outcomes of this work have also been sent to several forums in the forms of full papers, and we are expecting to get more feed back from the outside scientific community.

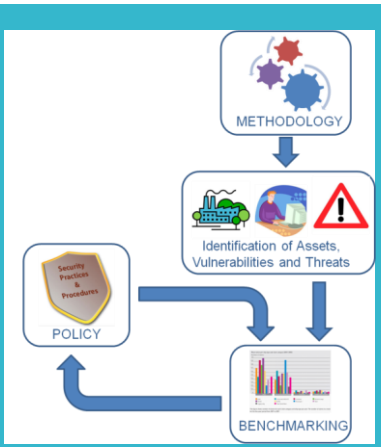
Road ahead

The PRECYSE consortium is now proceeding with the planning and development of the first full version of its **PRECYSE Methodology for Critical Infrastructures**. Important on-going tasks include selecting a suitable set of metrics, relevant for end users, as well as clarifying and defining the interfaces between the methodology and the PRECYSE tools.

In addition a report containing a suggested benchmarking test suite will be delivered as part of the methodology.

PRECYSE Methodology at a Glance

A specific methodology must be applied to the CI being assessed in order to systematically identify its assets, their vulnerabilities and the associated threats. Then, the security strategy being applied by the relevant CI manager will be analysed to see to what extent it is adequate to protect its critical assets from known threats.
With this information the CI will be benchmarked in terms of security, resilience, trust, privacy and other metrics. This process will give the CI manager a roadmap and the suggested next steps to improve its current security level.



Architectural Framework of PRECYSE Project

The primary goal of the PRECYSE Architectural Framework is the definition of a model for **resilient architectures applied to a Security Platform**, capable of assessment, inventory, detection and mitigation functionalities against cyber-attacks performed against the ICT of a critical infrastructure.

The main activities performed so far have been focused on the definition of the following architectural viewpoints, based on the RM-ODP/UML language:

- Analysis of the most relevant Use Cases and Scenarios to identify high level components/actors and Business processes;
- Identification of logical Components and services;
- Description and allocation of functionalities to components;
- Analysis of collaboration between components – Consumers / Producers identification for Service elements;
- Identification of Tools to be associated to each functionality;
- Identification of data-model structures entailed by the collaboration;
- Iterative definition of data model content (starting from a draft proposal to be refined according to allocated functionalities);
- Proposal for component context deployment – ESB Detailed Aspect and embedded logic.

As shown in the figure below, these activities result in the definition of a PRECYSE Security Operation Center (SOC) distributed architecture model, where each segment of the target network system (i.e. SCADA Network, Office Network, External/Perimeter Network) is managed, as for security data collection and analysis, by a separated PRECYSE domain instance, communicating with other PRECYSE instances through a service bus.

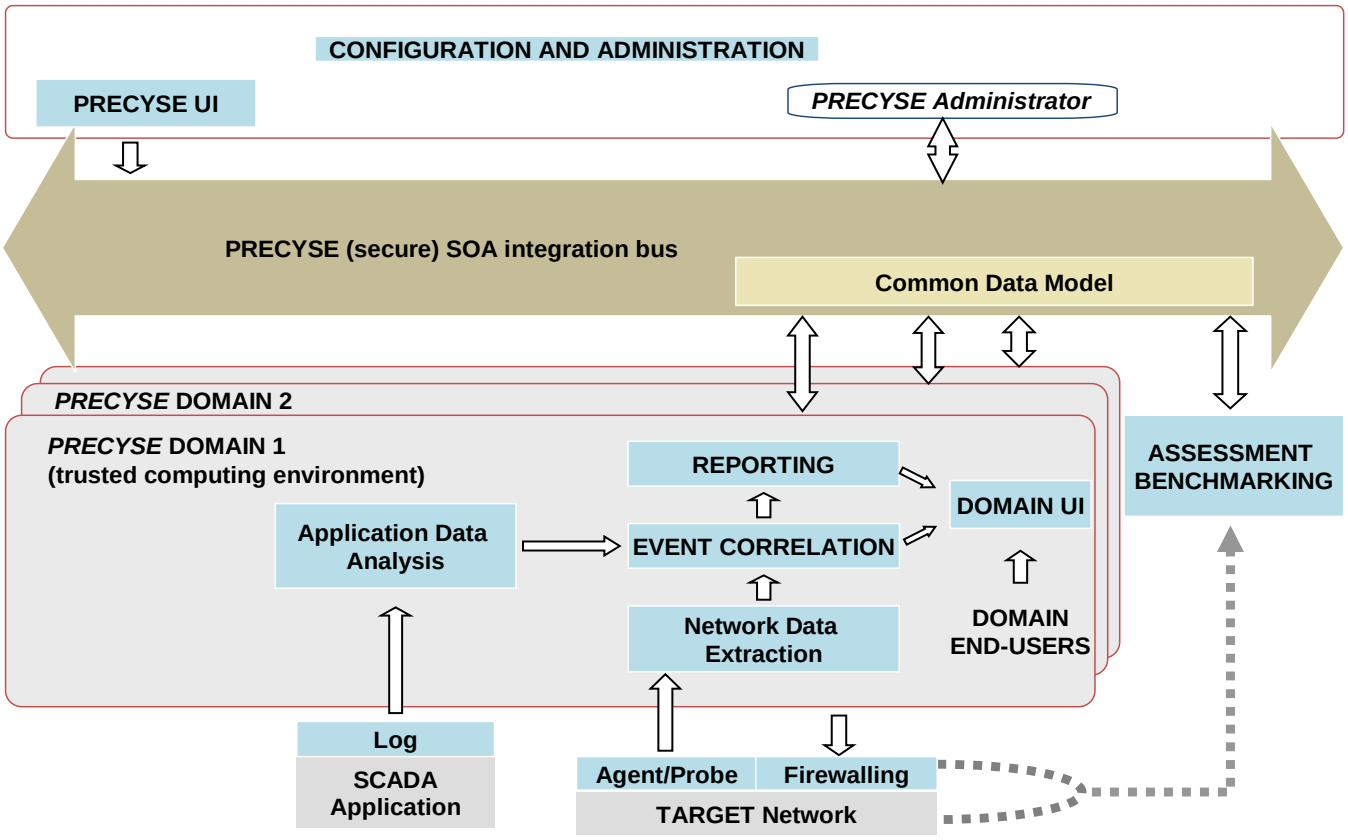
Going Beyond

Road Ahead

A first version of the Architectural Presentation for the PRECYSE Framework report is currently under discussion among PRECYSE project partners.

Current important on-going tasks associated with the architecture include – but are not limited to - :

- Definition of guidelines for SOA and WS security;
- Full identification of architectural components and the allocation of current state-of-the-art technologies onto these components;
- Identification of interoperability interfaces and integration design.



Invited Project

SECCRIT

SECCRIT is a multidisciplinary research project that is investigating **security and resilience for Cloud computing** in the context of critical infrastructure services. It will evaluate the security risks associated with Cloud, and develop methodologies, technologies and best practices for creating a secure, trustworthy, and high assurance Cloud computing environment for critical infrastructure IT. The project consortium has ten partners from across Europe. ETRA I+D, Ajuntament De Valencia and AIT (who coordinate the project), are members of the SECCRIT and PRECYSE consortia, and will ensure a strong connection and sharing of results between the projects.

seccrit

SEcure Cloud computing for CRitical infrastructure IT

Outcomes from SECCRIT will include a risk assessment and management method for Cloud, a policy-based management system that enforces security and resilience requirements, novel anomaly detection approaches to detect attacks, and forensic analysis techniques that can be used to determine the root cause of a potential outage or security problem. These outcomes will be developed in conformance with European legislative and regulatory requirements; the project anticipates novel guidance in this area, also. The outcomes of the project will be evaluated using two demonstration scenarios – a city-wide traffic control system in Valencia, Spain, led by Ajuntament De Valencia, and critical infrastructure – airports, borders, government buildings, etc. – video surveillance in Finland, led by Mirasys Ltd.

On the 28th and 29th of January, the consortium members of the SECCRIT project met for the official project kick-off. At the meeting, there were lively discussions about the research challenges to be addressed by the project.

Web site: www.seccrit.eu

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