Simulation Team

La SECURITY nella DOMOTICA: il problema della SICUREZZA nel BMS

Prof. Agostino G. Bruzzone

Email agostino@itim.unige.it
URL www.itim.unige.it

Università degli Studi di Genova

www.liophant.org

Simulation Team

La SECURITY nella DOMOTICA: il problema della SICUREZZA nel BMS

Prof. Agostino G. Bruzzone

Email agostino@itim.unige.it

URL www.itim.unige.it

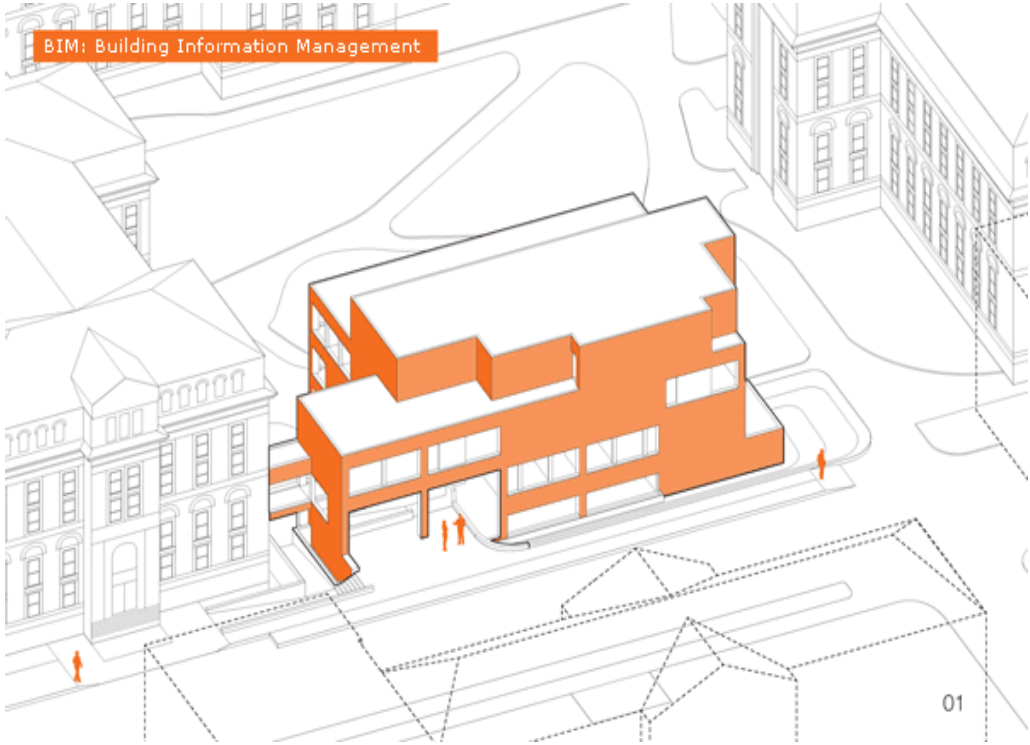
Università degli Studi di Genova

www.liophant.org

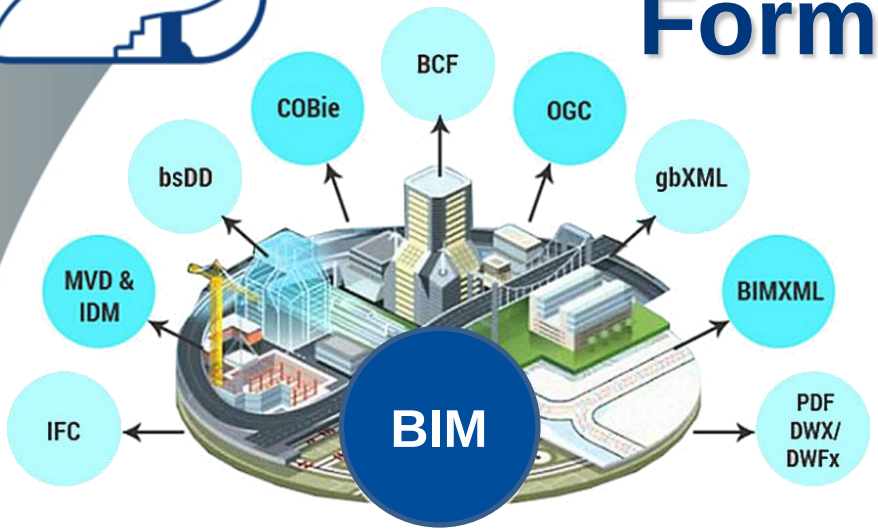
BIM: Building Information Modeling

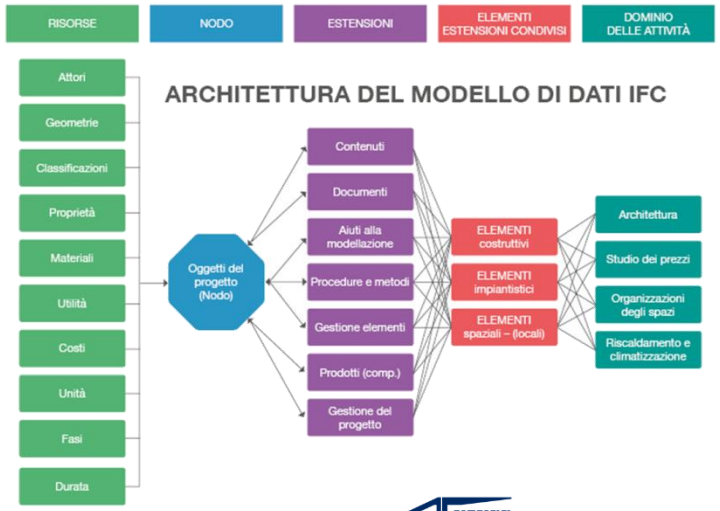
BIM is the activity devoted to create a Cyber Physical System from a Building

BIM is the process to generate and manage all digital representations of physical and functional characteristics of a Building. In the BIM thee are many different files which can be extracted, exchanged or networked to support decision-making regarding the building or management of the Infrastructure.



BIM & Interoperability Formats



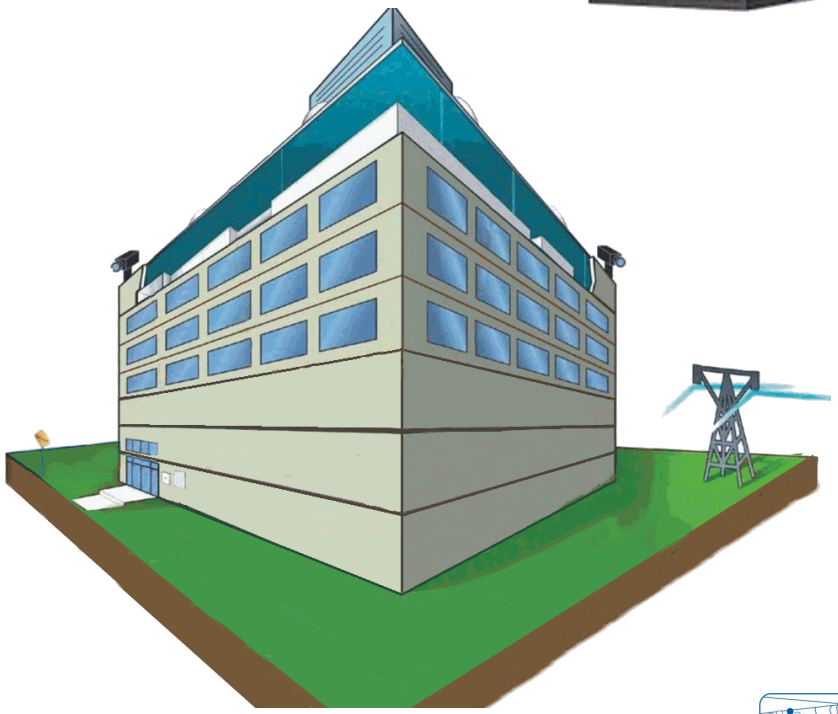


AIM	Asset information Model
BAS	Building Automation System
BIM	Building Information Modeling
BMS	Bulding Management System
CAFM	Computer Aided Facility Management
CMMS	Computerized Maintance Mngmt. Sys.
EMM	Environmental Management Manual
HS&E	Health, Safety & Environmental Mngmt.
PIM	Project Information Model
RAS	Radio Alarm System
bSDD	Building Smart Data Dictionary
BCF	BIM Collaboration Format
COBie	Construction Operations Building Information Exchange
IFC	Industry Foundation Classes
IDM/MVD	Information Delivery Manual/Model View Definition
OGC	Open Geospatial Consortium
gbXML	Green Building eXentsible Markup Lanaguage
DWFx	Design Web Format XML

BMS: Building Management System

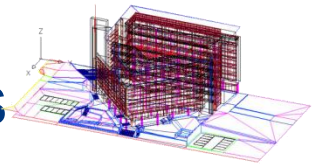
BMS is the Control System of the Building and addresses widely automation and monitoring

BMS is a computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as HVAC (Heating, Ventilation and Air Conditioning), Lighting, Power Systems, Fire Systems, Communications, Elevators, and Security Systems



BMS & BIM

ICT, IoT, IIoT are the enablers for BIM & BMS



BIM corresponds to the creation of a reliable interoperable model composed by set of data and information

BMS controls the different systems, sensors and automation solutions in the building

ICT Information & Communications Technologies
IoT Internet of Things
IIoT Industrial Internet of Things

Not only Saving & Comfort… but Selling Business

The Global Sensor and Device Market for Home Security and Automation was expected to grow from $1.4bn in 2015 to $4bn in 2019

92% Installers say **Home Automation** is growing and works on:

81% IP CCTV
74% Alarms
72% Smart Locks
54% Electric Blinds
48% HVAC
47% AV

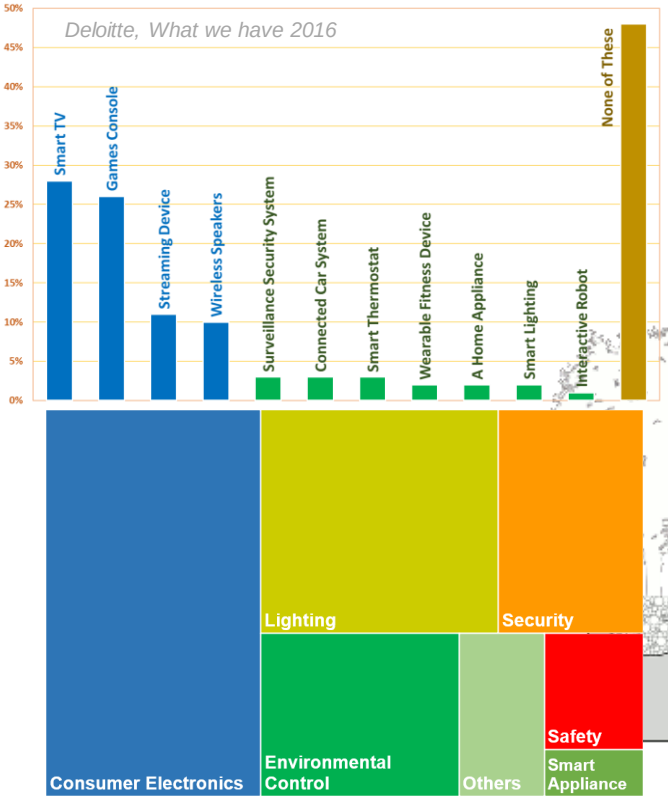
IFSEC Global Research

Barriers to Adoption

Price Barrier 48%
Technology Limits 26%

Deloitte, UK 2016

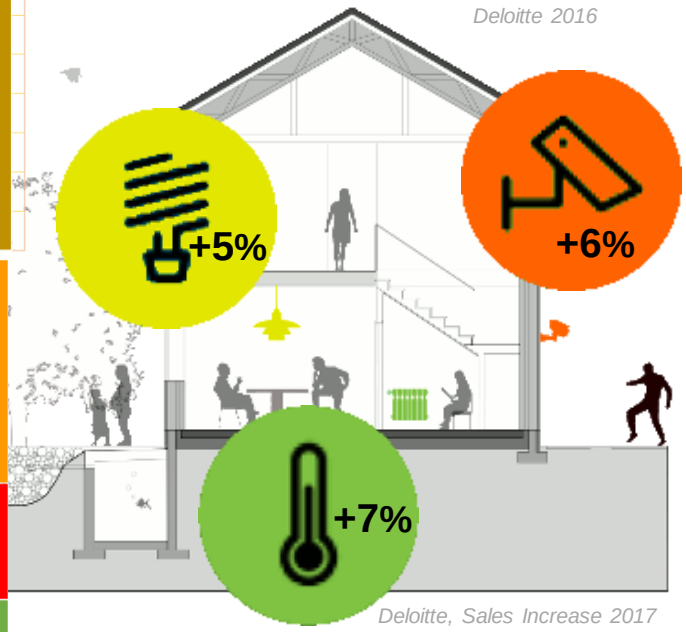
Deloitte, What we have 2016



Berg, North America Market Share 2014

ABI Research, 2016

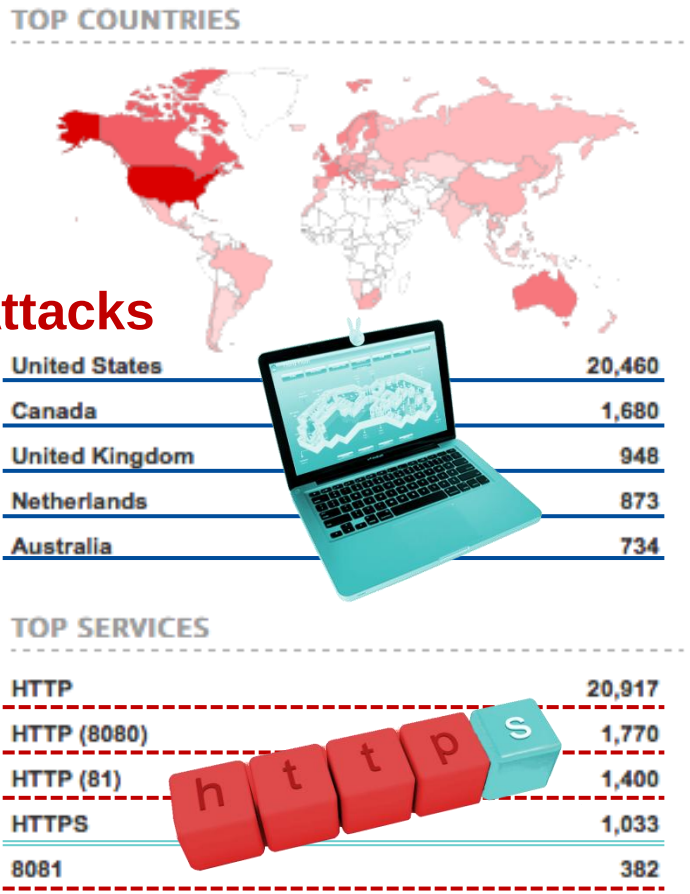
Deloitte 2016



Deloitte, Sales Increase 2017

40% of BMS has been Attacked

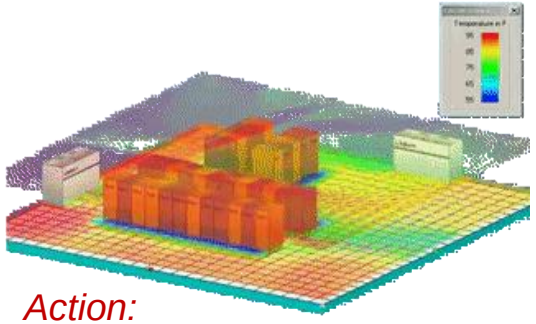
- **40%** BMS and Industrial Automation Systems have been subjected to Cyber Attacks Just in the 2nd half of 2016 (Kaspersky Labs)
- A Statistics on 28'406 Honeywell Niagara BMS in use through Web service shows that only **3.6%** adopted **HTTPS** (Hyper Text Transfer Protocol with Security) (Alpha Guardian)
- The ratio between Shield and Sword is still very in favor of Attackers



Cyber & Smart Buildings

BMS and EMS (Energy Management Systems) have vulnerabilities not just unique, but also extended to most digital control systems. Most BAS communication protocols have their origins with serial communications and have often no protection respect cyber attacks. Today BMS and EMS are interconnected to the Ethernet networks, linking these systems to the corporate networks and many others. Virtually every building has a BMS or HVAC system.

Joke:
Cooling Meeting Rooms
… or Diversionary Tactic



Action:
Overheating Data Farm Room
Shutting Down Key Servers

Do you stuck your Password on the Fridge?

It is not necessary to attack your PC or Mobile… new Kitchen Appliance provide new vulnerabilities:

- **To get your Google Account by MiMT from a Fridge able to propose you the Google Calendar (2015)**
- **To generate a Junk Mail Campaign spamming 750’000 emails from 10’000 Home Devices (2014)**
- **To watch your home from Always On Camera from Smart TV (2015)**

Domotics as Backdoor?

There are many reports of hacking activities successfully compromising thousands of gadgets, for instance to launch malicious email attacks.
Today Surveillance Cameras, Smart TVs, Garages, Refrigerators and Thermostats are offering connectivity and represent example of IoT for Domotics, therefore most these devices are pretty vulnerable and not protected by anti-virus, nor adequately regularly monitored to update patches resulting as Back Door to entry in your Buildings, Plants and Homes

Cyber Attacks…? *Are Now!*

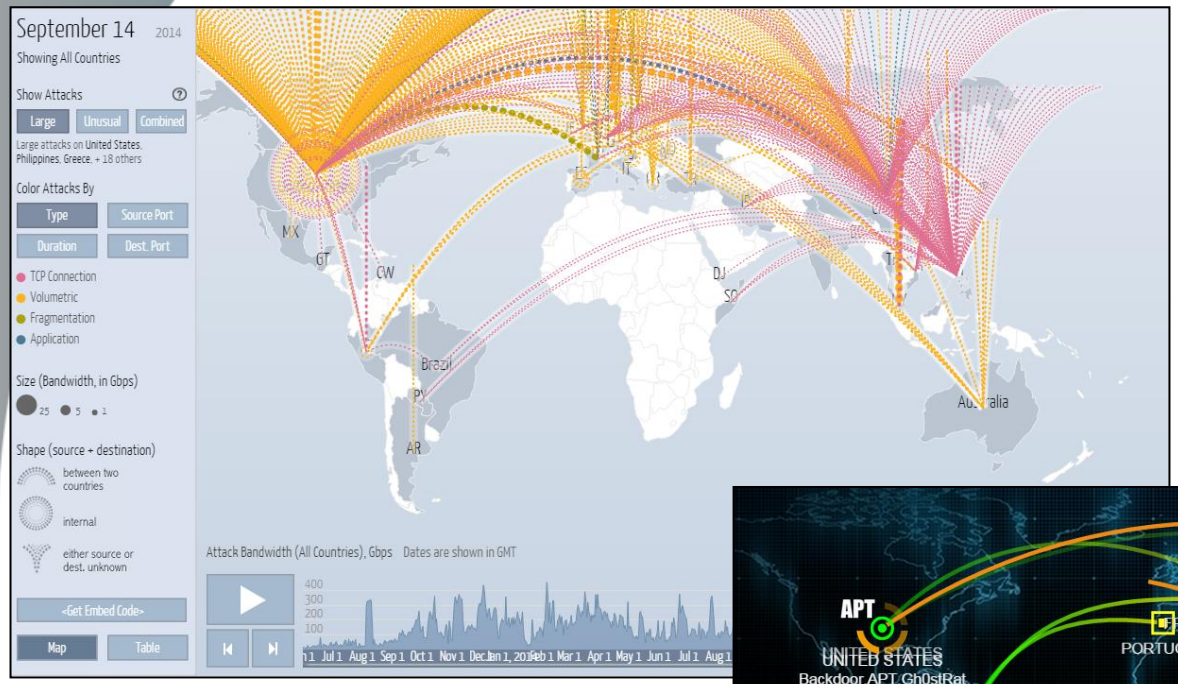
Friday, November 17, 2017, 0700 Z

Cyber Attacks are able to disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple strategic assets & critical infrastructures such as Communications, Power, Transportations, Finance, Health Care.

Cyber Attacks are addressing both **Civil** and **Military Targets**

Cyberwarfare is a Cyber-based Conflict involving motivated attacks on information and information systems.

Cyber Attacks are on going



- **Cyber Attacks are on going second by second. Therefore in correspondence of critical events Specific Attacks demonstrated much high virulence**

- ***Llyod's*** **estimates Costs for around 400 bUSD year due to Cyber Attacks… *but 2.5 bUSD. premium doubling in 2 years***

Cyber Security & Cyber…

Cyber Security** is defined as… the protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide* ***Morrie Gasser (1988) Building a Secure Computer System

κυβερνάω: (et.to turn a cylinder) to Steer, to Govern to Control

Cyber: the scientific study of control and communication in the animal and the machine ***Norbert Wiener (1948) Cybernetics***

Cybermusic: There is some cyberpunk for you… DJ on Gary Neuman (1979) Cars

Cyber… what? Love or War?

Cybersex: Zaphod had spent most of his early history lessons plotting how he was going to have sex with the girl in the cybercubicle next to him ***Douglas Adams (1982) Life Universe & Everything***

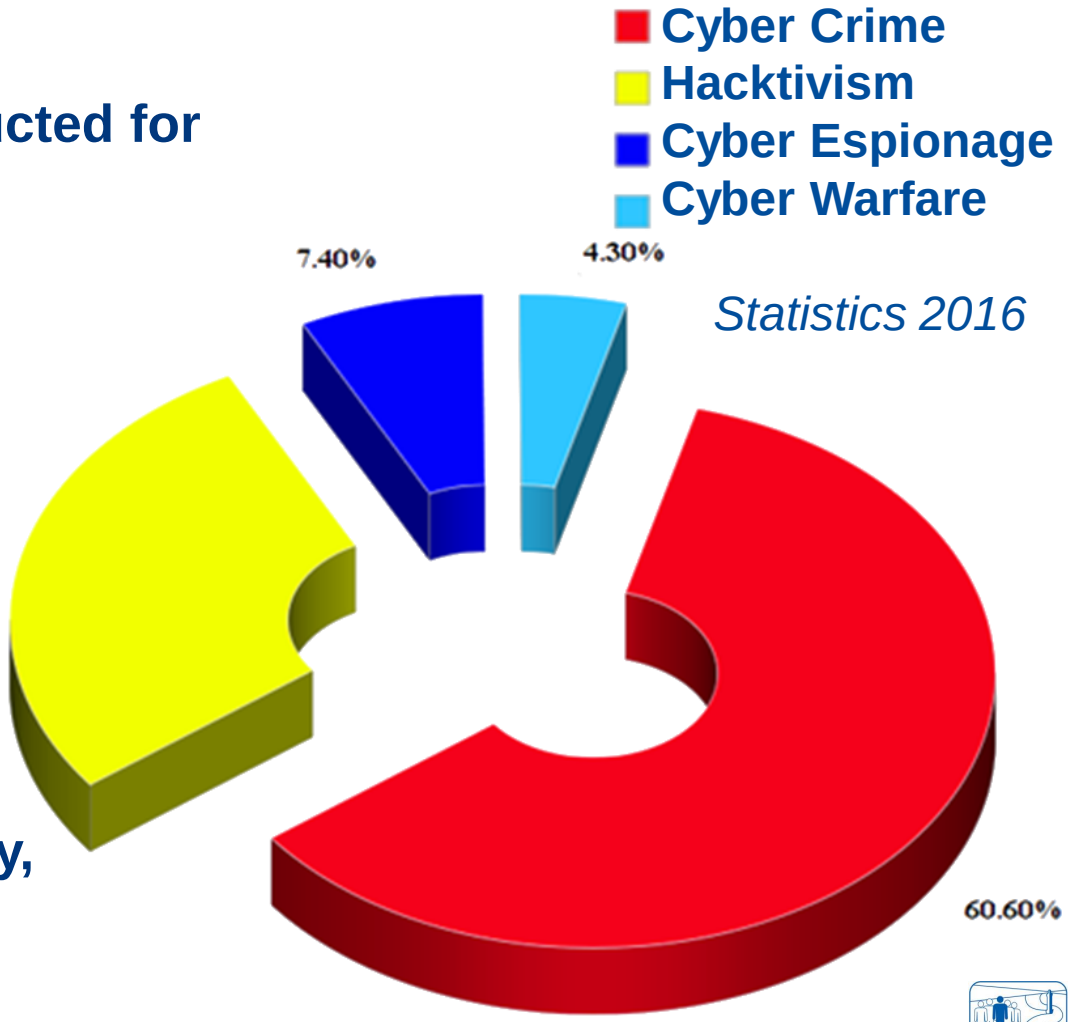
Cyberspace: Cyberspace Seven […] Chrome's castle is dissolving, sheets of ice shadow flickering & fading, eaten by the glitch systems that spin out from the Russian program, tumbling away from our central logic thrust and infecting the fabric of the iceitself. Me glitch systems are cybernetic virus analogs, self-replicating and voracious. They mutate constantly, in unison, subverting and absorbing Chrome's defenses ***William Gibson (1982) Burning Chrome***

Cyber Attacks for What

Cyber attack are conducted for different purpose:

- **Stealing of Information and Espionage**
- **Denial of Service**
- **Propaganda and Fake News**
- **Sabotage**

Every attack affects one or more crucial elements such as Confidentiality, Availability, Integrity or Privacy



Are we just stealing Data? …or Money?

Big Data are a resources also for Attackers in Cyberspace

- Yahoo 2013 & 2014, Over 1 billion accounts
- TJX, 2003, 45.7 million credit/debit cards, driver's licenses
- FriendFinder, 2016, 412 million accounts on dating
- Ebay, 2014, 145 million accounts
- Heartland Pay.Syst, 2008/2009, 130 million credit cards
- Target Stores, 2013, 110 million records compromised
- Sony OE., 2011, 102 million records compromised
- Anthem, 2015, 69 million health insurer records
- Home Depot, 2014, 56 million credit and debit cards 10.5 GUSD (~194 USD/card)
- LinkedIn, 2012, 6.5 million accounts (4%), password cracking in 72h for 90% cases

Your Money or Your Data… Ramsomware

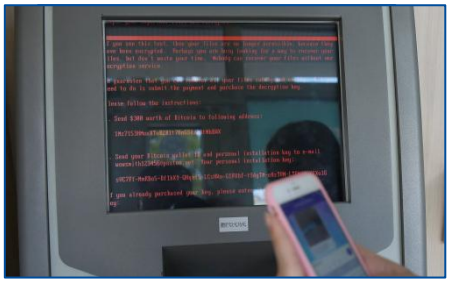
May 12, 2017: Worldwide Cyber Attack by WannaCry, Ransomware Cryptoworm, using EternalBlue against Windows OS, adopting Data Encrypting & Ransom Request in Bitcoin (600$/3 days, 300$/ 6 days). 130 k$ in 1 month. 230'000 PC Infected. 150 Countries. UK Health Care infected

June 27, 2017 Glogal Cyber Attack by the Petya, Ransomware, based on EternalBlue targeting Windows OS. First action on Ukraine, followed by France, Germany, Italy, Poland, UK, USA, etc. Targets: Companies, Nuclear Plants, Health Care, etc. NATO discussed on adding Cyber among Art.5 triggers

Eternal is attributed to NSA

Simulation Team

Playing Cyber War?



- Estonia, April 26-May 23, 2007, DDS, Botnet, Ping floods: All Government, 2 Banks, Political Parties, No Parliament Email, No Credit Cards, no ATM
- Georgia, August 7-12, 2008, DDS, Botnet, Web Defacement, Sql Injections, Spamming: News and Government Websites Down, Gov.Comms down with the World, Banks & Cell Phones down.
- Kyrygistan, January 18-31, 2009, DDS, ¾ IPS down, 80% internet down, mobile down
- Ukraine, Dec 2015 / Jan 2017, SCADA, Blackouts 230'000 People for ~2 hours

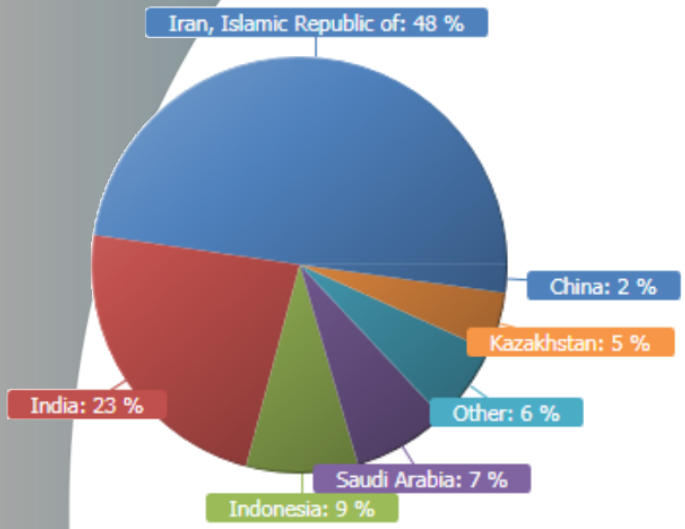
The "Response":

NATO	October 2007 CD Report & 2008 CCD Coe Center
CERT	*we believe the attacks were DDoS Attacks*
CIOC	*tuteliamo il C2 per un'efficiente condotta militare*

DoS	Denial of Service
DDoS	Distributed Denial of Service
IPS	Internet Provider Server
CD	Cyber Defense
CERT	US Computer Emergency Readiness Team
CCD COE	Cooperative Cyber Defense Center of Excellence
CIOC	Comando Interforze per le Operazioni Cibernetiche
C2	Command and Control

STUXNET 36 Months Later

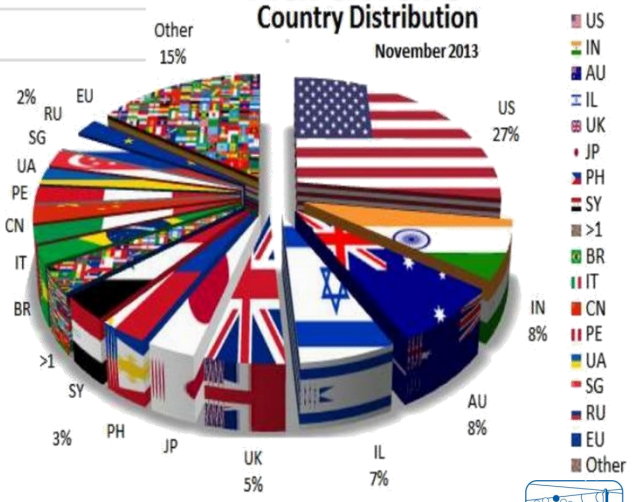
Geographical distribution of Stuxnet infections 2013-2014.



Percentage	Infection Records	Trojan
47.71	198	Iran, Islamic Republic of
23.13	96	India
8.67	36	Indonesia
7.47	31	Saudi Arabia
6.27	26	Other
4.58	19	Kazakhstan
2.17	9	China

Country distribution of Stuxnet infections 2013-2014.

- **Discriminating Targets and adopting Deception and Sabotage on Hardware**



- **SCADA (Supervisory Control and Data Acquisition.) are so infected that 36 months after the attack there still major contaminations**

Simulation Team

Oil should keep going…

- Middle 2012, Ramadam month, Aramco Saudi Offices: a click on a scam email injects a Virus… August 15, the Virus turn on:
- 35'000 Computers Partially/Totally wiped out in few hours
- Millions of File Erased, People Ripping Cables of Serves Worldwide
- Oil production steady at 9.5 million barrel per day and keeps going
- Turning Down the Internet Connections, the Company Phones, the ICT Services for Supplies, Shipping, Gov. & Private Contracts
- Company forced to go back on Typewriters, Paper & Fax signatures
- Overload for manual operations, Stops in local Oil sales
- After 17 days of block, Oil is given for free to keep it flowing
- Emergency Acquisition and Installation of 50'000 Hard Drives
- 5 Months to restore the Network, Cost Estimation over 1 billion $

The Game is Changed

- IoT (Internet of Things) vs. IoE (Internet of Everything): **People, Things, Data & Processes**

Massimo Porro, Safe & Secure An unfolding story CISCO

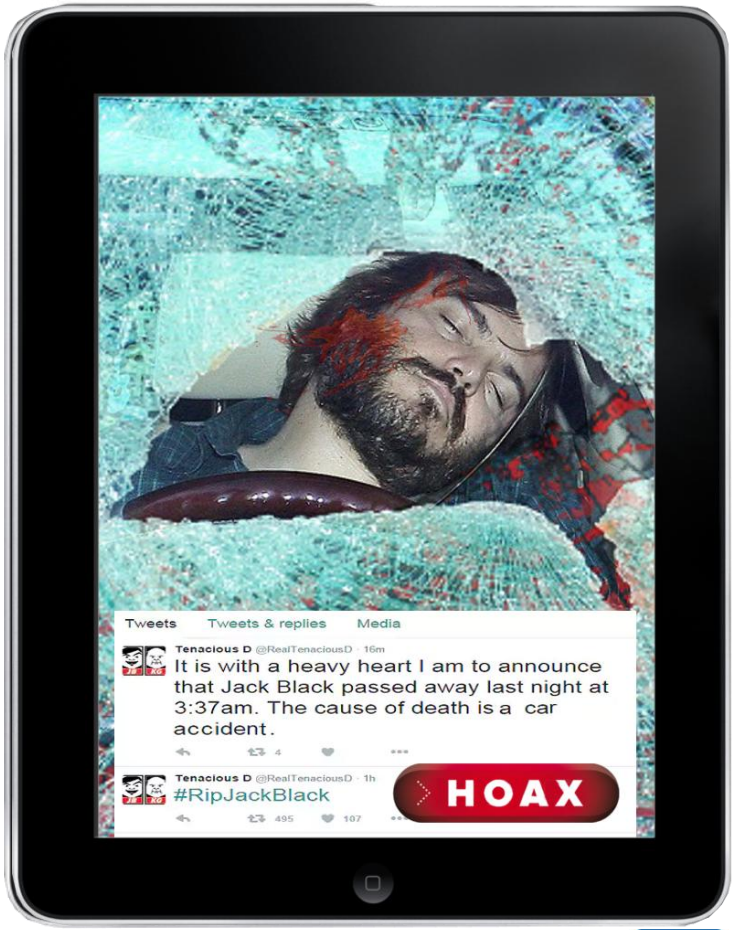
Scared by HVAC Failure… or People Panic?

- Society and People are very vulnerable to Deception & Fake News.
- Social Media reinforces these risks and requires Models to be able to evaluate the consequence of these events

1500 Injured People in few second for Panic during a Social Event

Social Networks… Vulnerabilities & Simulation

- Injection of Fake news is very easy and could change attitude of people
- It is important to simulate Population dynamic reactions to Scenario Evolution on Social Networks, driven by Intelligent Agents
- It is necessary to simulate the impact of fake news and other media attack and population reactions

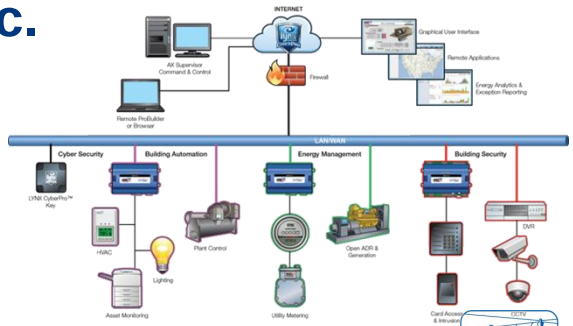


New Laws & New Regulations

- Networked power, cooling and security systems accessible through a remote VPN or other connections are part of the Industrial Internet of Things (IIoT). All these IIoT can be compromised from a Cyber, Physical or Operational basis, then the data systems that they support will be compromised as well.

- New regulations are emerging such as NIS (Directive on security of network and information systems), GDPR (The General Data Protection Regulation), NY Cybersecurity Law, etc.

- BMS should be compliant with these regulations



For instance

HVAC: you will feel hot not at the office… but in your Wallet

A major cyber attack on Target, a major USA Retailer, started by **Malware-laced Phishing Emails** sent to **employees of a supplier** of HVAC systems. This vendor had access to Target's network login credentials to **remotely monitor temperatures & energy consumption** in stores where the HVAC systems were installed. The phishing attack **turned up those credentials**, so the hackers used them to **access the store's corporate network** and, specifically, the **company's payment systems**. This is an example of a devastating low-tech simple attack.

Securing Doors… remotely… what a comfort.. but Hard to Fix!

Several Systems have been turned popular to remote control door locks… therefore these systems sometime are vulnerable. For instance in December 2015 Hacking Test successful demonstrate the capability to intercept the pin of SmartThing, Samsung IoT Platform (a reliable solution), when changing setting the door lock and to use to install a *Lock-Pick Malware Application* able to open the door, while it is “closed”, to change the pin and to lock it. In addition it was possible to set off the “vacation mode” on lights and disable fire alarm.

The issues were hard to fix and a lock's PIN code could still be snooped and reprogrammed by a potential hacker at least up to May 2016

Power Building… Vulnerable

- **Primary Power Systems**
  - Switchgear, Power Panels, PLC's
- **Backup Power Systems**
  - UPS, Power Distribution Units, Generators
- **Mechanical Systems**
  - Chillers, Air Handlers, Cooling Towers, Boilers
- **Building Management Systems**
  - BMS, EMS (Energy Mngt System, DCIM (Data Center Infrastructure Management)
- **SCADA (Supervisory Control And Data Acquisition) Systems**

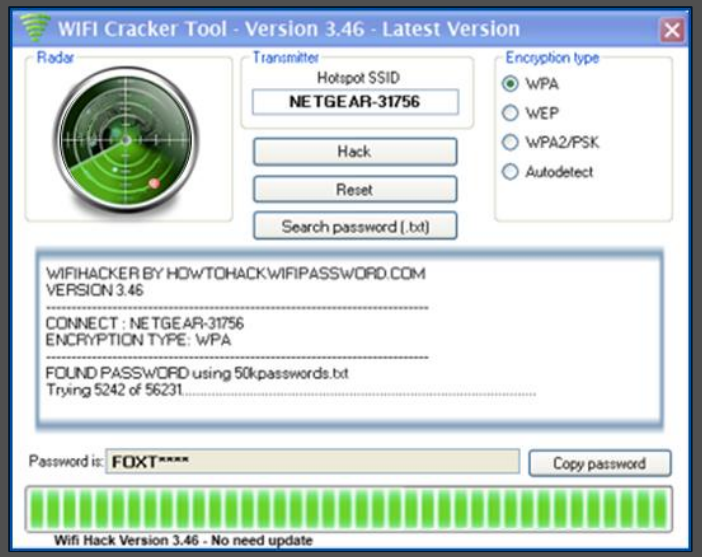
Example
Power Control Systems

- SNMP (Simple Network Management Protocol) are often vulnerable to Spoofing
- PLCs (Programmable Logic Controller) allows hackers with modest skills to access them and take control of switchgear in absence of firewalls

… & WiFi: Lighting Vulnerable

- WiFi technology is extensively used in Domotics for instance WiFi lighting systems use WPA2 encryption feature

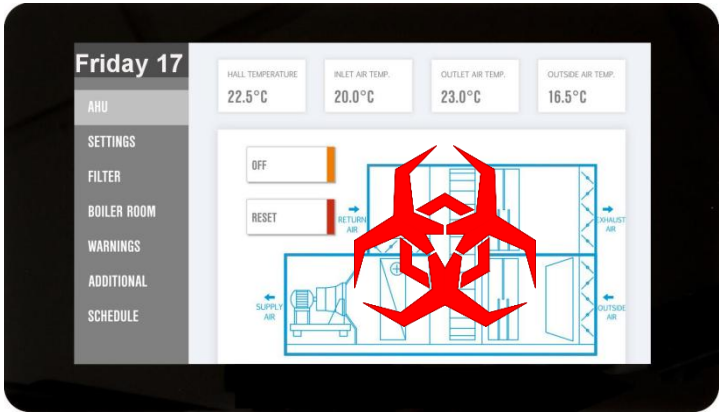
- New generations of WiFi Crackers is usually successful in 99% in breaking these systems and give access to the control



Blackout & Darkness… not only… even Fire!

- Ethernet network is a fairly new form of communication for fire systems. National Fire Alarm and Signaling Code (NFPA 72) covers the requirements for networking fire panels and control systems and it requires that all segments be separated and secured.
  NIST (National Institute of Standards Testing) identified Risks on new Fire Control Panels suggesting to add security barriers on HW layer.
- Indeed, some Fire Control Panel provide services by emails
  Simple passwords over HTTP are at risk of interception and email accounts could be easily captured .
  Once compromised it is possible to access configuration files, circumventing all fire panel system security.
- WannaCry, EternalBlue, Petya, etc. could affect these systems if not protected.

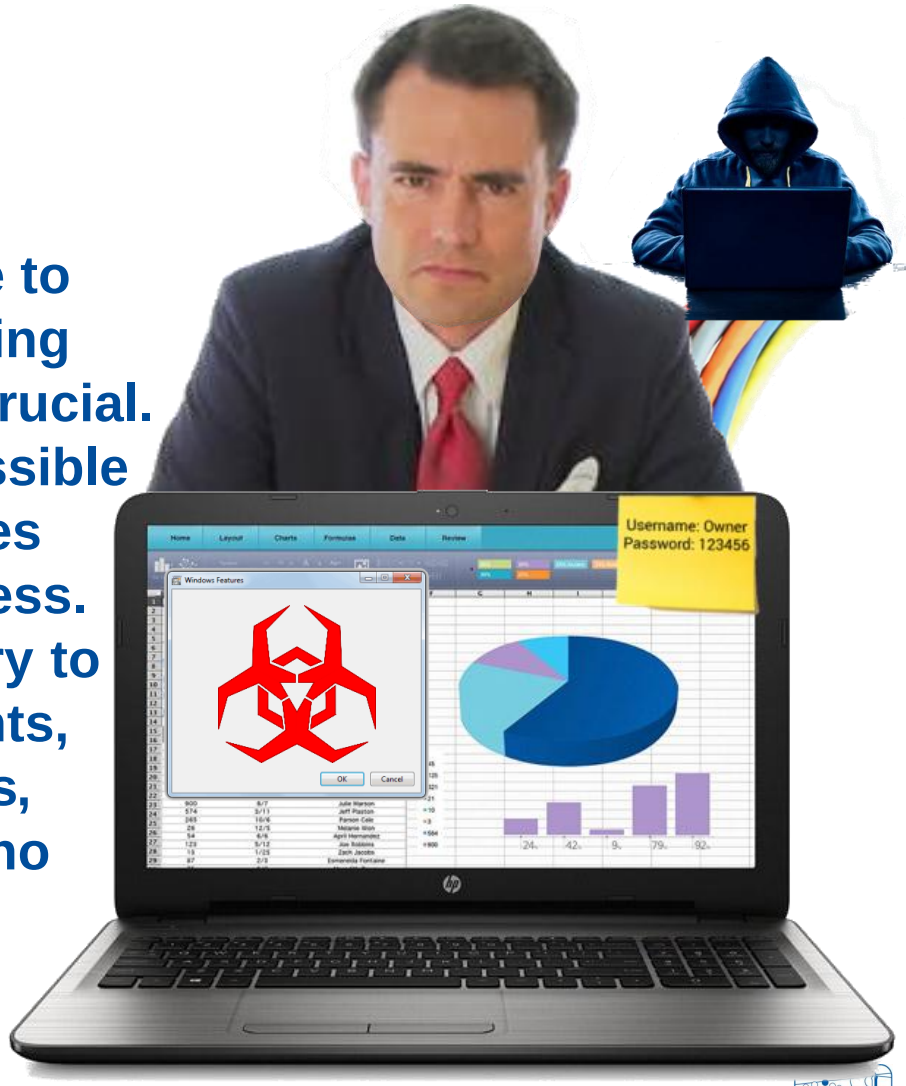
Saving by Web Services… but pay attention to backdoors



Web servers and new BAS enable to concentrate controls and Reduce Costs in installation & operations for buildings

It's common in facilities and engineering departments to have a supervisor machine that has a web server for the control system; to simplify things, often a second network card is added to the machine for accessing the corporate network. Once that happens, it's possible for attackers to enter via the BAS and pivot to the organizational network. Indeed today it is easy to bridge networks. In facts, some hacking is just for fun, but often they are addressing specific goals.

Risks from Outside… and Inside



BMS vulnerability is no only due to external attacks: Social Engineering and safeguarding from within are crucial. BMS are often multi-user web accessible This provide additional functionalities And use but introduce cyber weakness. To secure the systems it is necessary to reengineer process, manage accounts, control privileges. Expiring accounts, disabling immediately employees who Leave as well as changing accounts when people switch roles are good practices to address some issues.

Ignorance & Lack of Awareness are major Weakness

Due to the evolving, diverse & complex nature of BMS and EMS, many system owners simply do not know where to start when it become necessary to define a cyber security strategy. Lack of Awareness about their vulnerability state means that the effective application of security technology or process is not possible. Many customers have difficulties in determining vulnerability levels, exposure, and possible impacts as well as the inability to monitor who has access to networks and critical assets. They face difficulties also in distributing and enforcing appropriate policies and procedures.

BMS Vulnerabilities are… not just on Naive People Homes

May 2013: Google Offices BMS at Wharf 7, Sidney is simply penetrated by using Shodan and by exploiting the password of Tridium Niagara AX platform

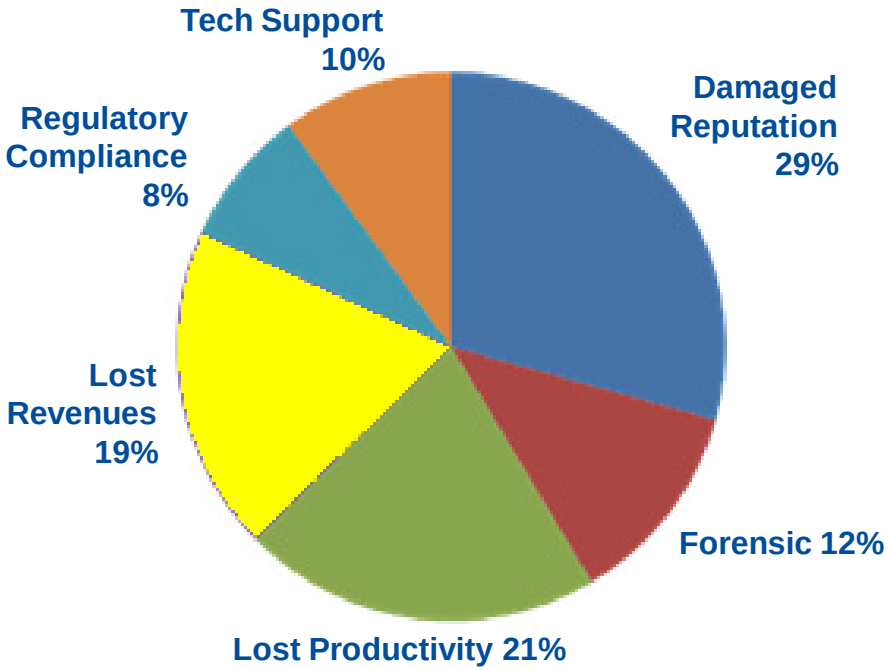
The penetration granted: HVAC Control, View of Active Alarms and Overrides, LAN Diagram, Schedule, Blueprints of floors and roof plans, water pipelines & temperatures online

How safe we want to be?

We need to carry out trade off analysis and consider second effects. Usually in BMS is crucial to address:

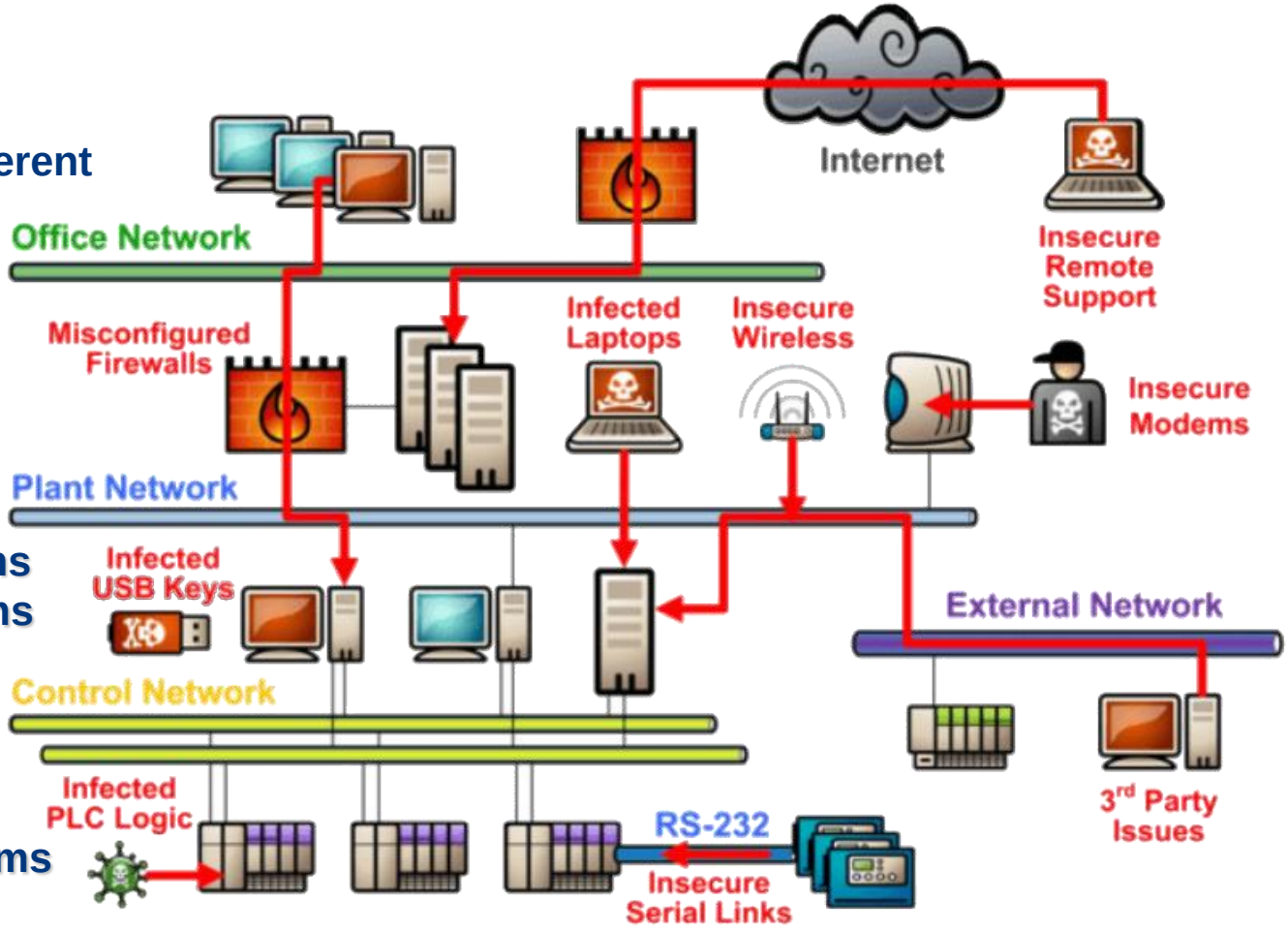
- Password management
- Network management
- User management
- Software management
- Vulnerability management

Cyber Attack Cost Breakdown



Accessing & Affecting…

- Approaching Different Systems
- Approaching from Different Layers
- Compromising Systems Affecting other Systems
- Capturing Credentials To access other Systems



Domotics & Security….
… an Ideal World…





- Today is possible to Secure Buildings by means of a variety of security options (e.g. Absence Alarm, Smoke Alarm, Personal Emergency Alarm, CCTV & Sensors, Perimeter Controls etc.).
- It is possible to activate Alarm notifications by phone or SMS and activate various alarms, including active burglary prevention solutions.
- These systems include often Wireless Burglar Security Alarms and Burglary Alarm Reports by email, SMS and phone. The CCTV camera systems enable to monitor buildings and, if the alarm sounds, to record images and video of the situation available for download and review from anywhere anytime

… lets take a look inside...

How to Hack your Home CCTV in 6 easy steps

don't do it at home and be sure your vendors take all the countermeasures

Since several years (Houston, 2013 & Cincinnati, 2014) there are reports of baby monitor hacking. Hackers yelled at child in the middle of night: "Wake up!" plus obscenities. The monitor maker claimed vulnerabilities were due to lacks in firmware updates, by families, of devices dating over 6 months.

1. Download
2. Choose IP e)
3. Configure
4. Search for
5. Start IP Range Scanning and access detected CCTV through Browser
6. Use Default Usernames & Passwords (e.g. **admin**, *none*, **12345**, **9999**)

CONGRATULATION you set a good password on your CCTV System

Does not Work!

7. **TOO BAD:** we crack the CCTV Camera Password (e.g. Kali Linux with Hydra)

39

Secured by Producer Smart Design

Smart Lamps HACKED by accessing trough a nearby computer (e.g.UAV). In 2016 a distributed unit was forced to accept a nefarious firmware update by exploiting a weakness in the Touchlink aspect of the ZigBee Light Link system and bypass built-in safeguards against remote access. Then extracting the global AES-CCM key used by manufacturer to authenticate & encrypt new firmware Malicious firmware disable downloads, cause one permanent blackouts, constant flickering, etc. The attack is a worm able to jump from a device to another device through the air, potentially knock out an entire city with just one infected bulb at the root in minutes.

Click for more

Thermostat HACKED through physical access to the device. It was take control of Nest's Linux operating system during device boot and loaded custom software onto it (jailbreaking) through device's USB port. It was loaded "hacker custom software" onto it, stopping the envoy of thermostat data to Nest's servers and starting to attack other vulnerable systems on WiFi Network

SOS Message on the Lamps imposed by Hacking from UAV

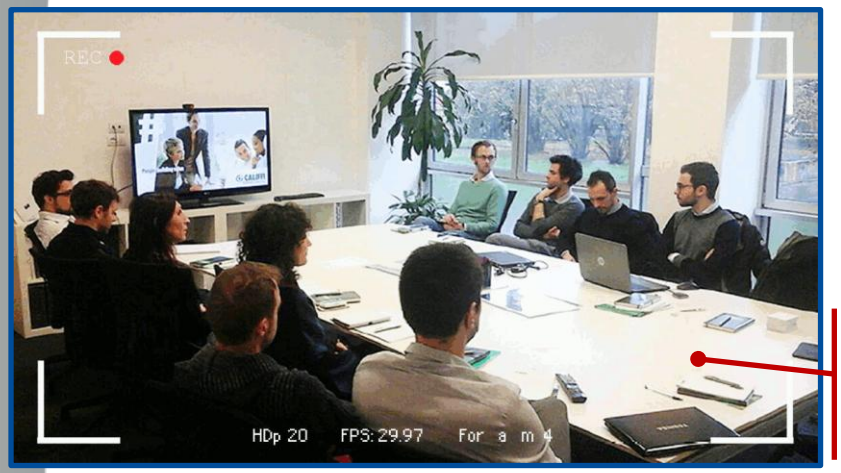
compromise HomeKit This not platform because as a HomeKit accessories cannot communicate directly among themselves. HomeKit-only devices are still highly secure, while only attack path is through an iOS device (iPhone/Apple TV) even if it is still very hard to crac, plus if attackers gain control of an iOS device he could just spread malware to this bluetooth low energy light switch.

QR Quick Response Code
RSA Rivest–Shamir–Adleman
TLS Transport Layer Security

Thinking bad…

HVAC overheating Server Room

Fake Alerts on Speaker & Panels create Panic



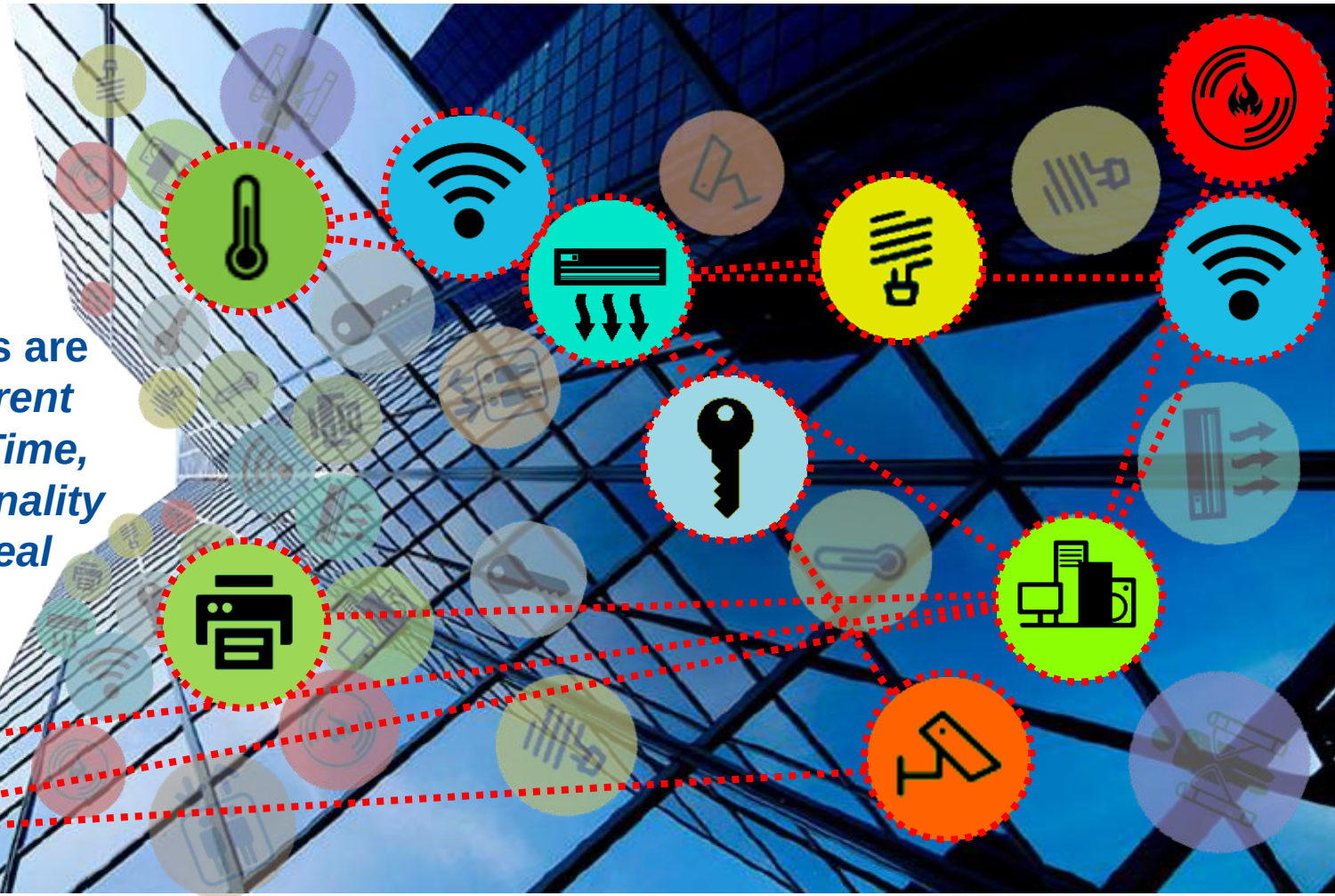
Fire Control & BMS blinded during Fire

Intrusion via BMS In Company TIc System

Seeing through Walls

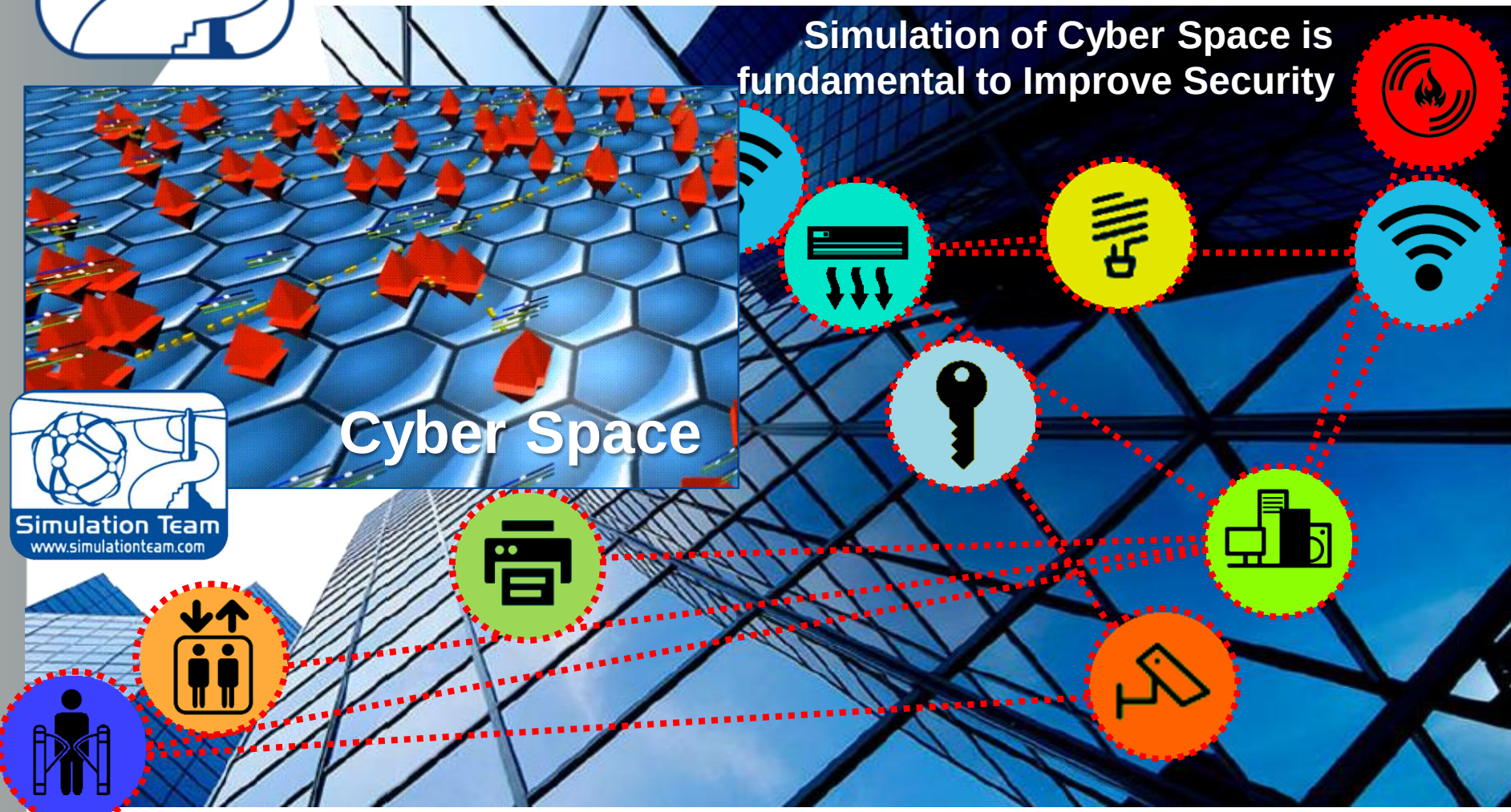
Buildings & Plants
are plenty of devices that live concurrently in Physical World and Cyber Space

Seeing through Walls…



Cyber Attacks are *based on different logic respect Time, Space & Cardinality Concepts of Real World*

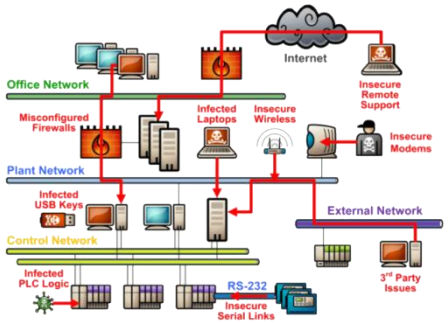
…Prevention by Simulation



Improving Security of BMS

Password Mngt.

Vulnerability	Reason	Best Practice
Too many Accounts	Leaving access around and behind	Auto-expire all accounts
Former Users	People leaving could spill access credentials	Immediately remove accounts of this people
Employer Access Level	Too many privileges could be dangerous	Change Account when Role Change



Vulnerability Mngt.

Network Mngt.

Vulnerability	Reason	Best Practice
Web interface	SQL injection	Install firewall
USB port		Disable Auto-Run
TCP/IP ports		
Open protoc		

Vulnerability	Reason	Bes
Default credentials	Available in online databases	Chang before
Simple passwords	Easily cracked	10- to multi- passw
Demonstration systems	Hard-coded credentials	Chang
Same credentials for all sites	All sites at risk if credentials hacked	
Credentials shared among a group of users	Lack of traceability and accountability	

User Mngt.

Vulnerability	Reason	Best Practice
Controlling systems and services in BMS	This could lead to improper use and damages	Identify Impact of a Vulnerability
Direct and Remote Access to a System/device	Access could introduce & inject changes/viruses	Define the process to access Systems/Devices
Procedures and Methods to access the Systems	Vulnerability could arise for process and procedures	Address the factors affecting the access
Prevention and Reaction based on Common Sense	People under estimates risks and act on contingency	Define a Vulnerability mangament Plan

Vulnerability	Reason	Best Practice
Identified Vulnerabilities in Installed Software	Software vulnerabilities are used by Hackers	Apply Software Security Patches
Applications for Users without Credential	Software could contain Trojans or Viruses	Install only authorized Software

Software Mngt.

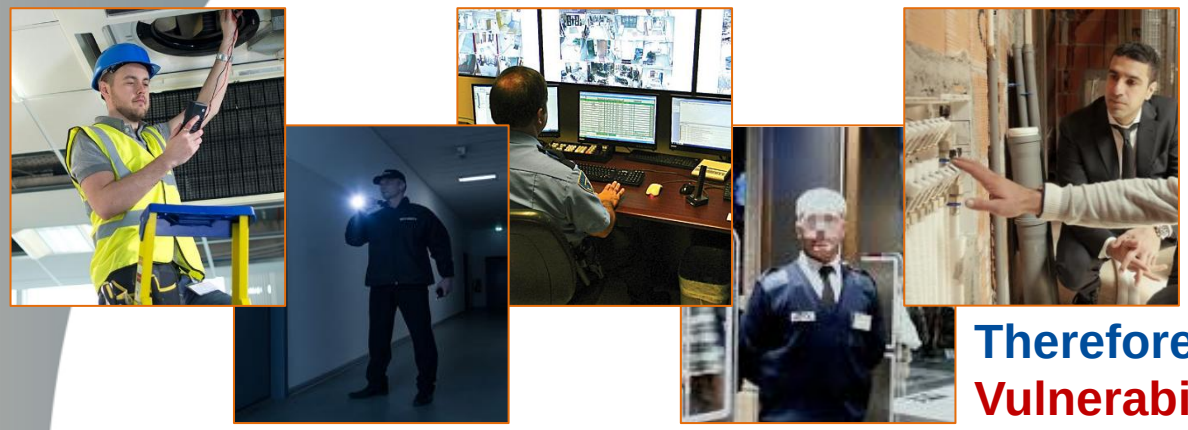
45

Simulation Team

who watches the watchmen?

Quis custodiet ipsos custodes?

Juvenal, Satires, 347-348



New Technologies are too much convenient to be neglected or even to consider to return back to old solutions

Therefore, New Solutions introduce Vulnerabilities to be addressed

Reduced Personnel, Centralized Supervision, Quick Response, Real Time Monitoring, Distributed Control, Improved Efficiency, 24/7 Support, Big Data for Improving,…

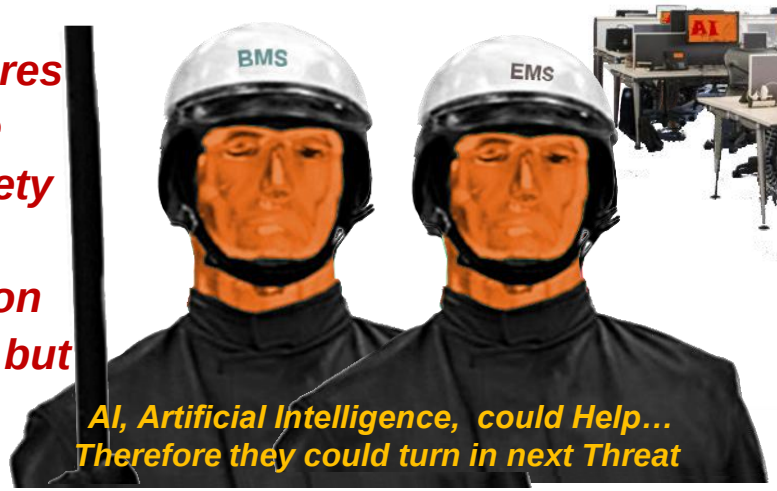
Computers are more efficient than human beings, not better

Spock, Ultimate Computer

Smart Systems based on AI (Artificial Intelligence) and IA (Intelligent Agents) could improve resilience and defensive capabilities

Therefore, future AI, could have Different Perception and Priorities!

AI could adopt measures that could be affecting Safety and Security. Their evolution Is inevitable, but It requires attention



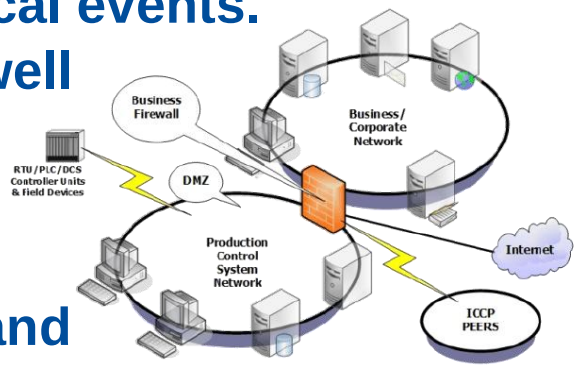
AI, Artificial Intelligence, could Help…
Therefore they could turn in next Threat

Protecting Smart Buildings

BMS is a potentially **Victim**, **Vector**, even **Source**, of **Cyber Attacks**

To prevent these problems it is required to address these issues along design, installation, maintenance, etc. Currently Builders, Engineers and Critical Services Specialists are **Accountable** respect cyber threats in case their design or activities expose assets, the occupants and the public to potential risk. To address these issues is necessary to adopt a **Multi Layer Approach** able to consider mutual relationships and potential consequences of critical events.

BMS provides collaborative opportunities as well as potential sources of risk; it is necessary to jointly address electrical & mechanical systems such as HVAC, Elevators, Fire Safety, Access Points, Power Systems, Networks, Lightings and Surveillance Systems.

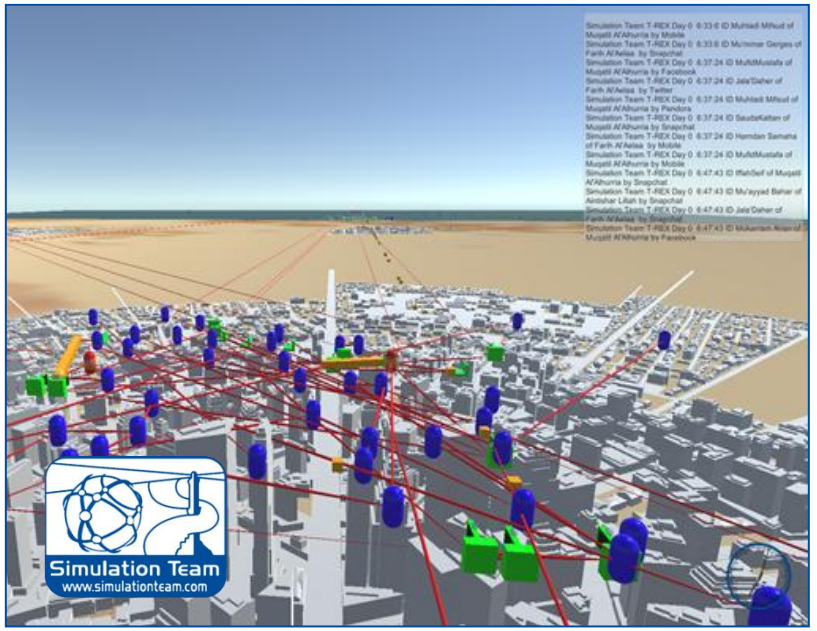


DMZ Demilitarized Zone
ICCP Inter Chassis Control Protocol

De Docta Ignorantia… Periculi et Ingenio Simulatoris

The idea to reduce risk by limitation on use and diffusion of IoT results hard due to the Costs and Benefits used by this approach
The idea to add protections is for sure necessary, but it is evident that in Cat-and-Mouse Game Attackers keep an advantage position

To be conscious of the Risks and quantify them is crucial
To Plan Preventive Measures, Mitigation Actions & Reactions is fundamentals
The key point is to use MultiLayer Engineering Approach and Simulation to Reduce Vulnerabilities and guarantee Improvements



DMZ Demilitarized Zone
ICCP Inter Chassis Control Protocol

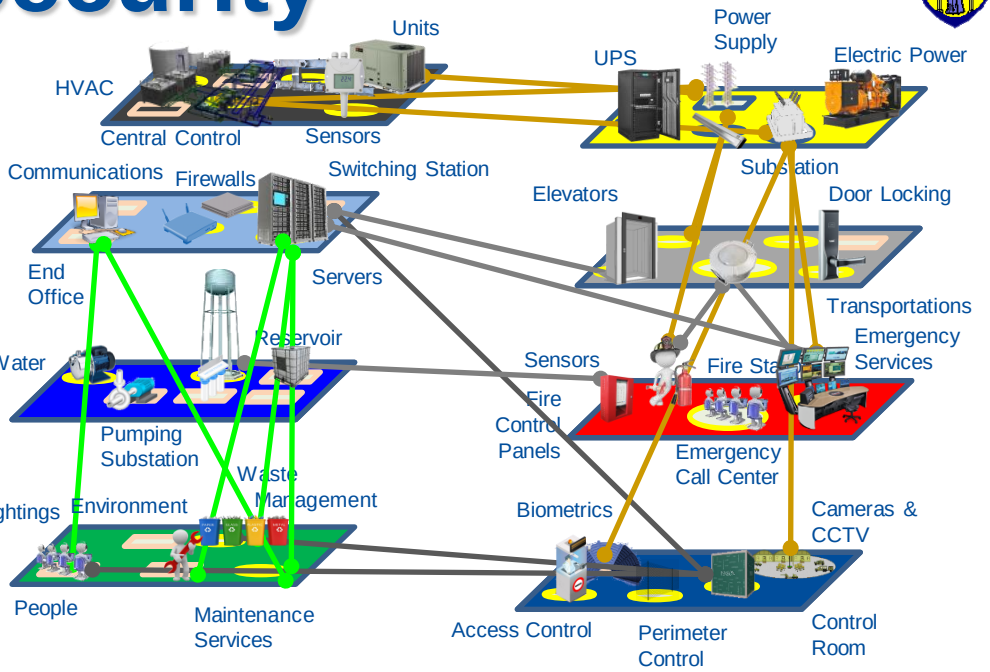
Simulation Team

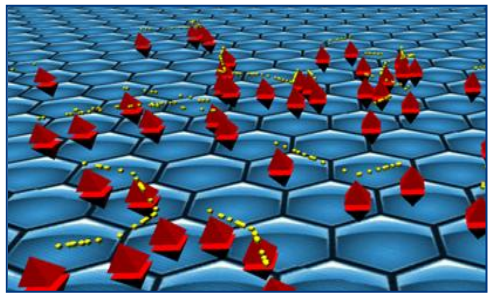
Multi Layer Approach to Safety & Security

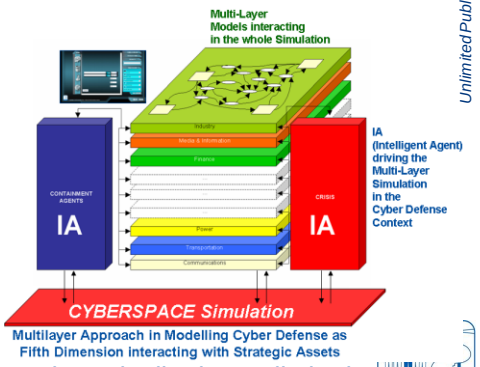
The Modern Building are usually addressing Multiple Layers and requires to consider multiple aspects for developing

- Joint System Design & Engineering
- New Policies & Procedures
- New Technologies and Processes
- Table Top Exercise in order to understand and raise awareness by Human and Machine Learning
- Education & Training Programs for Multiple Users

The use of AI & Intelligent Agent is crucial to automate Smart Simulation







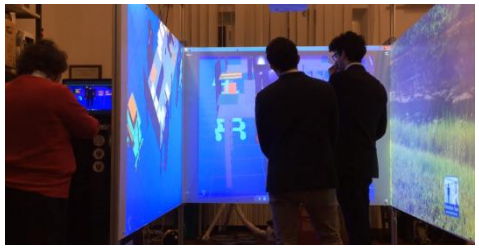
Simulation Team

Interoperable Virtual Simulators & Models

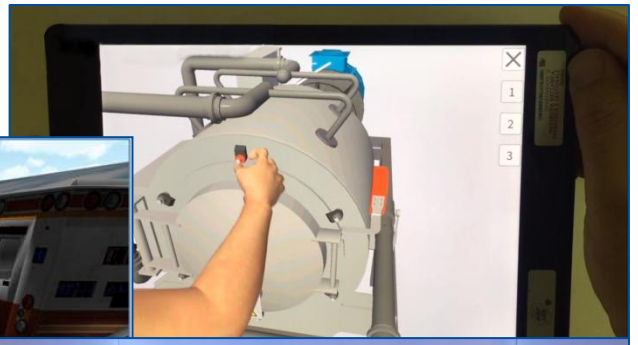
The Smart Simulators represent the crucial element to support advance and revolution in Engineering for Security & Safety. The Virtual Simulators are aids for Operative Resources, Technical Staff & Decision Makers. The Interoperability of simulators could be based on most advanced standards and paradigms (i.e. HLA High Level Architecture, MS2G, Modeling, Interoperable Simulation & Serious Games). These Solutions enable stand-alone and Federated Simulation of Operations, Activities and Processes.

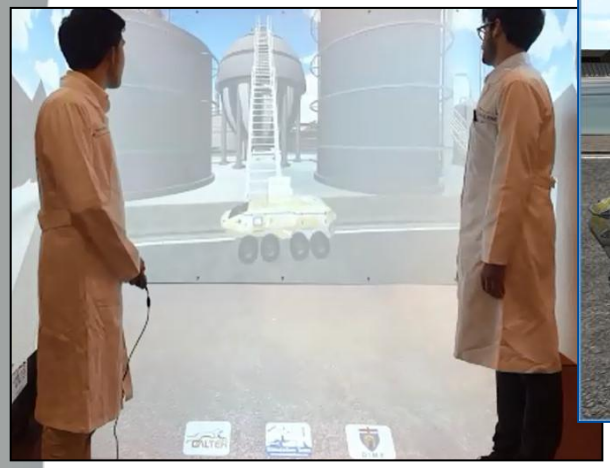
Simulation Team have very long experience in Project with major Industries and leading International Agencies and Institutions

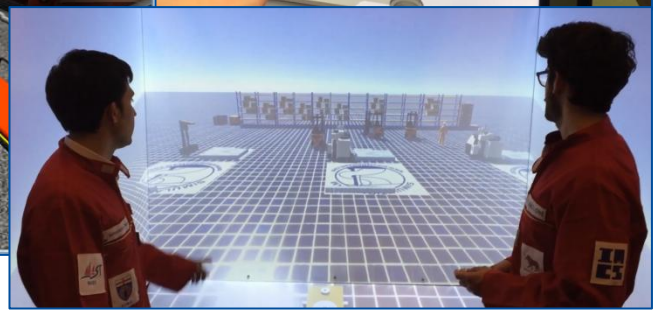
MS2G Paradigm as new Enabler



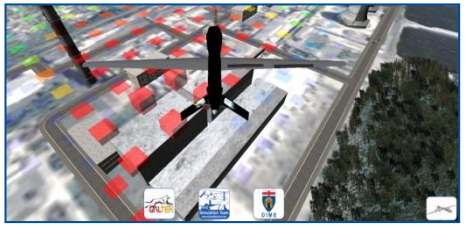
The innovative concept of *MS2G* (*Modeling, interoperable Simulation and Serious Games*) allows to develop interoperable scalable and reusable simulators with benefits of new Immersive Solutions. MS2G is very flexible and enable use from different platforms: regular laptops, computers, CAVE (Computer Automatic Virtual Environment) large enough to immerse 4-5 people in the Virtual World, HDM, HoloLens as well as Smartphones and Tablets





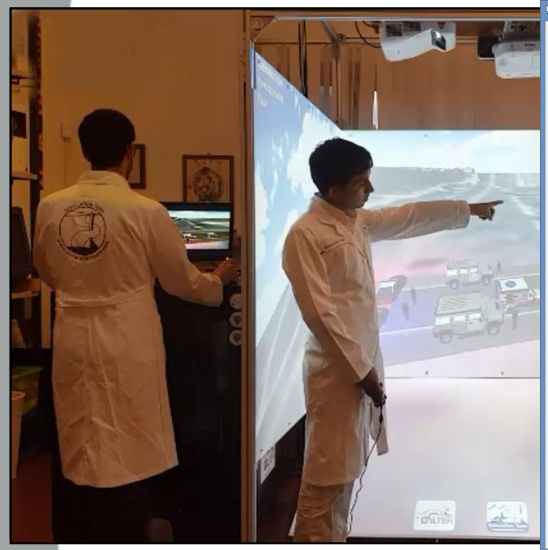


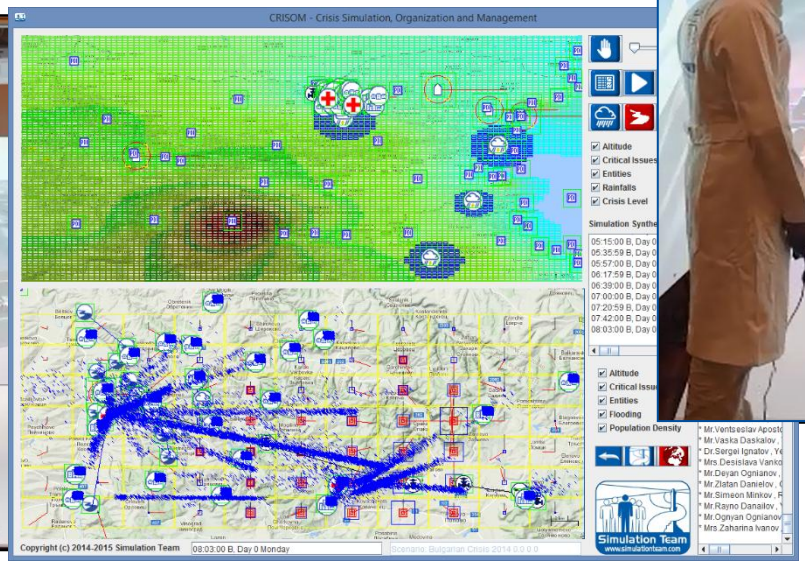
Simulation Team



MS2G and IA-CGF

The MS2G (Modeling, interoperable Simulation and Serious Games) could be combined with use of IA (Intelligent Agent such as IA-CGF by Simulation Team). The Intelligent Agents simulate concurrently many actors, people and actions enabling to recreate and study very complex scenarios to improve trainee engagement



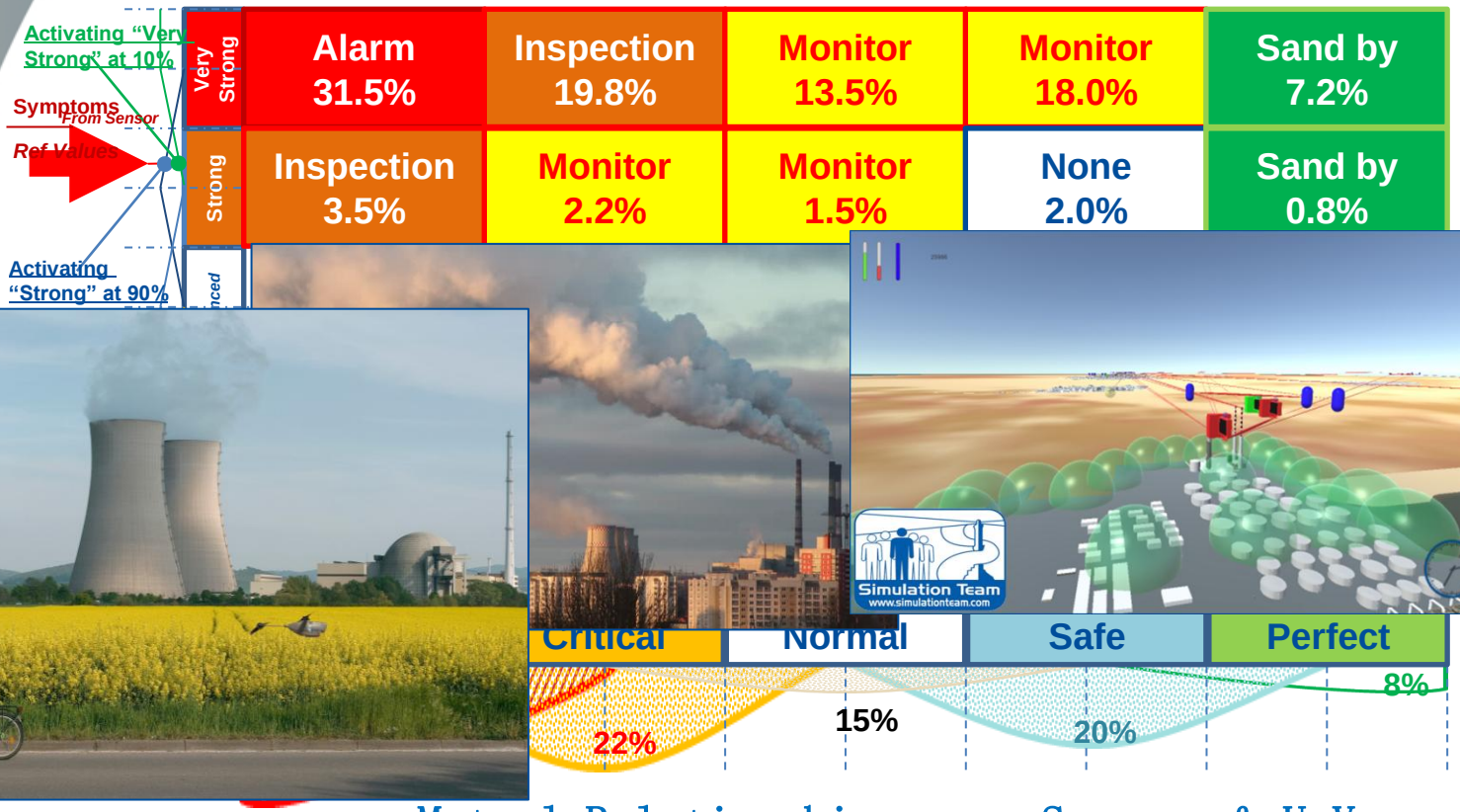


Simulation Team

AI… Artificial Intelligent for Awareness driven Initiatives

Danger	31.5%
Inspect	35.2%
Monitor	23.3%
Stand by	8.0%

General Situation on the Plant



Mutual Relationship among Sensors & UxV

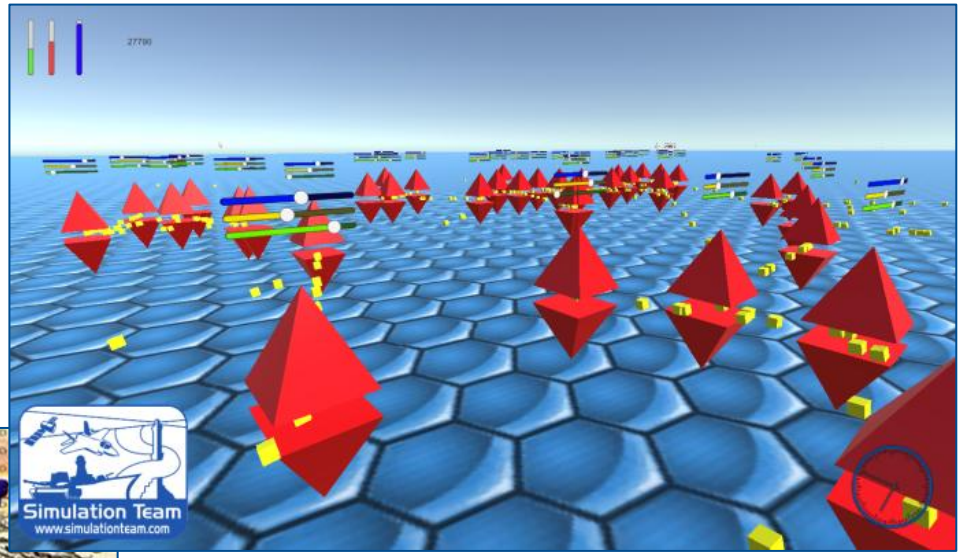
Simulation Team

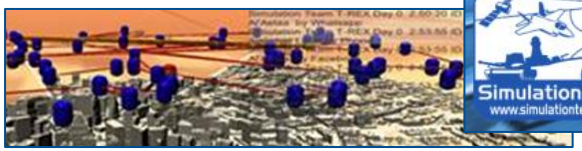
T-REX Cyber Layer

T-REX and IA-CGF (Intelligent Agents Computer Generated Forces) drive actions on the Cyber Layer where it is mapped the ICT domain and related levels of Confidentiality, Accessibility and Integrity for *each node and link*

Cyber Attack:
- Resources
- Responsiveness
- Efficiency
- Effectiveness
- Virus Dynamism
- Virus Initial Injection
- Virus Infectivity
- Virus Resilience
- Virus Level

Cyber Defense:
- Resources
- Responsiveness
- Efficiency
- Effectiveness
- Anti Virus Diffusion
- Anti Virus Resilience
- Anti Virus Level

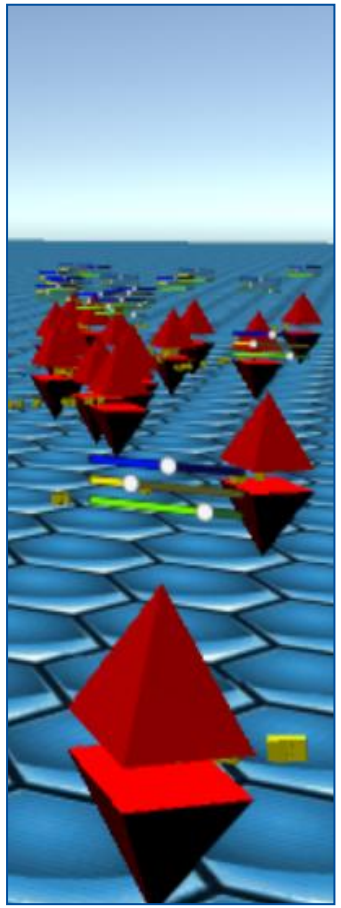




CIAP: Confidentiality, Integrity, Availability, Privacy

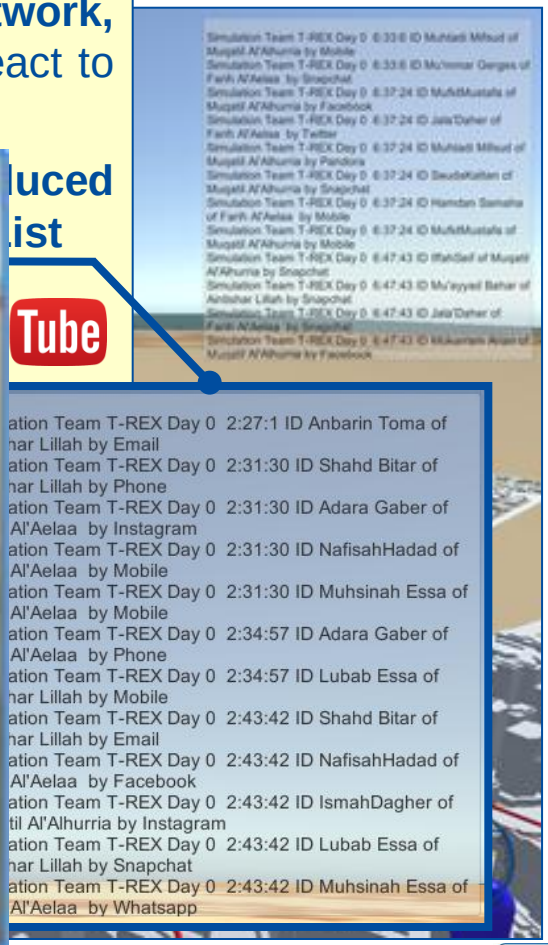
CIAP are concepts which have vast goals in Information Security:

- **Confidentiality:** Ensures that data or an information system is accessed by only an authorized person. User Id's and passwords, access control lists (ACL) and policy based security are some of the methods through which confidentiality is achieved
- **Integrity:** Assures that the data or information system can be trusted. Ensures that it is edited by only authorized persons and remains in its original state when at rest. Data encryption and hashing algorithms are key processes in providing integrity
- **Availability:** Data and information systems are available when required. Hardware maintenance, software patching/upgrading and network optimization ensures availability
- **Privacy:** Capability to capture private information to create new profiles and promote Identity Theft



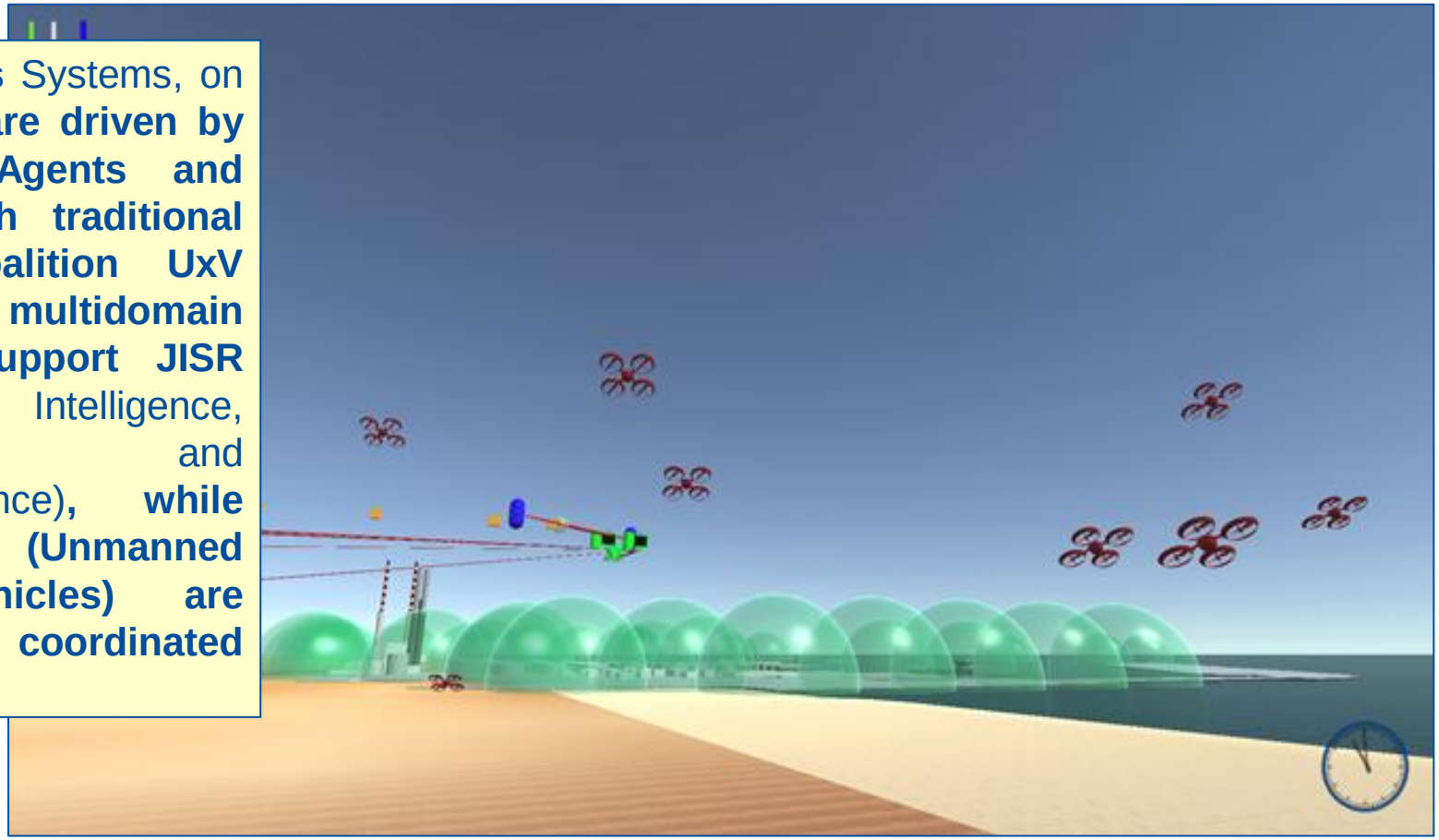
T-REX: Socials & Population

The Simulator reproduces the Social Network, Cyber Space and Population and how they react to their perception of the Scenario Evolution.



T-REX: Autonomous Systems

Autonomous Systems, on both sides, **are driven by Intelligent Agents and interact with traditional Assets. Coalition UxV (Umanned multidomain Vehicles) support JISR (**Joint Intelligence, Surveillance and Reconnaissance)**, while hostile UAV (Unmanned Aerial Vehicles) are conducting coordinated attacks**



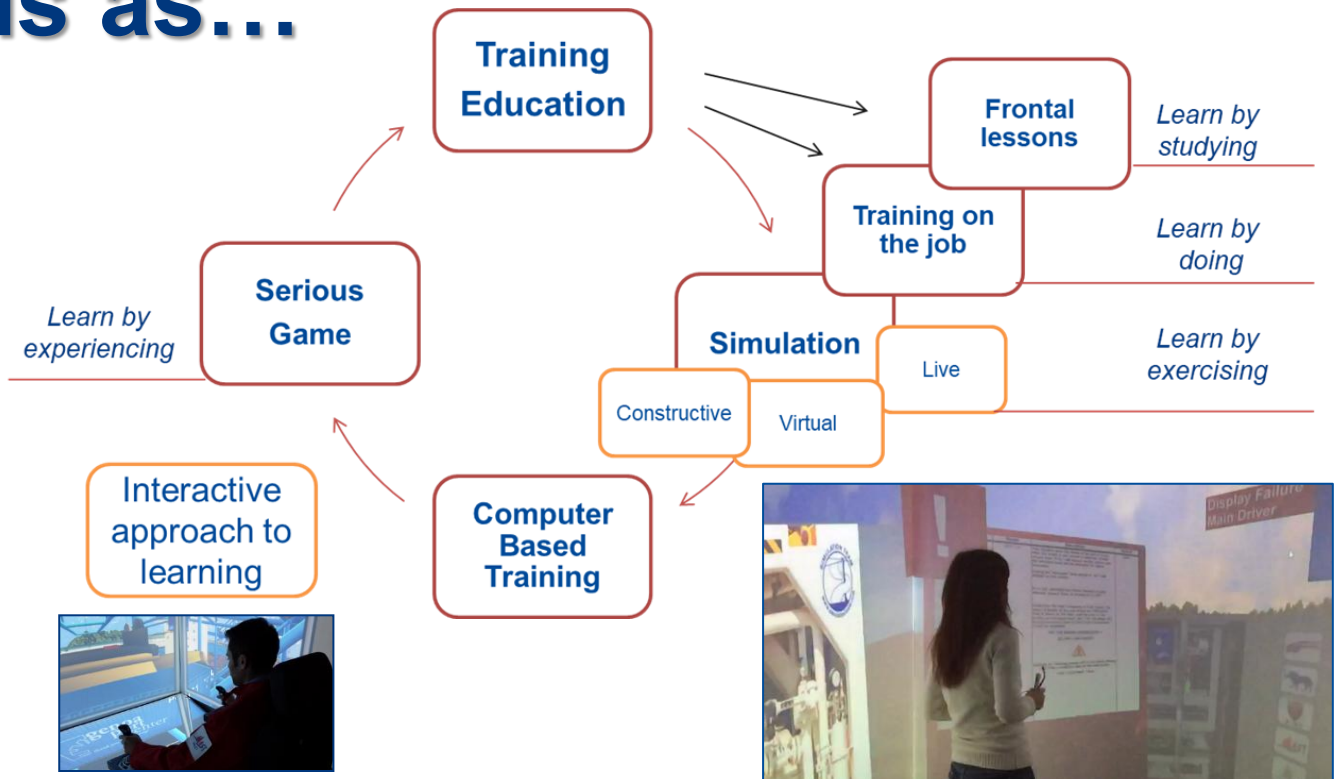
One Reason to adopt Models, Simulation & Serious Games?

- *Determining if Training is Needed*
- *Identifying Training Needs*
- *Identifying Goals and Objectives*
- *Developing learning activities*
- *Conducting the training*
- *Evaluating program effectiveness*
- *Improving the program*
- *Training must align with job tasks.*

Training Guidelines for Safety, OSHA

OSHA Occupational Safety and Health Administration, USA

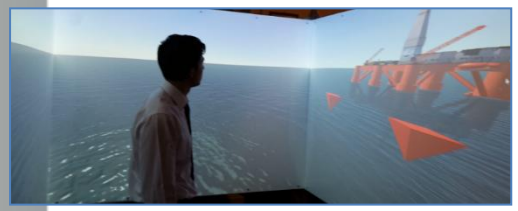
Cyber Security & Training Aids as…



"Tell me and I will forget. Teach me and I will remember. Involve me and I will learn", Confucius

Simulation Team

… Serious Games Evolve into Simulation Team Roadmap



Training on the Job

Simulation for Training

Experimenting on the Simulator

Serious Games for Training

Playing while Learning

Experimenting on Games

Many Installations
Many More Users

New Education Modes
New Utilization Modes

[Nuclear War]
..a strange game the only winning move is not to play
Joshua in War Games Movie

MMO Massively Multiplayer Online Game
MMORPG massively Multiplayer Online Role-play Game

Conclusions

- Cyber Security is a major issue dealing with crucial vulnerabilities addressing not only ICT Systems, but also on real systems such as: Buildings, Critical Infrastructures, Plants, Vehicles...
- The evolution of the technology forces to extend used of cyber physical systems increasing impact of Cyber Attacks and enhancing risks in terms of Human Safety.
- *Safety and Security* need to be addressed jointly to succeed against malicious forces and intrinsic complexity of the System of Systems
- *Modeling and Simulation* represent the key approach to complete Security and Safety Assessment and to support System of Systems Engineering as well as development o new solutions to improve Safety

Simulation Team

Simulation Team.. Who We Are?

Universities, Research Centers and Companies operating worldwide in synergy for developing Innovative Solutions with a particular focus in Modeling & Simulation

DIME
Università
di Genova

Liophant
Simulation

CentraLabs
Cagliari

CSU
Australia

Genova

CIREM
Università di Cagliari

Mik
Riga TU

Universidad
de la Rioja

DIPMEC

abria

Università di Perugia

SimCenter Universitat
Autonoma de Barcelona

LSIS
Marseille

SPIIRAS Russian
Academy of Science

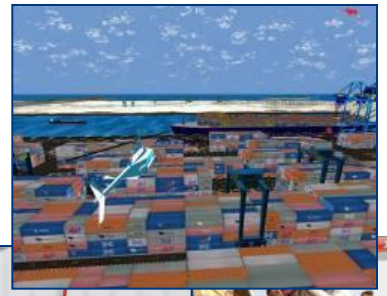
McLeod Institute of Technolo
Interoperable Modeling Simu
Genoa

IMS-LAPS
Univ.Bordeaux

Rio de Janeiro
Brazil

Simulation Team

References



Simulation Team, MITIM
DIME Genoa University
via Opera Pia 15
16145 Genova, Italy
www.itim.unige.it
Agostino G. BRUZZONE
agostino@itim.unige.it

DIME