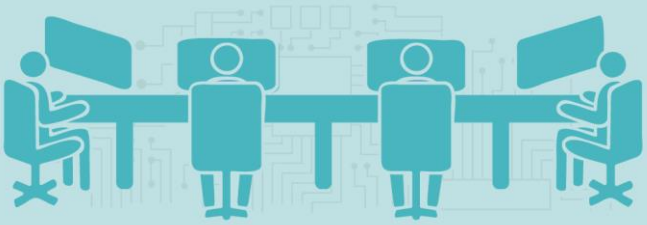
Prevention, protection and REaction to CYber attackS to critical infrastructurEs

PRECYSE

PUBLISHABLE SUMMARY



DESCRIPTION OF THE PROJECT

PRECYSE defines, develops and validates a methodology, an architecture and a set of technologies and tools to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures (CI).

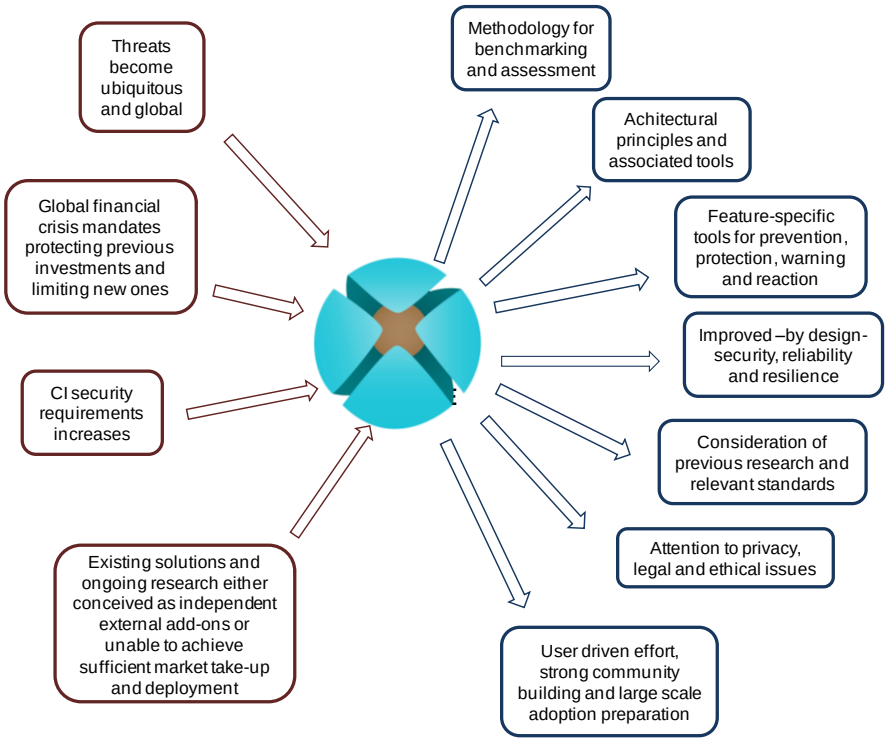
It builds on previous research and existing standards, and pays due attention to performance demands of current CI systems, as well as to relevant security, privacy, policy, legal and ethical issues.

Users from various fields like transportation or energy are involved either as partners hosting demonstrations or as members of a User Group. PRECYSE is a user driven project, with a strong community building effort and activities aimed at preparing the large scale adoption of the project results.

The challenge

During the last few years the need for ICT systems and networks with a higher degree of security, reliability and resilience against cyber attacks strongly increased for Critical Infrastructures in multiple areas such as the transport, energy, oil and water domains.

As new, more sophisticated cyber threats to telecommunication networks and supervision systems emerge, breakthroughs and innovations in security technologies, architectures and methodologies are required.



CONTENTS

Attackers are using more sophisticated technologies, making existing "add-on" security solutions obsolete or insufficient, and the number of stakeholders involved is always increasing. Thus, designing and embedding of new security mechanisms directly into the systems is needed

To make the current situation even more challenging, the global financial crisis has imposed unprecedented budgetary restrictions to both the public and private sectors.

This means that new security solutions must be **both technically efficient and financially cost-effective, facilitating the protection of previous investments and the flexible incremental evolution of the security systems protecting European CI.**

DESCRIPTION OF THE PROJECT

Project Objectives

The strategic goal of PRECYSE is to define, develop and validate a methodology, an architecture and a set of technologies and tools to improve –by design– the security, reliability and resilience of the ICT systems supporting Critical Infrastructures.

This strategic goal can be mapped into a set of specific Scientific and Technical objectives:

- To specify a **methodology** in order **to identify the assets, associated threats and vulnerabilities** to thus improve the level of security for CI. This methodology will be based on best practice and standards for critical infrastructure protection and security information management, and will be presented to relevant standardization organizations.

- To specify and develop a **security architecture that improves resilience**. This architecture will not be developed from scratch or as a standalone element, but instead it will encompass a set of architectural principles -including well proven methods and best practice- and the tools to instantiate them into existing or to-be-created CI architectures.

- Develop a **set of tools and technologies for the protection of CI** and the prevention of cyber attacks against them.

- Develop a **set of tools and technologies for the early warning of attacks to CI and the issuing of countermeasures**. This will include processes, procedures and technologies that alert the managers of a CI when an attack or intrusion is taking place, as well as a series of countermeasure tools, technologies and processes to defeat the intrusion and quickly restore the CI to a fully functional, safe and secure state.

- Instantiation of an **integrated prototype of the methodologies, technologies and tools** developed in the project (one lab prototype in the first implementation iteration), so that PRECYSE results can be evaluated in realistic conditions within two demonstrations in the fields of Energy and Transport (two full demonstration in the final implementation iteration).

- Investigation of the **ethical and privacy issues** as well as the legal and policy implications associated or relevant to the developments carried out by the project.

- **Dissemination** of the project activities and results and liaison with relevant research initiatives and standardisation fora –both research and industry related- in order to ensure the **transferability, impact and exploitability** of the results of PRECYSE. This includes user's community building among users and management of the project's Users Group.

PRECYSE at a GLANCE

PRECYSE

Prevention, protection and REaction to CYber attackS to critical infrastructurEs

Project Coordinator

Name: Antonio Marqués
Organisation: ETRA I+D
Email: info@precyse.eu

Project Technical Manager

Name: Santiago Cáceres
Organisation: ETRA I+D
Email: info@precyse.eu

Project Website:
www.precyse.eu

Project participants: ETRA I+D (Spain), AIT (Austria), Fraunhofer IOSB (Germany), Queen's University Belfast (UK), Skytek (Ireland), THALES (Italy), University of Agder (Norway), Ajuntament de València (Spain) and LINZ AG (Austria).

Duration: 36 months

Start: 01/03/2012

Total Cost: 4,676,111 €

EC Funds: 3,292,792 €

Contract nr.: 285181-SEC

Progress and Achievements

PRECYSE has just concluded successfully its first year of life.

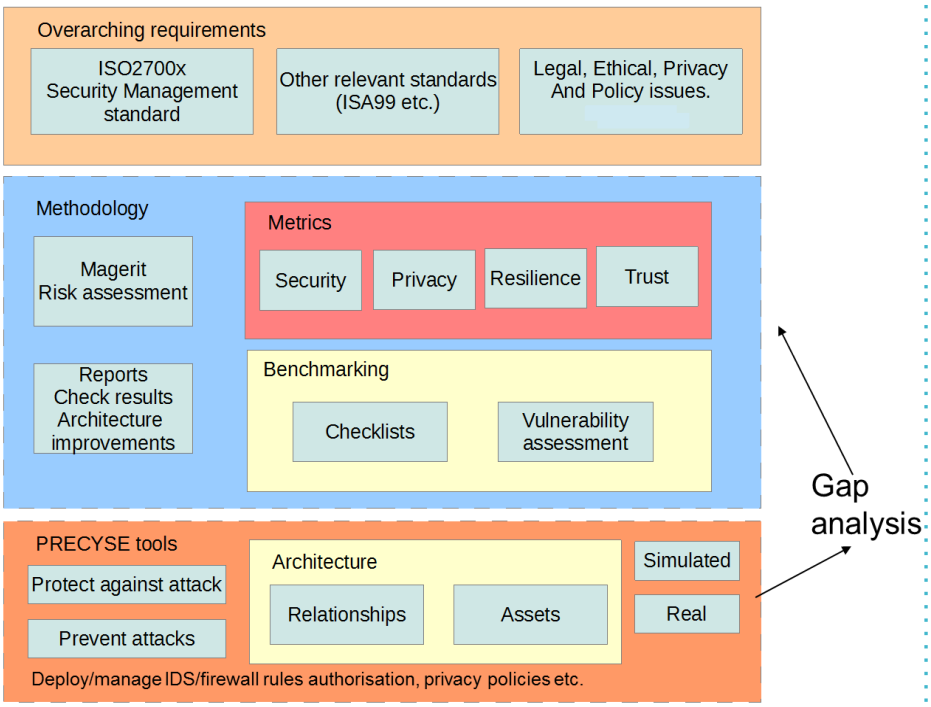
To enable continuous progress tracking, the project is split into three phases nearly corresponding to ach of the three years of the planned work plan.

- Phase 1 (March 2012 – February 2013): **Specification and design**
- Phase 2 (March 2013 – February 2014): Implementation of technologies
- Phase 3 (March 2014 – February 2015): Demonstration and dissemination

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).

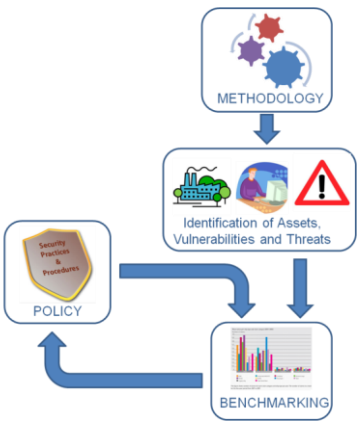


All these results will be complemented by the delivery of the first draft implementation of the **PRECYSE Methodology** and the **PRECYSE Security Service Framework** (SSF) by the first semester of the second year (first prototype), that is expected to be immediately validated in the two pilot sites of the project.

The results of this first phase will be used in the following phases as input and as evaluation criteria.

Hence, the overall progress and success of the PRECYSE project can be measured after each phase using the following three high level milestones:

1st Phase: Coverage of requirements with selected use cases
2nd phase: Percentage of covered requirements
3rd Phase: Percentage of realized use cases



In addition the project has been presented in several relevant events, like the Chip-to-cloud security forum 2012 in Nice (France), and papers have been also presented at various conferences.

Expected Final Results and Impact

The principal impact of PRECYSE is to **enhance the resilience of ICT systems supporting Critical Infrastructures**, in order to make them more robust and reliable. PRECYSE also provides a better overview and handling of security incidents than currently exists. All objectives and outputs of the project are driven at the core by end-users, and accordingly the end result is focused rigorously on industrial demand and real-world deployment. One of the main motivating factors for PRECYSE is that its impact can be as relevant to as many end-users as possible, and be compatible with as many end-users as is practicable.

The objectives of PRECYSE are achieved by developing benchmarking tools, integrating a number of state-of-the-art and emerging technologies in the field of network defence, and by proposing best practice that are transferable and interoperable across a broad spectrum of industrial environments and end-user profiles. A key principle that applies across all objectives in the project is to generate tools that are platform-neutral by design. This principle is fundamental to ensure that the impact of PRECYSE can be as wide as possible.

PRECYSE Final Results in Short:

- A **methodology** in order to identify the assets, associated threats and vulnerabilities
- A security **architecture** that improves resilience
- A set of **tools** and technologies for the prevention, protection and reaction against cyber attacks to CI
- An integrated **prototype** deployed in tow pilot sites, one in the energy sector and another one in the transportation area
- Investigation of the **ethical and privacy issues**

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 km².

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.