LEONARDO CYBER & SECURITY SOLUTIONS

SC2

SECURITY MANAGEMENT PLATFORM

LEONARDO

SC2 is the Leonardo platform designed to provide a common operational picture for Command & Control, security management, situation awareness and resilience, creating a handling center for safety and security in several operational contexts.

Security challenges increase more and more for critical infrastructure, industries, cities and territories. Providing the right answer to a determined threat is a matter of collecting all the relevant information from heterogeneous systems, combining them and coordinating the reaction in line with the standard operating procedures.

Based on OODA (Observe, Orient, Decide, Act) methodology and built upon a robust Service Oriented Architecture (SOA) and Web Services organization, SC2 supports a wide range of proactive and/or reactive security activities to achieve strategic or tactical outcomes in an integrated security vision.

INTEGRATION OF HETEROGENEOUS SYSTEMS

Core of this system integration is a comprehensive platform able to manage information from multiple systems to provide a single point of view of all operations. With an integrated control centre solution, security authorities can benefit from situational awareness and quickly assess and proactively respond to an incident before it escalates to a serious security incident. Enterprise service bus based architecture facilitates the subsystem integration regardless its complexity.

DATA ACQUISITION & CORRELATION

The integration of different systems and the correlation of heterogeneous information in an innovative way, providing a useful support for a better situation awareness, are the main features of the platform.
SC2 allows to collect, normalize and correlate the right information, highlighting “situations” that otherwise would be hardly detected in advance.

EVENT MANAGEMENT

Thanks to a Complex Event Processing (CEP) rules-based engine, SC2 can define relationships among heterogeneous events, even if apparently unrelated, generated by various subsystems, in order to generate new entities, new alarms (smart alarms) or identify possible false alarms.

WORKFLOW CONFIGURATION

The workflow engine included in the platform is an extremely effective tool for the security management of critical infrastructures. Through an easy-to-use graphical interface it is possible, for example, to introduce into the system all the encoded processes (SOP - Security Operating Procedures) that implement the security plan for a specific asset. In this way the system can ensure that the actions done in response to an alarm event are always linked to a codified process related to that specific event.

CARTOGRAPHY AND GEO-REFERENTIATION

The integrated management of cartography gives to the user a geo-referenced integrated view of all the resources and information in the system.
In this way it is possible to understand the situation and know the possible actions to carry on. SC2 cartography is Geoserver based and is fully compliant with Open Geospatial Consortium (OGC) standars, such as Web Feature Service (WFS) and Web Coverage Service (WCS).

COMMUNICATION INTEROPERABILITY

SC2 supplies complete integration with Professional Radio systems leveraging Leonardo communications interoperability platform. Narrowband technolgies (TETRA, DMR) as well as broadband technologies (Wi-Fi, LTE) can be used to exchange data with the system and coordinate on field resources.

RESOURCE MANAGEMENT

Sophisticated resource management allows the identification, visualization tracking and administration of sensors, cameras, radio terminals and security officers.

FEDERATION

Multiple instances of SC2 can be hierarchically structured federations allowing alarm escalation and, in general, more flexibility in security management.

INTELLIGENT VIDEO MANAGEMENT

SC2 provides native video management functions of ONVIF based cameras including recording and investigation capabilities. Third-party Video Management System can be integrated as well.
Either on the camera and on the server, video analysis capabilities are included in the system with the possibility to implement a number of algorithms applicable to different business domains.
OCR for License Plate Number and Face are examples of existing integrations.

INVESTIGATION

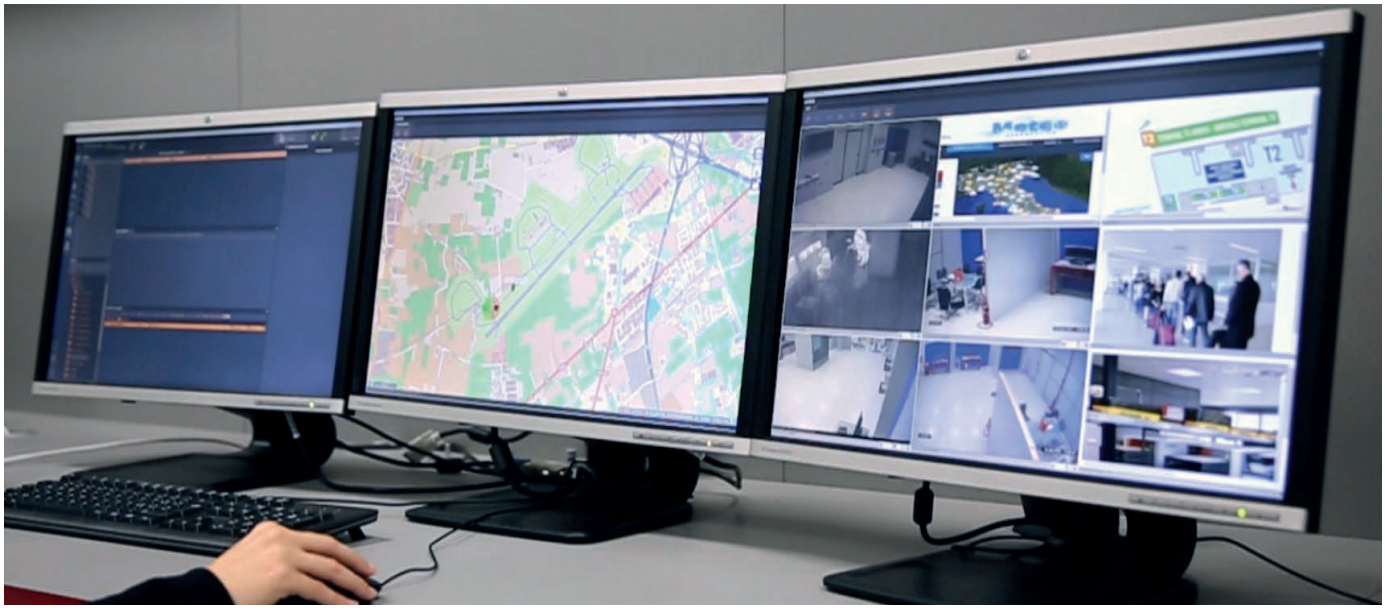
Events video and information recorded in the system can be queried for post-event investigation with a sophisticated browsing interface.

ENTERPRISE DATA MANAGEMENT

Data and multimedia contents can be securely exchanged by the integration of a secure data management function that can trigger events and be part of a SC2 workflow increasing operational effectiveness.

PRESENTATION

The presentation layer is entirely based on web technologies. This choice guarantees a greater simplicity in the distribution of applications and, above all, the capability of making more flexible the accessibility to all contents. Typical client configuration features three monitor workstation, but videowall, tablet and flat multi-touch monitor (tactical table) client configurations are available as well.



Events Management (left) GIS & Cartography Data/Info Resources (right)

APPLICATION DOMAINS

SC2 platform provides a flexible solution to security requirements of different domains through a unified answer to the need of:

- Sensors and subsystems management
- Sophisticated events and alarms management
- Enhanced situation awareness
- Automation in response
- Workforce coordination.

SC2 flexibility allows different types of installation including deployable and mobile configurations.
HA (High Availability) characteristics may be exploited using software redundancies and virtual architecture features.

SC2 constitutes a valuable tool for the security of:

- Critical national infrastructures (ports, airports, railways)
- Energy and utilities
- Enhanced situation awareness
- Cities and territories
- Major events.

SC2 – PSIM VULNERABILITIES AND EXPOSURES

Vulnerability and Exposures management is all about reducing risks in IT systems. The following tables summarize all identified vulnerabilities for SC2 platform

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY [MEDIUM]		
TEST	**CVSS3.1 Metrics**	**Value**
Insertion of files through file upload functionality, in order to prevent introduction of potentially malicious or non-compliant elements.	Attack Vector	Network
	Attack Complexity	Low
	Privileges Required	High
RESULTS	User Interaction	None
Application does not check the bytes of the file, but only the extension. This exposes to the risk of intrusion of potentially malicious files which could generate unexpected exceptions	Scope	Unchanged
	Confidentiality	None
	Integrity	Low
	Availability	Low

INFORMATION EXPOSURE [LOW]		
TEST	**CVSS3.1 Metrics**	**Value**
Possibility to acquire useful information about the application: technologies, services or software versions in use.	Attack Vector	Network
	Attack Complexity	Low
	Privileges Required	High
RESULTS	User Interaction	None
Vulnerability can increase the attack surface of the system and could allow an attacker to design and build complex attacks based on the acquired data	Scope	Unchanged
	Confidentiality	None
	Integrity	Low
	Availability	Low

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber and Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM08887 05-25