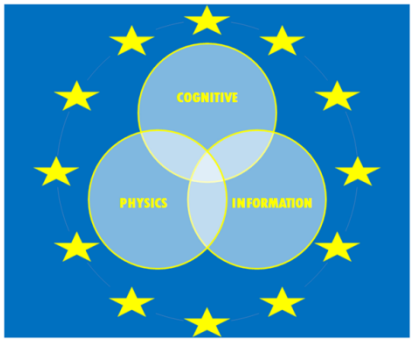
3.1 Publishable summary



NI2S3
NEC Enabler

Complex interactions between the elements of a critical infrastructure indicate, that there is a need to deploy a corresponding infrastructure protection system, which is capable of extending security control to all elements of the protected system, and, at the same time, of maintaining a global view of the infrastructure.

The key objective of the NI2S3 project is to research and implement a reference methodology for developing security systems based on NEC Information and Integration Services (I2S) for Critical Infrastructures. The security systems must be capable to collect and process information from many heterogeneous sources in order to build up or improve the situation awareness of critical infrastructures and to enable the decision making.

More specifically, the NI2S3 Project aims:

- to provide a definition and a design of an NI2S3 critical infrastructure protection system regarding the security, resiliency and availability of the subject infrastructure,
- to define performance indicators and tools for system validation,
- to develop a technology for the evaluation of the performance, robustness and reliability of such protection system,
- to develop a NI2S3 application demo as a proof of concept.

The NI2S3 project is focused on the research and development of a reference methodology to guide the design and the implementation of security systems for critical infrastructure protection, basing on the philosophy and the concepts of the NEC-based systems approached with SOA techniques.

The refining and validation of this methodology is performed by an application demonstrator, realized in accordance with NEC and SOA concepts.

Therefore, the practical implementation and commercialization of a real NI2S3 will require a “step ahead” in this direction, not addressed by the project itself.

Figure 1: Ni2S3 Scenario

The activities within the project are articulated into seven work packages:

- Management
- Analysis of the state of the art;
- Definition of scenarios, analysis and extraction of the system specifications;
- Development of a reference methodology for design, and realization of a NI2S3;
- Definition of a set of metrics and validation capabilities for the components and the protocols involved in NI2S3;
- Project and design of prototype;
- Dissemination and exploitation.

Ni2S3 project completed the activities by September 30 and achieved the following main results:

- Proposal of a reference architecture for CII (Critical Information Infrastructure)

A new comprehensive architectural framework named CrAF (Critical Architecture Framework) was proposed starting from a base reference (TOGAF ADM specialized for CII) and extending it with contribution of other selected architecture framework, namely:

- DoDAF to present viewpoints of the Enterprise Architecture
- COBIT to manage IT process life cycle.
- SABSA concepts to analyze security aspect of the architecture
- TOGAF ADM phases for CrAF sub-methodologies:
  - Data acquisition
  - Data fusion and correlation
  - Vulnerability assessment.

The resulting methodology was applied to a demonstrator case with the objective to monitor and control an Highway analyzing and protecting the information infrastructure which is underpinning such application environment.

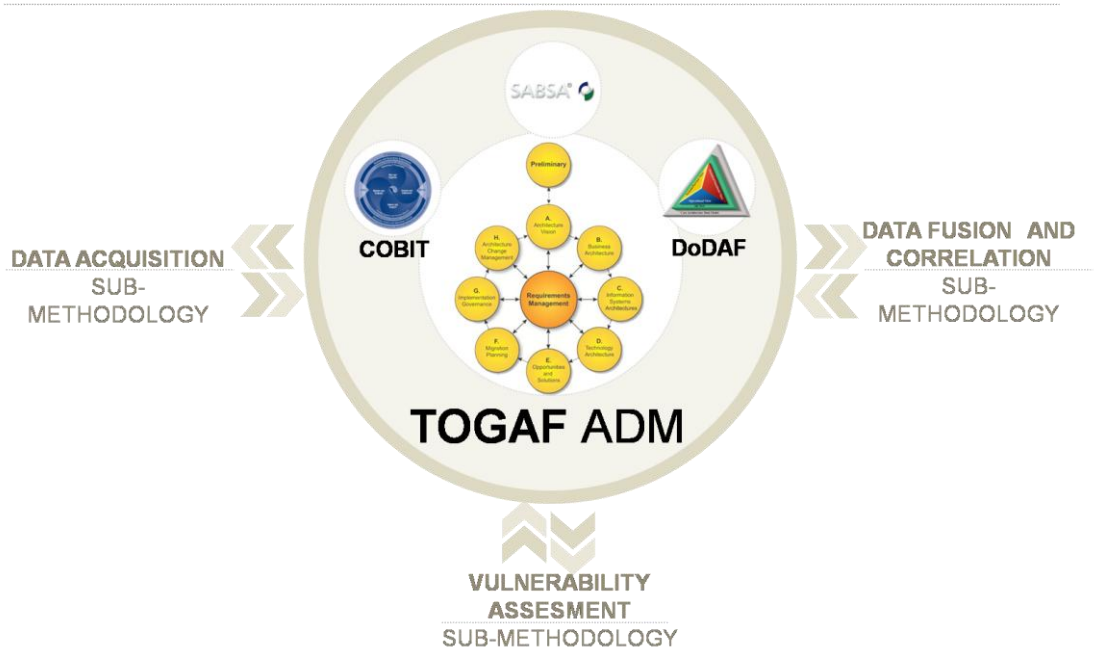


Figure 2: CrAF constituting blocks

- Improved techniques for situational awareness.in CII

  To improve the security and the overall control of the whole system it was suggested and included in the demonstrator a situation awareness mechanism relying on events correlation n a general architecture SOA based. This has been used for correlating application sensible events and infrastructure data and events so enhancing the standard capabilities of a simple

infrastructure monitoring using temporal and logical correlation templates enabling proactive security mechanism mainly in distributed systems sensible to cyber attacks.

- Exploitation of SOA architecture for implementing NEC concept of information centric system
  The project, both through demonstrator and in the analysis exploited SOA as a way of communication and integration adopting OASIS Standards. In particular a gateway from SCADA Systems and a standard ESB was developed demonstrating the suitable adaptation of SOA architecture to distributed data acquisition and control environments.
- Vulnerability Assessment methodology and tools
  VA analysis and tools where applied and investigated suggesting a specific attention to this subject through dedicated design and testing activities in case of CII, supported by validation tools and some guidance on how to address a measurement of the robustness and reliability of a designed infrastructure. A demonstration tool for general application of stress and validation tests was also implemented.
- As a proof of concepts a demonstrator was finally developed where all the outcomes of the research phase and methodology construction were put in actual implementation. The demonstrator has a special focus on the relationship to SCADA systems which due to the evolution of the embedded systems and the ability to integrate and interconnect low level controlling systems in distributed architectures will reserve a special care on protection of the infrastructures which should enable this type of scenarios.

Critical transportation systems have an intrinsic transnational value, so that the most suitable instrument to achieve advances in the protection of such infrastructures is transnational co-operation.

NI2S3 confirmed to be a cross-border project, which will give the chance of develop technology and reference methodology for developing Critical Infrastructures security systems that can be better accepted by the potential stakeholders, being them designed under the guidelines of each of the participant's country needs.

NI2S3 outcomes address scenarios which are emerging in all the distributed systems architecture able to collect data from remote sites, collect them to analyse the resulting information and (this is the new and important stage in the next future) to correlate in temporal and spatial. These systems

are typically Net Centric and are becoming a significant part of the services delivery so becoming more and more critical just in the sense this project intends to address the proposed solutions.

The contact details for Ni2S3 project are:

Project Coordinator: Walter Matta

Phone: +39 06 88202567

Mobile: +39 335 7716488

Fax : +39 06 8820 2288

E-mail: w.matta@vitrociset.it ; ricerca@vitrociset.it

The project web site is:

http://ni2s3-project.eu/