Cyber Security Risk Assessment of ALES Safe Smart Building System

Federico Giannoni [187406]
Marco Mancini [187403]
Federico Marinelli [187419]

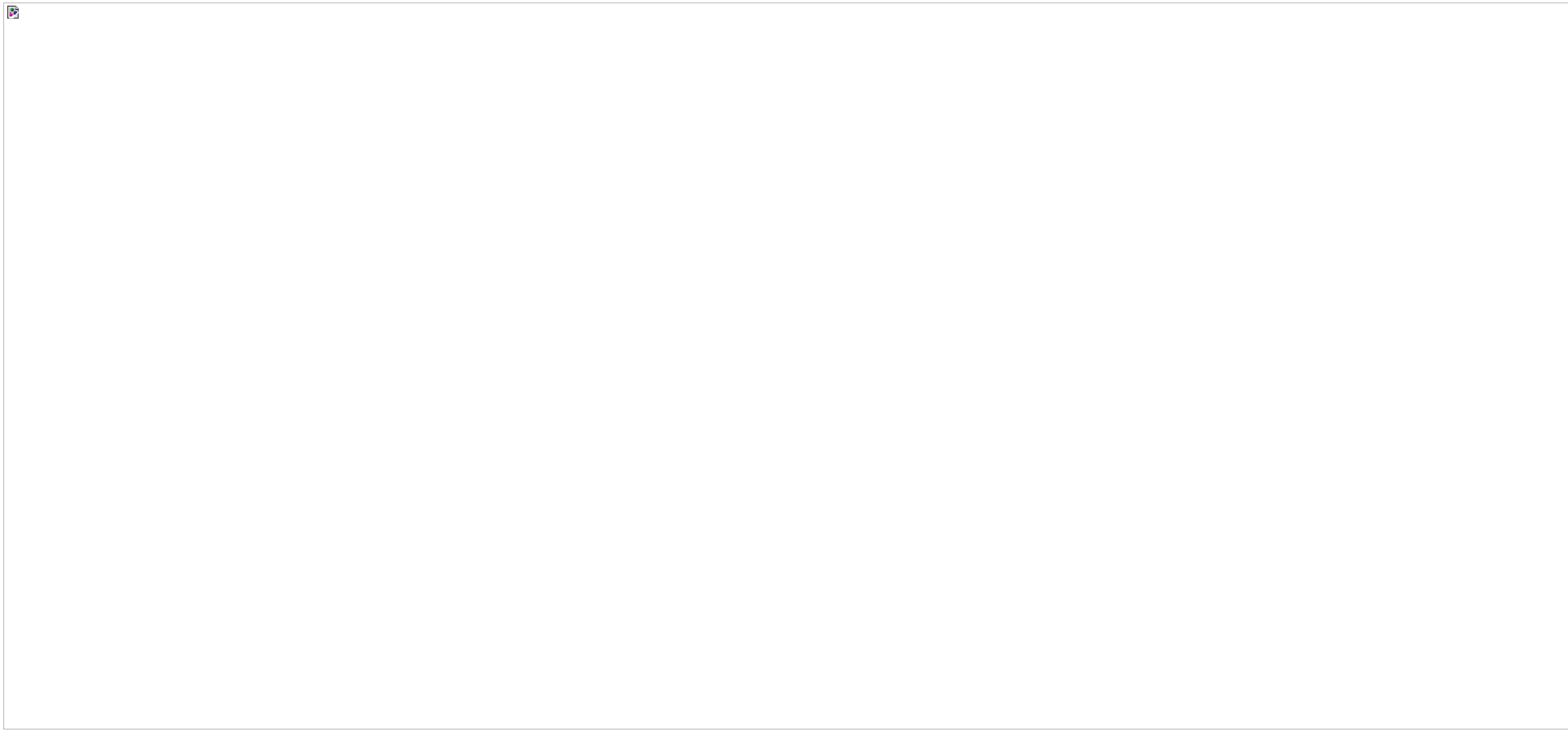
ALES Safe Smart Building system

- How does an I-eGRESS system work?
  - Wireless sensor network gather data.
  - Estimation servers analyze and process gathered data.
  - Web servers allow interaction with the system.
  - Main objective: Save lives.

- Our I-eGRESS system:
  - Specifications of the WSN.
  - Remotely flashable firmwares.
  - No sensor data encryption.
  - No public IP for analytics servers and sensors.
  - Escape route computed on alarm triggering.
  - Elevator manual controlling suspended during evacuation.
  - Redundant web servers.
  - UPS units.
  - and more...

Target of Analysis

- **PA1:** Raw visual data and sensors data
- **PA2:** Data produced by estimators
- **PA3:** Directions displayed by Dynamic Intelligent Signs (DIS)
- **PA4:** Elevator control
- **PA5:** Actuators control
- **PA6:** Alarm control
- **PA7:** Communications with Emergency Control Center (ECC)



Scenario 1: Cyber attack [1/2]

T#	ASSET(S)	THREAT/RISK	RANK
T1	Wireless Sensor Network	Telnet/SSH intrusion. Very high impact and moderate likelihood.	High
T2	Web servers	Denial of service. Very high impact and easy to carry out.	High
T3	Central Control Box	Abuse of rights by technicians. Very high impact.	Medium

Scenario 1: Cyber attack [2/2]

SC#	Threat	SECURITY CONTROL(S)
SC1	Telnet/SSH intrusion	Change default access configuration and institute a policy to periodically update these configurations.
SC2	Telnet/SSH intrusion	Install an Intrusion Detection System able to raise alerts in case of suspicious accesses (e.g. access from non-whitelisted IP)
SC3	Denial of service	Install a Firewall and institute a configuration policy.
SC4	Denial of service	Implement filters to block unwanted traffic.
SC5	Abuse of rights by technicians	Log the commands that are issued to the CCB, in order to provide accountability in case of accidents.

Scenario 2: Cyber-physical attack [1/2]

T#	ASSET(S)	THREAT/RISK	RANK
T1	Web Servers	Malware planting through USB or flash drives. High impact and moderate likelihood.	High
T2	Uninterruptible Power Supplies	Unplugging from the sockets. High impact and medium likelihood.	High
T3	Wireless Sensor Network	Criminal damages. High impact and moderate likelihood.	Medium

Scenario 2: Cyber-physical attack [2/2]

SC#	Threat	SECURITY CONTROL(S)
SC1	Malware planting through USB or flash drives	Block the USB ports or have security personnel and detectors at the entrance of the server room, so that no one is allowed access to the room with suspicious drives on them.
SC2	Malware planting through USB or flash drives	Run periodical anti-virus scans to make sure that the servers haven't been compromised. Institute a reconfiguration policy so that, in case of viruses, the servers can be cleaned up and set back up as fast as possible.
SC3	Unplugging from the sockets	Isolate the UPS into locked cages accessible only by authorized personnel using keys. Some barriers on the sockets could be installed and the keys must be given only to the authorized personnel.
SC4	Unplugging from the sockets	Hire security personnel to supervise the UPS rooms. If something suspicious happens they must intervene.
SC5	Criminal damages	Make use of barriers to guarantee a suitable physical protection of sensors and actuators.
SC6	Criminal damages	Hire security personnel in order to intervene in case of theft or tampering with sensors and actuators

Rationale behind results

- Study and analysis of what an i-eGRESS system is and how it operates.
- Study and definition (through assumptions) of the i-eGRESS system to be assessed.
- Identification of primary and supporting assets and how they could be affected.
- Main sources for threats and controls identification:
  - Scientific papers*.
  - Personal knowledge.
  - Verizon breach and incidents report 2016.

* All the references used can be found on the report