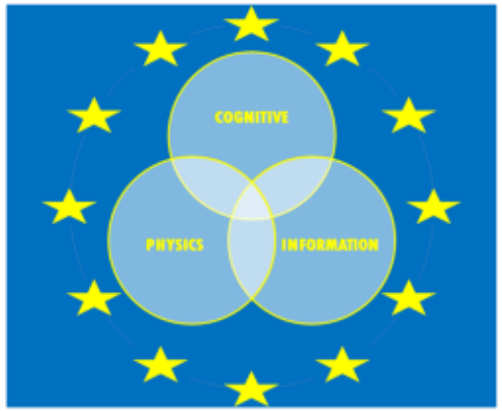


NI2S3
NEC Enabler

NET-CENTRIC INFORMATION & INTEGRATION SERVICES

FOR SECURITY SYSTEMS

Funded by

SEVENTH FRAMEWORK PROGRAMME

Critical Infrastructure Protection
A Real Time Alerting System: Tools & Models

Contract References

Grant Agreement: "**N**et-centric **I**nformation & **I**ntegration **S**ervices for **S**ecurity **S**ystems"

Contracting Authority: European Commission (EC)

Contractor: Vitrociset S.p.A.

Programme: FP7

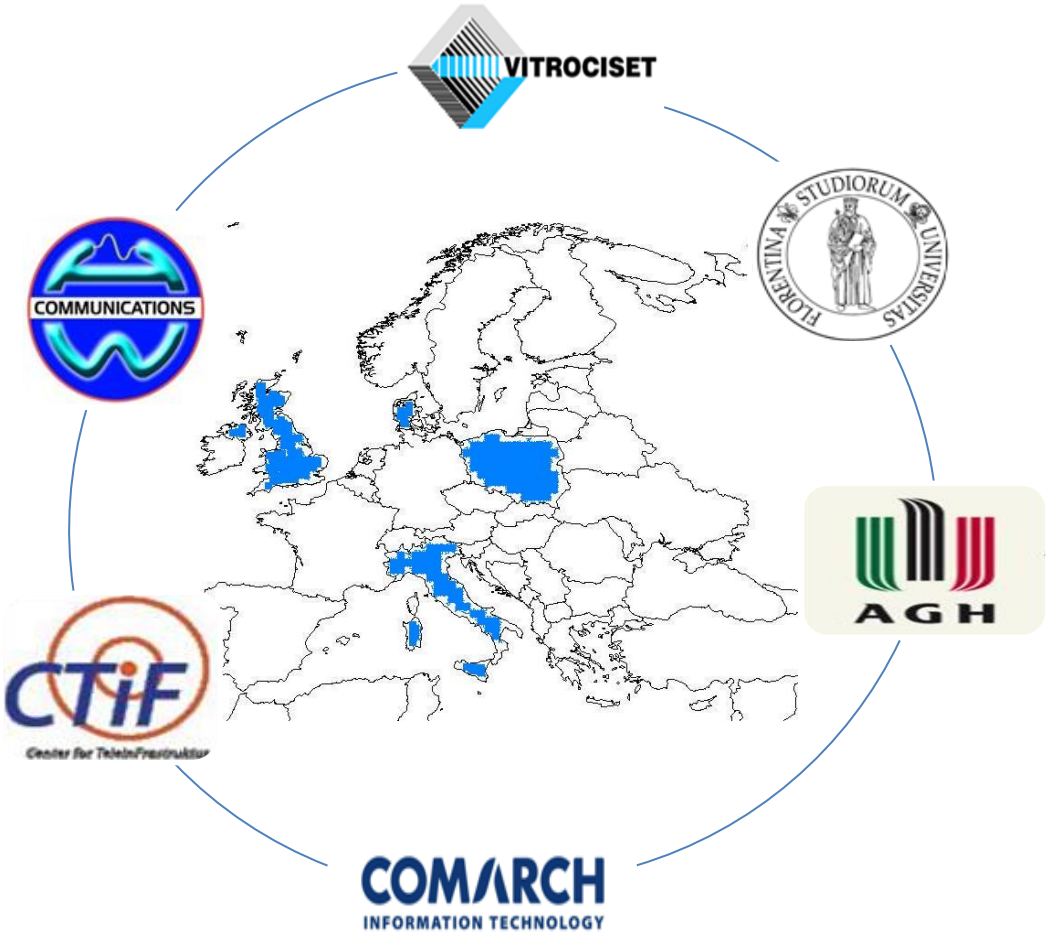
Call: ICT-SECURITY 2007

Duration: 24 Months

Budget: 4.3 MEuros

Funding: 2.7 MEuros

Consortium



Countries	Entities
Denmark	CTIF
Italy	**VITROCISET (Coord.)** UniFI
Poland	AGH COMARCH
United Kingdom	HWC

NI2S3 at a glance

Key Idea

- Research and implement a reference methodology for developing security systems based on **NEC Information and Integration Services (NI2S)**, able to integrate information from many and heterogeneous sources, in order to build up or improve the situation awareness of critical infrastructures.

Overall Goal

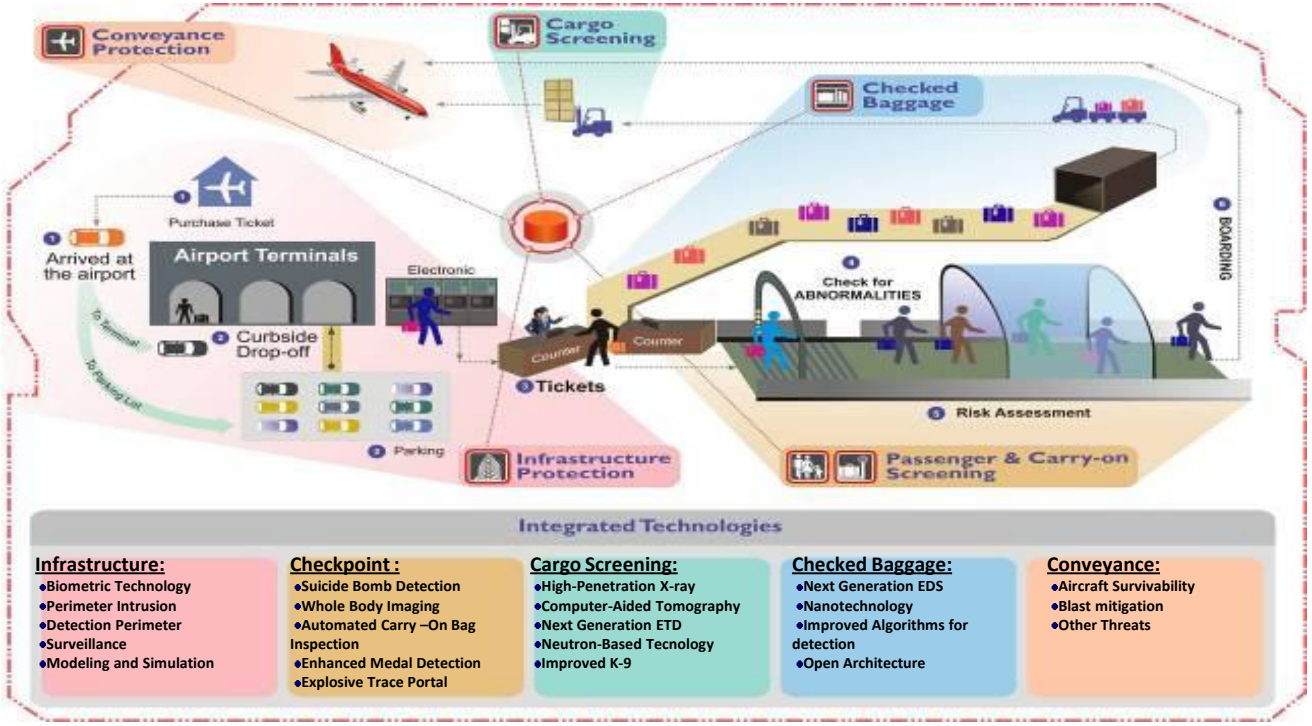
- Definition of a methodology to develop Critical Information Infrastructure Protection(CIIP) Architecture in secure SOA technology environment
- Development of Vulnerability Assessment (VA) procedures
- Application and Demonstration

Project Objectives

Main Objectives

- Definition of operational scenarios, analysis and extraction of the system specifications.
- Definition and design of a NI2S3 for the decision making support regarding the security, resiliency and availability of the subject infrastructures.
- Definition of a set of metrics or tools and setting up validation capabilities to develop the ongoing architecture and system.
- Develop a NI2S3 application demo.
- Develop a technology for measuring the performance, robustness and reliability of such system.
- Dissemination and exploitation of the results

Example of Critical Infrastructures



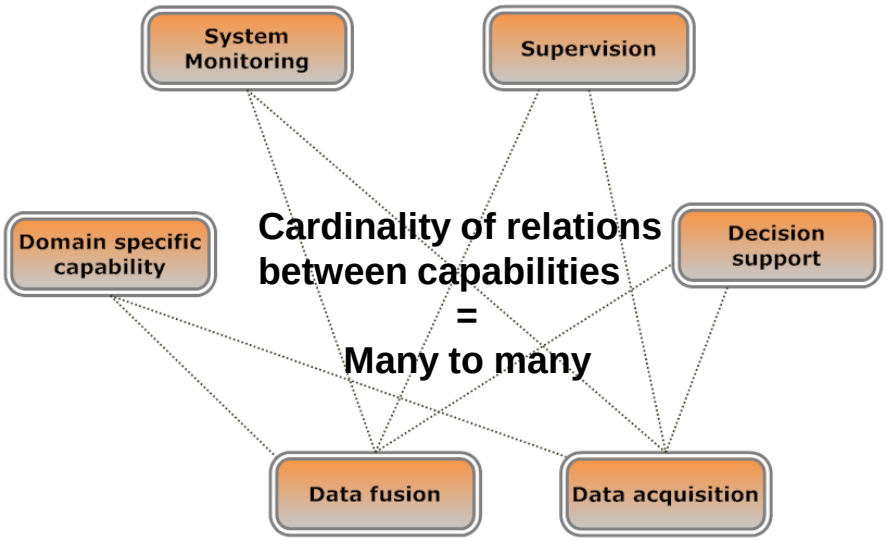
Amount of information comes from many sources

Each user needs a different set of information formatted in different shape

Situation awareness have been proved to be a key concept in securing the critical infrastructure

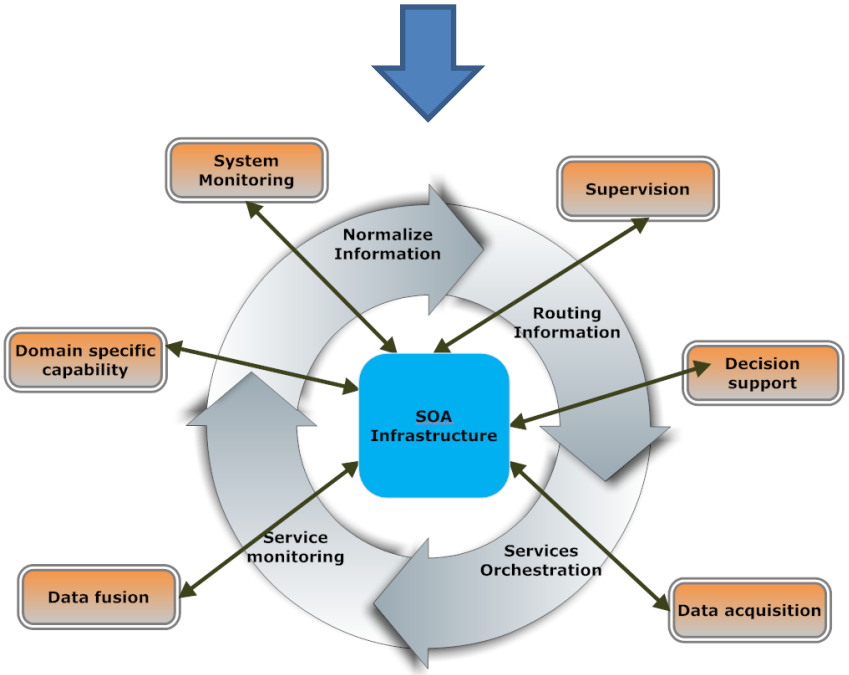
BEST SOLUTION: NEC SOLUTION

Why SOA ?



Critical Infrastructure management systems commonly has a strong NEC orientation

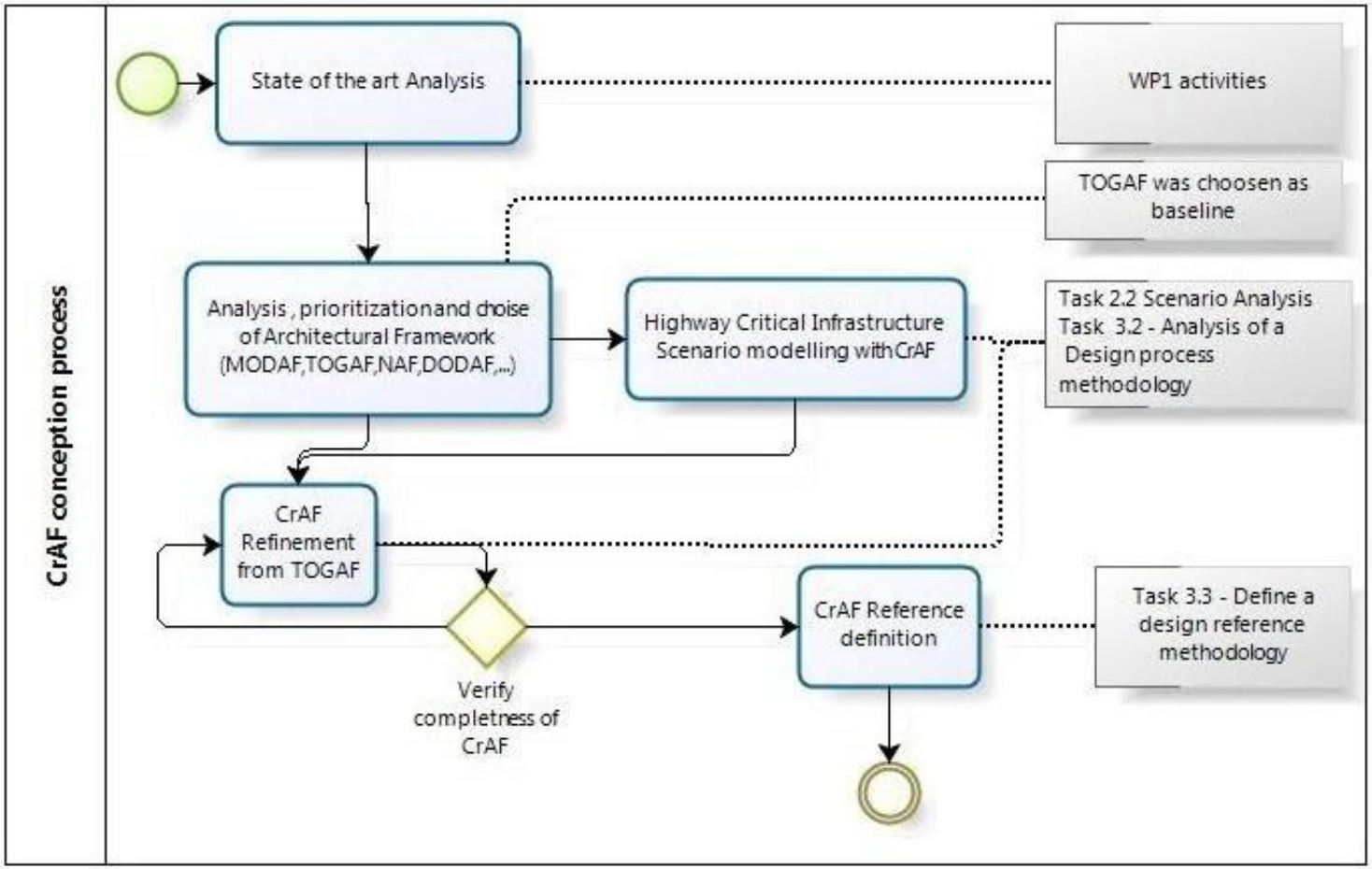
The users need a limited representation of the information space constituted by all data gathered or produced by sensors on scenario, services, ...



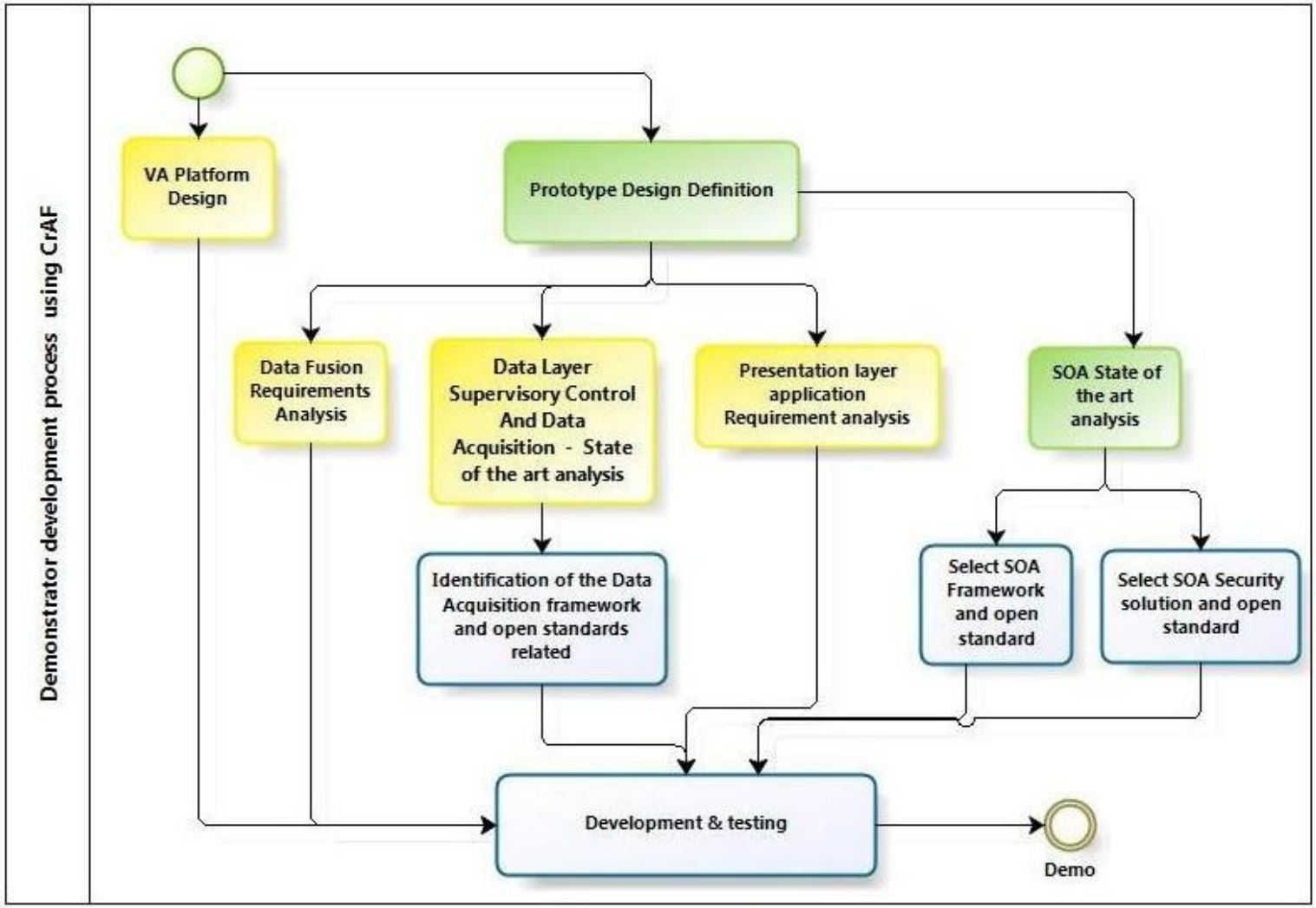
SOA approach offers specific instruments to manage the multiple aspects these class of application

Ni2S3 - Objectives & Strategy

The process carried on by the Consortium to achieve the Critical Infrastructures Architecture Framework (**CrAF**)

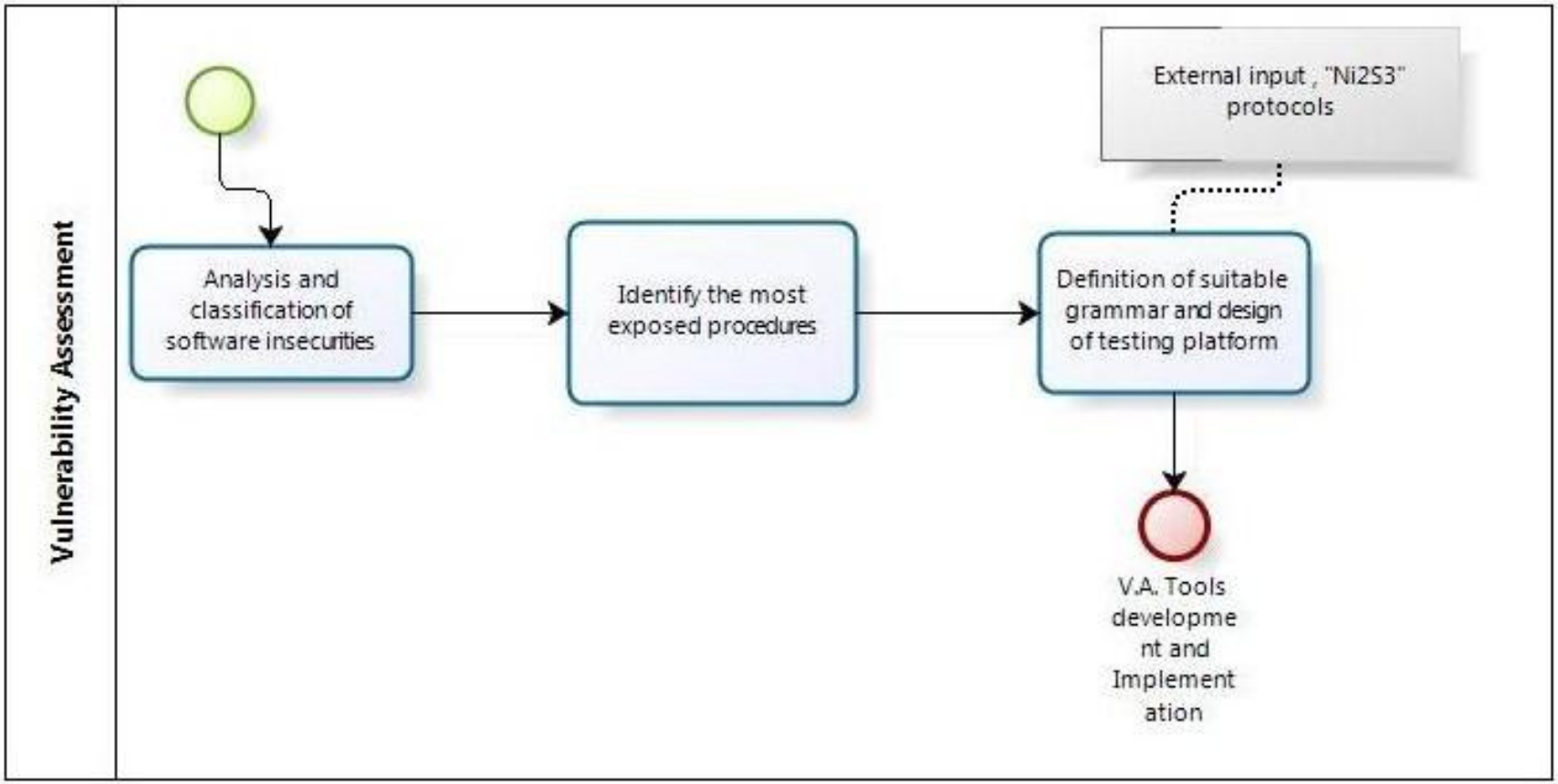


Ni2S3 - Objectives & Strategy



Ni2S3 - Objectives & Strategy

Vulnerability Assessment key idea



Ni2S3 - Objectives & Strategy

Infrastructure Protection key idea

The needs

- To increase availability of information system
- To protect the network from cyber attach
- To mitigate vulnerability

Some relevant key solutions identified in NI2S3

- To be compliant with **open protocol specification** related with SCADA and SOA technologies (OPC-UA, OASIS WS-*,...) in order to remove “proprietary constraints” and “proprietary insecurities”
- To adopt **SOA distributed environment** in order to enable geo distribution and cooperation between remote control room (Open Source Apache ServiceMix **ESB** and **WS-Notification** standard implementation)
- To **protect network** in SOA environment using **XML Gateway** device
- To evaluate Critical Information Infrastructure carrying on **Vulnerability Assessment**

Thank you !