SEVENTH FRAMEWORK PROGRAMME

SAWSOC

Situation Aware Security Operations Center

Research Report

Luigi Romano – University of Naples "Parthenope"

65th IFIP WG 10.4 Meeting

January 23-27, 2014 Sorrento - Italy

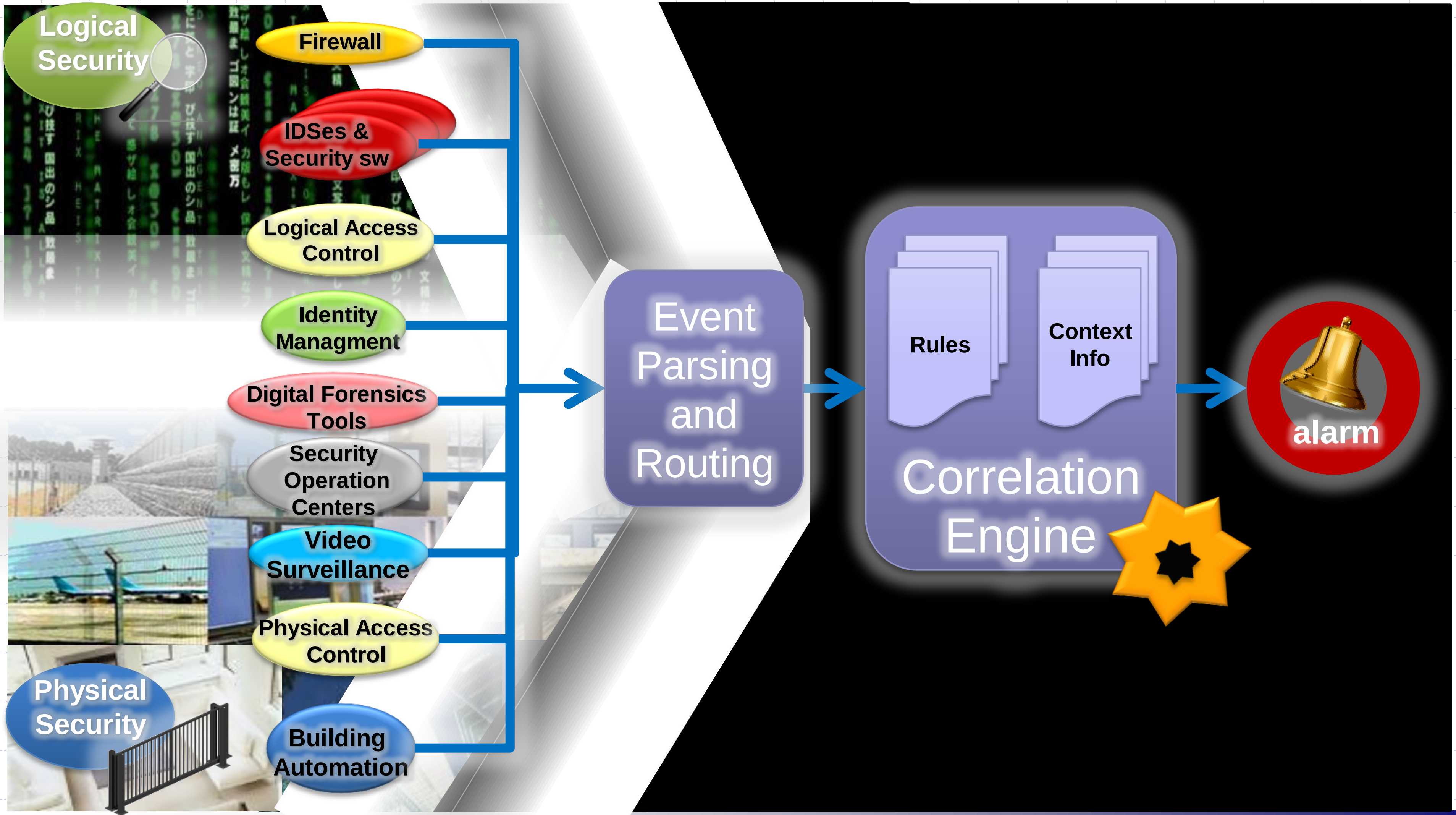
Context

- Technologies for implementing security services in the physical and in the electronic domain are both stable and mature, but they have been developed independently of each other.
- Technologies for implementing security services in the physical domain encompass a whole variety of solutions, ranging from simple tools such as spiked walls to sophisticated products such as Physical Security Information Management (PSIM) systems.
- Security-enabling technologies for the electronic domain are also very varied, ranging from anti-virus programs for Personal Computers to enterprise wide installations of Security Information and Event Management (SIEM) products.
- Security Operation Centres (SOC) have been created for diversified and tailored needs, with vertical approaches for separate physical and logical security purposes

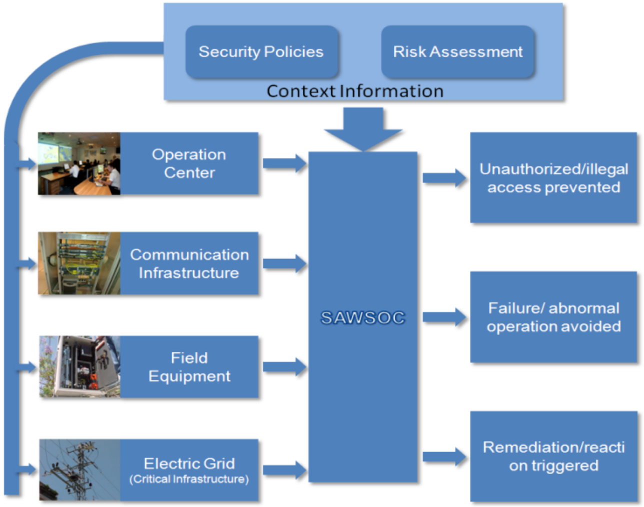
Objective: to identify, implement, and validate techniques for achieving the convergence of physical and cyber security solutions. By "convergence" we mean: effective cooperation (i.e. a concerted and results-oriented effort to work together) between previously disjointed functions

- To develop techniques for correlating physical and logical security services from the physical and electronic domains
- To achieve a consistent view and to be able to produce an irrefutable record of who did what, where, and when
- To demonstrate and validate project results in three example areas of Critical Infrastructure Protection, specifically: Air Traffic Management, Energy Production and Distribution, Crowded Events

A leap forward in the convergence path



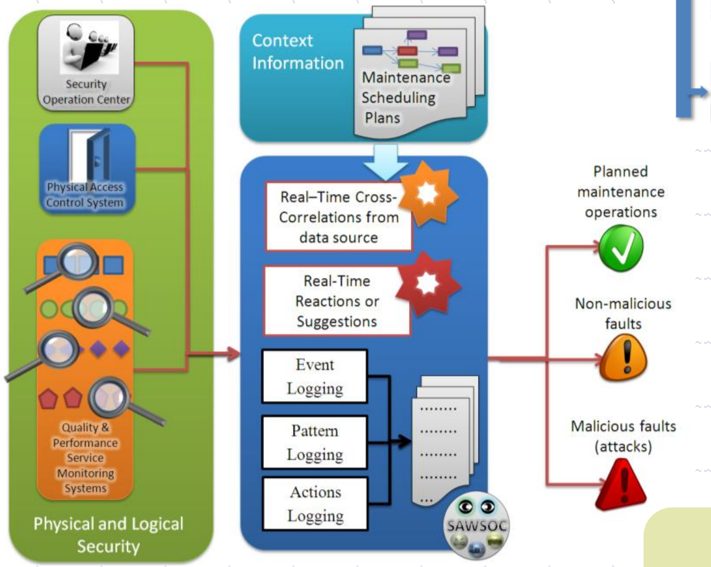
Use-cases



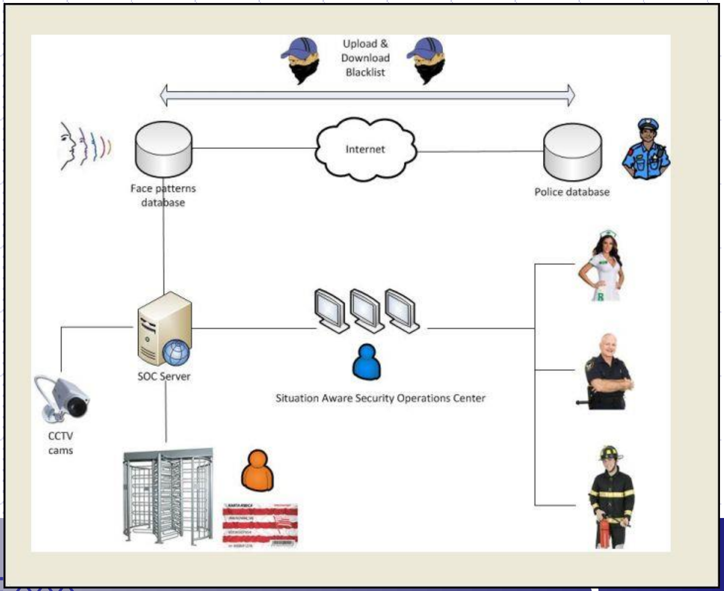
Security Policies
Risk Assessment
Context Information
Operation Center
Communication Infrastructure
Field Equipment
Electric Grid
(Critical Infrastructure)
SAWSOC
Unauthorized/illegal access prevented
Failure/ abnormal operation avoided
Remediation/reaction triggered

ATM
Maintenance Impacts and Attack Recognition on Critical Infrastructures

Power Grid
Critical Infrastructure for Energy Distribution and Production



Security Operation Center
Physical Access Control System
Quality & Performance Service Monitoring Systems
Physical and Logical Security
Context Information
Maintenance Scheduling Plans
Real–Time Cross-Correlations from data source
Real-Time Reactions or Suggestions
Event Logging
Pattern Logging
Actions Logging
SAWSOC
Planned maintenance operations
Non-malicious faults
Malicious faults (attacks)

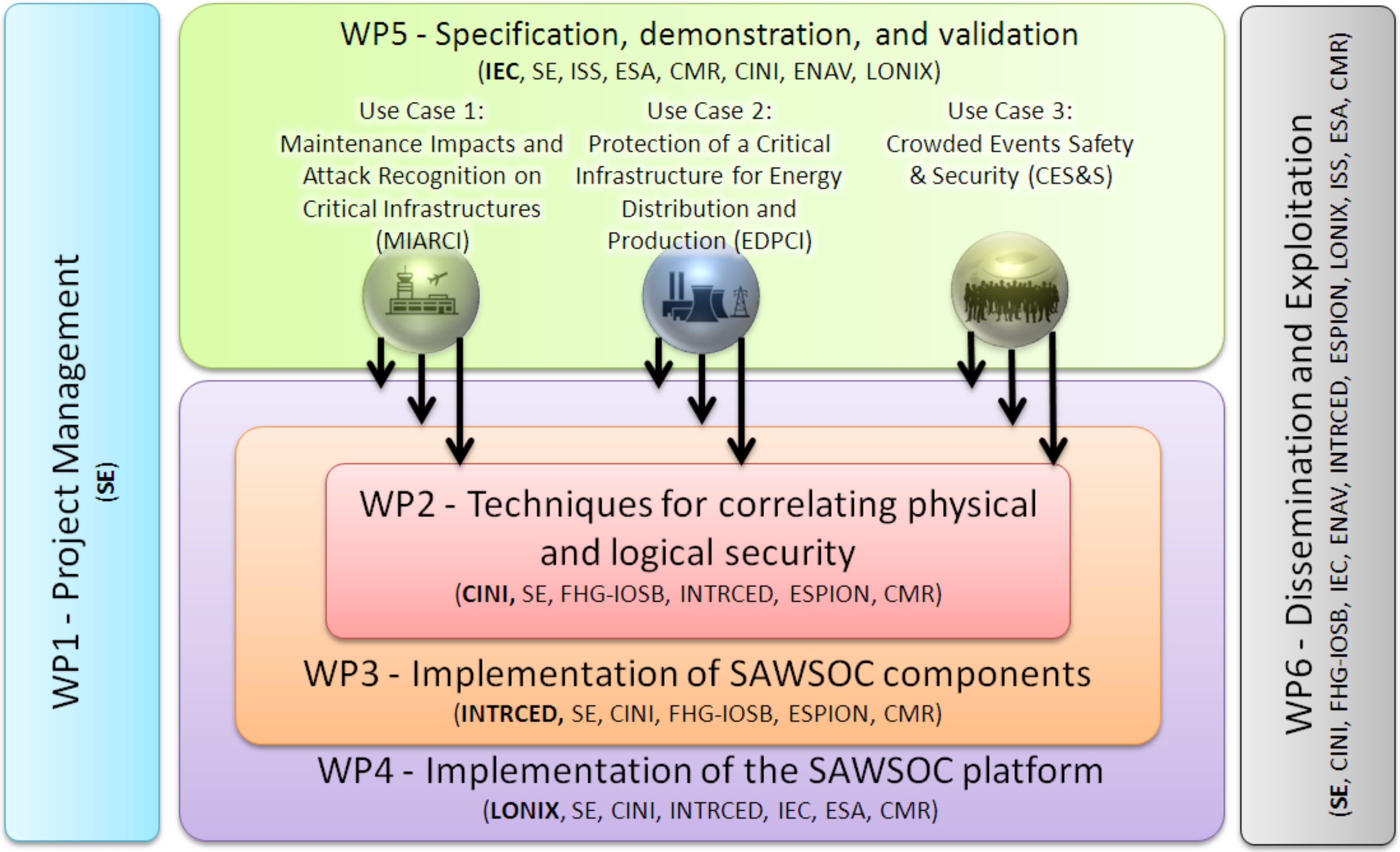


Upload & Download Blacklist
Face patterns database
Internet
Police database
SOC Server
Situation Aware Security Operations Center
CCTV cams

Stadium
Crowded Events Safety and Security

Dissemination Level: XXX

Use-case driven approach



WP5 - Specification, demonstration, and validation
(**IEC**, SE, ISS, ESA, CMR, CINI, ENAV, LONIX)

Use Case 1:
Maintenance Impacts and Attack Recognition on Critical Infrastructures (MIARCI)

Use Case 2:
Protection of a Critical Infrastructure for Energy Distribution and Production (EDPCI)

Use Case 3:
Crowded Events Safety & Security (CES&S)

WP2 - Techniques for correlating physical and logical security
(**CINI,** SE, FHG-IOSB, INTRCED, ESPION, CMR)

WP3 - Implementation of SAWSOC components
(**INTRCED,** SE, CINI, FHG-IOSB, ESPION, CMR)

WP4 - Implementation of the SAWSOC platform
(**LONIX**, SE, CINI, INTRCED, IEC, ESA, CMR)

WP1 - Project Management
(**SE**)

WP6 - Dissemination and Exploitation
(**SE**, CINI, FHG-IOSB, IEC, ENAV, INTRCED, ESPION, LONIX, ISS, ESA, CMR)

Partners

espion

intercede™

BERGISCHE UNIVERSITÄT WUPPERTAL

Fraunhofer IOSB

Selex ES
A Finmeccanica Company

ENAV S.p.A.

cini
Consorzio Interuniversitario Nazionale per l'Informatica

חברת החשמל
Israel Electric

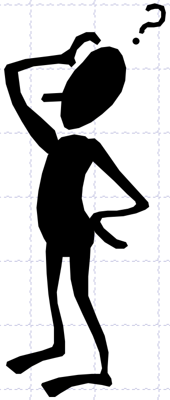
COMARCH

esaprojekt

LONIX
BUILDING CONNECTIVITY

© SAWSOC All rights reserved

Questions and More Info

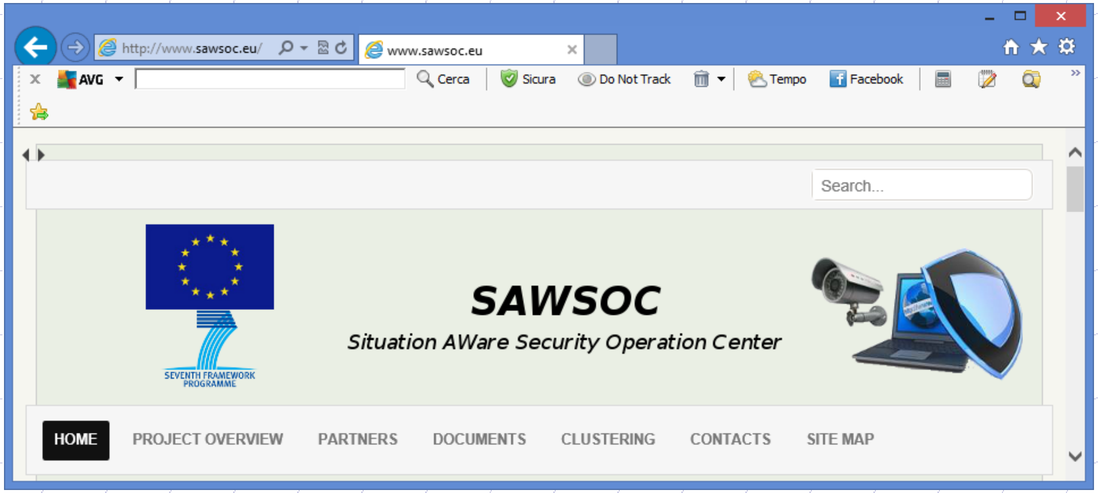


Luigi Romano

e-mail: luigi.romano@uniparthenope.it

Cell: +39-333-3016817

Tel: +39-081-5476700



http://www.fitnesslab.eu/

http://www.sawsoc.eu/

Acknowledgements

- This research receives funding from the European Commission within the context of the Seventh Framework Programme (FP7/2007-2013) THEME [SEC-2012.2.5-1] [Convergence of physical and cyber security - Capability Project] under grant agreement n° 313034