



Information Security: Threats & Opportunities in a Safeguarding Perspective



Prof. Agostino G. Bruzzone



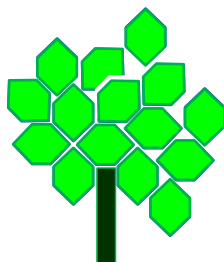
Università degli
Studi di Genova



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



www.liophant.org



World Engineering Forum



Information Security: Threats & Opportunities in a Safeguarding Perspective



Prof. Agostino G. Bruzzone



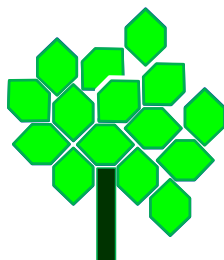
Università degli
Studi di Genova



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



www.liophant.org



World Engineering Forum





Cyber Attacks...?

Are Now!

November 29, 2017, 0607 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 motives motivated attacks on information and information systems.





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?

The Lawnmower Man
1992



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 ice itself. 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*



Live Free or Die Hard
2007



Changes around the World

- How it is Changing the Industry & World?
- How Simulation enables to face new Opportunities?
- Way Ahead, Challenges and Opportunities



← 2017! →

Vs.



Game

Black Hornet

Reality



Some Open Questions?

- How it is Changing the Industry & World?
- How Simulation enables to face Risks & Dangers?
- Way Ahead, Challenges and Opportunities
- To Perish is just a Game Option... or is it Real?**



← 2017! →

Vs.



Opportunities

Tianjin Explosion, August 12, 2015, 800 tons Ammonium Nitrate, 173 casualties, 2km range, 9bUSD In Damages

Threats

Some new way to... Perish!



- 1995 Mercedes from Munich to Denmark, 1600 km
- 1996 Parma University follow lane marks, 1900 km
- 1997 NAHSC, 20 vehicles in I7 San Diego
- 2004 DARPA, failure on running in the Desert
- 2005 Parkshuffle near Rotterdam
- 2007 DARPA, urban challenge won by Chevy CMU
- 2014 Vislab 20' in Rush Time →30M\$ by Ambarella
- 2016 Daimler AG smart parking in Stuttgart HQs
- 2016 Tesla first Casualty
- 2016 Nutonomy in Singapore, Self Taxi Service
- 2016 Uber testing in Pittsburgh
- 2017 Uber banned in London after Vancouver & Austin

18 millions of Taxi Drivers Worldwide



900'000 Truck Drivers just in Italy



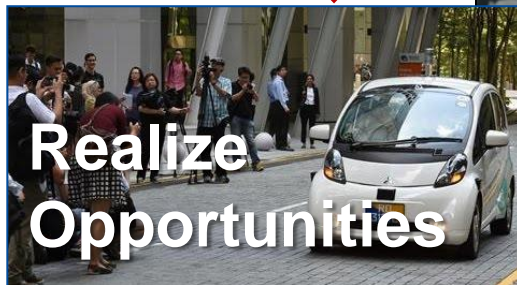
200'000 Uber Drivers Worldwide



CMU
DARPA
NAHS

Carnegie Mellon University
Defense Advanced research Projects Agency
National Automated Highway System Consortium

2015 Statistics





Cars... or People?

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



2005

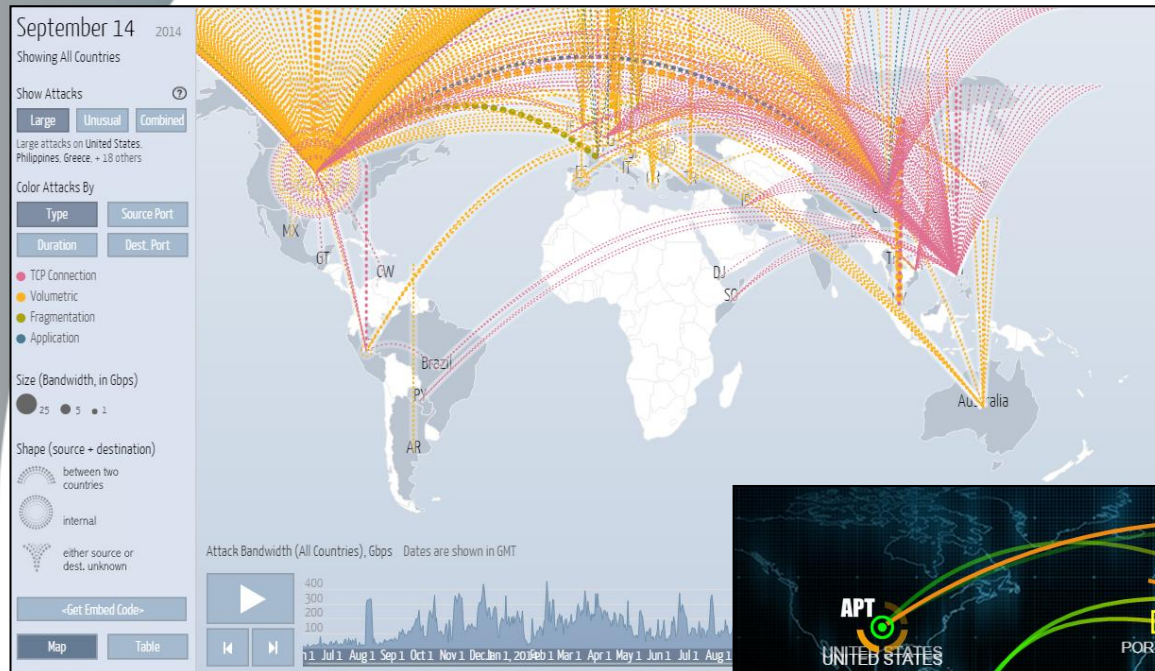


2015

Massimo Porro, Safe & Secure An unfolding story CISCO



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***





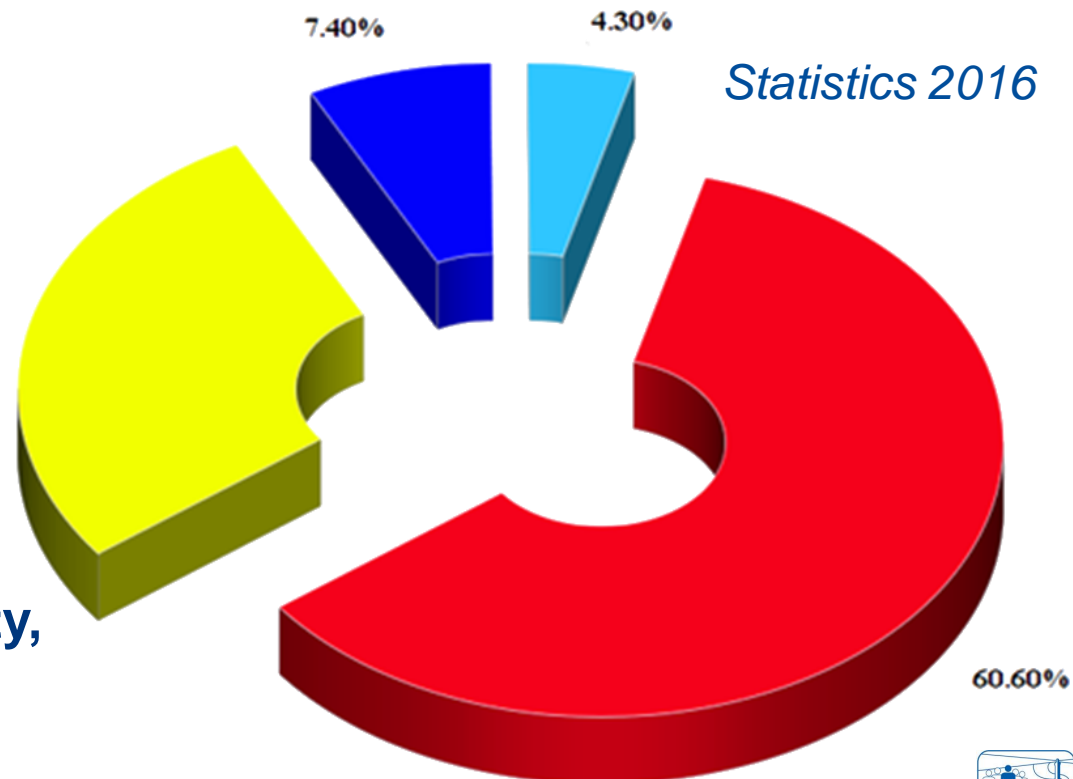
Cyber Attacks for What

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

- Cyber Crime
- Hacktivism
- Cyber Espionage
- Cyber Warfare





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... Ransomware



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 Gloal 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

```
Send me 100 Bitcoins and you will get my private key to decrypt any harddisk (except boot disks)
See the attached file signed with the key
https://mega.nz/#1YoLXWIwI1BpU1vMLLD_HiTWNg7ASihMRqs6RE8Z-6bXBMFWESXo
https://mega.nz/#1EWg3mSLL!ipiQ6cXA9GG1DPEjJWoWu5JWmMy48CxlAt270Gg1FHY
openssl dgst -sha256 -verify public.pem -signature public.sha256.dgst public.pem
Contact info https://kicnqmb5ggolftv6.onion/signup_user_complete/?id=1trno4d6hiripcmntp65re6ty
CA http://2shxd7xnyov2q375.onion/ca.crt
CA SHA1 fingerprint 7D:37:B2:79:38:3E:9B:0F:EE:DF:EB:D6:45:92:47:0A:05:0E:9E:B8
```

Eternal is attributed to NSA



Do you stuck your Password on the Fridge?

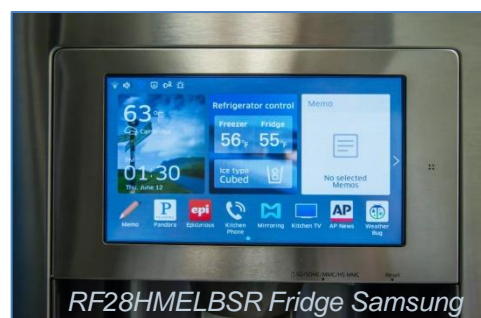


It is not necessary to attack your PC or Mobile...
new Kitchen Appliance provide new vulnerabilities:

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)





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

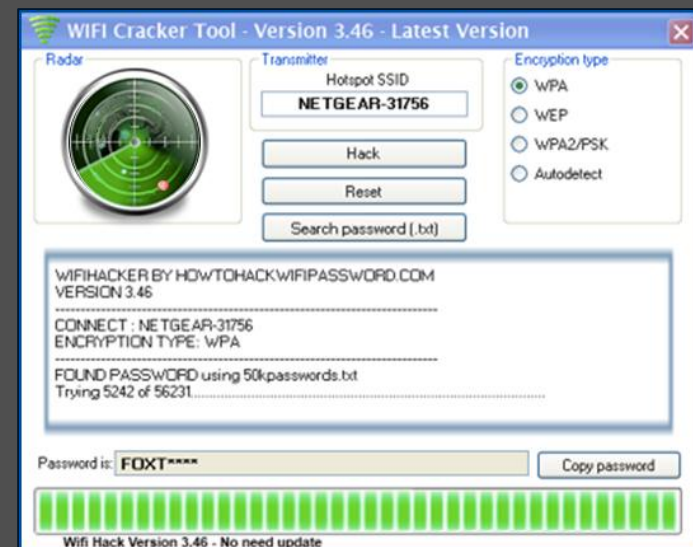
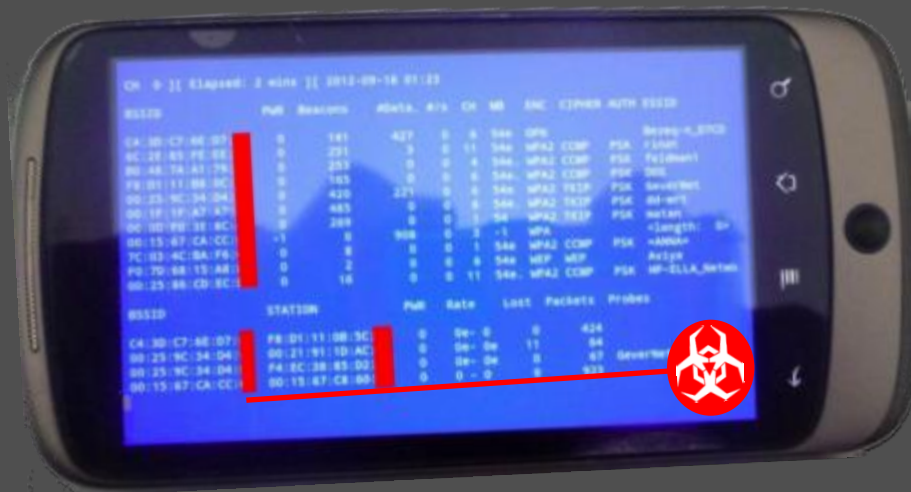
- SNMP (Simple Network Management Protocol) are often vulnerable to Spoofing
- PLCs (Programmable Logic Controller) allow hackers with modest skills to access them and take control of switchgear in absence of firewalls



... & WiFi: Lighting Vulnerable

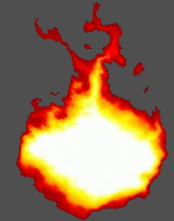


- WiFi technology is extensively used in Domotics for instance WiFi lighting systems use WPA2 encryption feature
- New generations of WiFi Crackers is usually successful in 99% in breaking these systems and give access to the control





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.

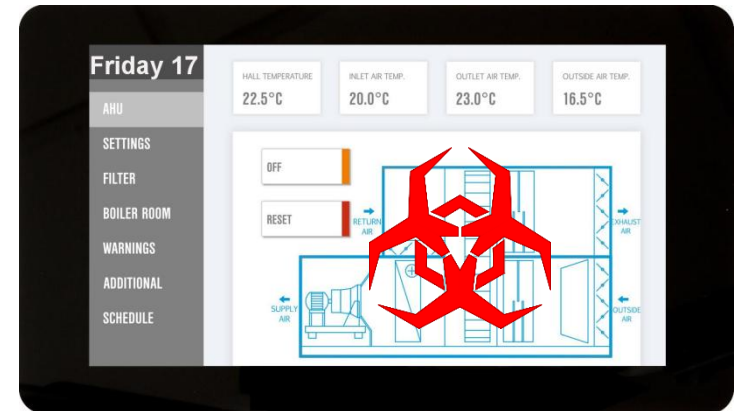
⦿ WannaCry, EternalBlue, Petya, etc. could affect these systems if not protected.





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**.



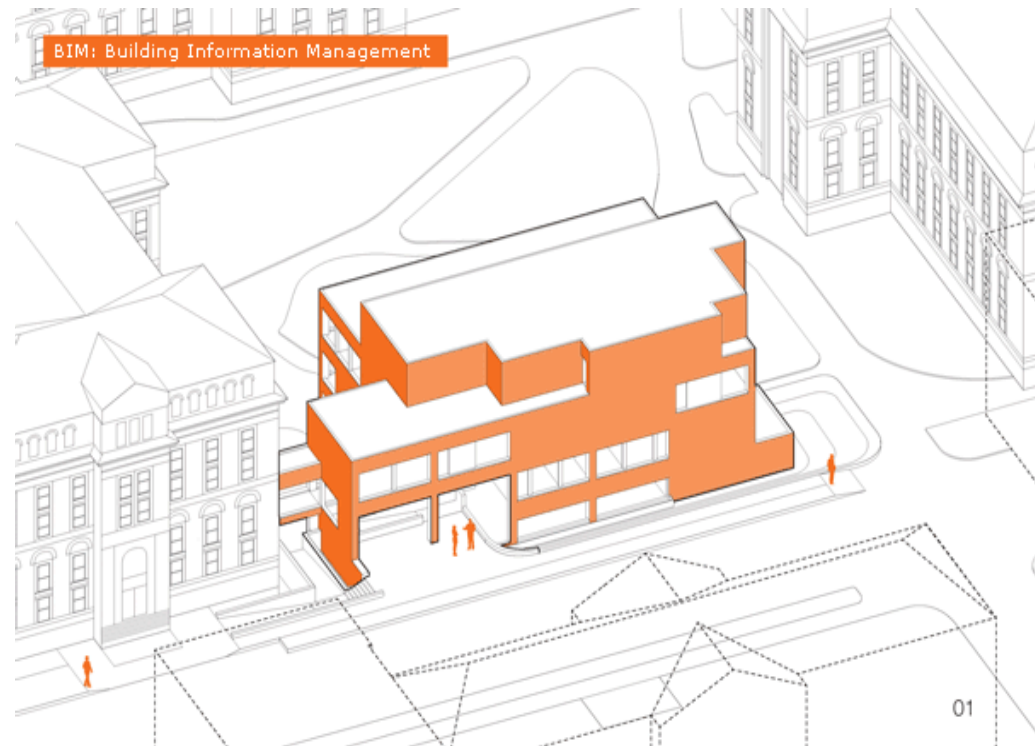


BIM: Building Information Modeling



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

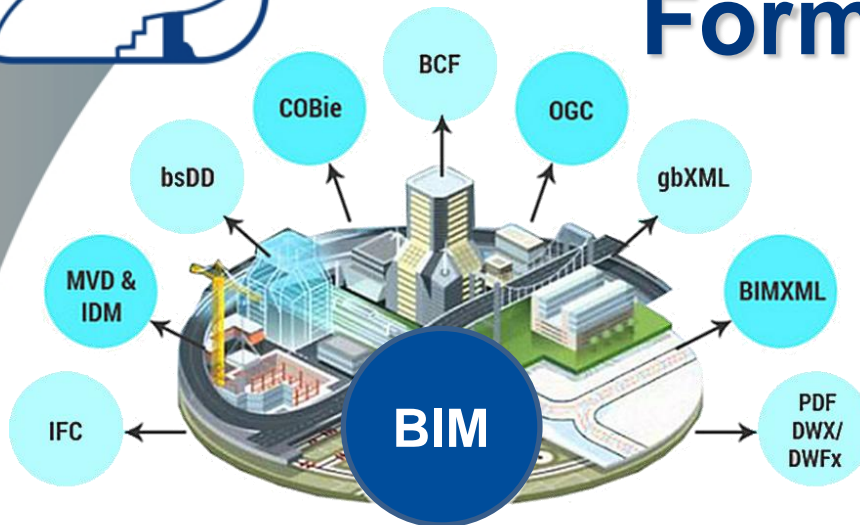
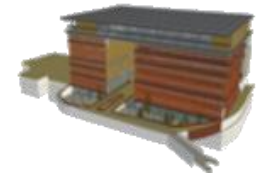
BIM is the process to generate and manage all digital representations of physical and functional characteristics of a Building. In the BIM there are many different files which can be extracted, exchanged or networked to support decision-making regarding the building or management of the Infrastructure.



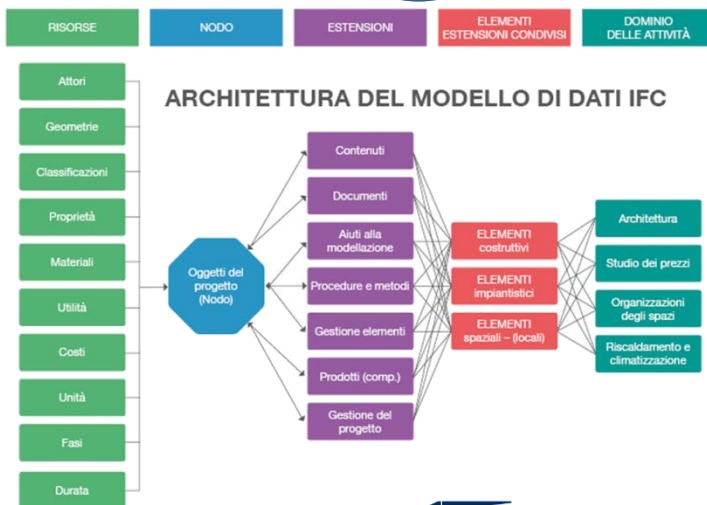
01



BIM & Interoperability Formats



- AIM Asset information Model
- BAS Building Automation System
- BIM Building Information Modeling
- BMS Building Management System
- CAFM Computer Aided Facility Management
- CMMS Computerized Maintenance 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 eXtensible Markup Language
- DWFx Design Web Format XML



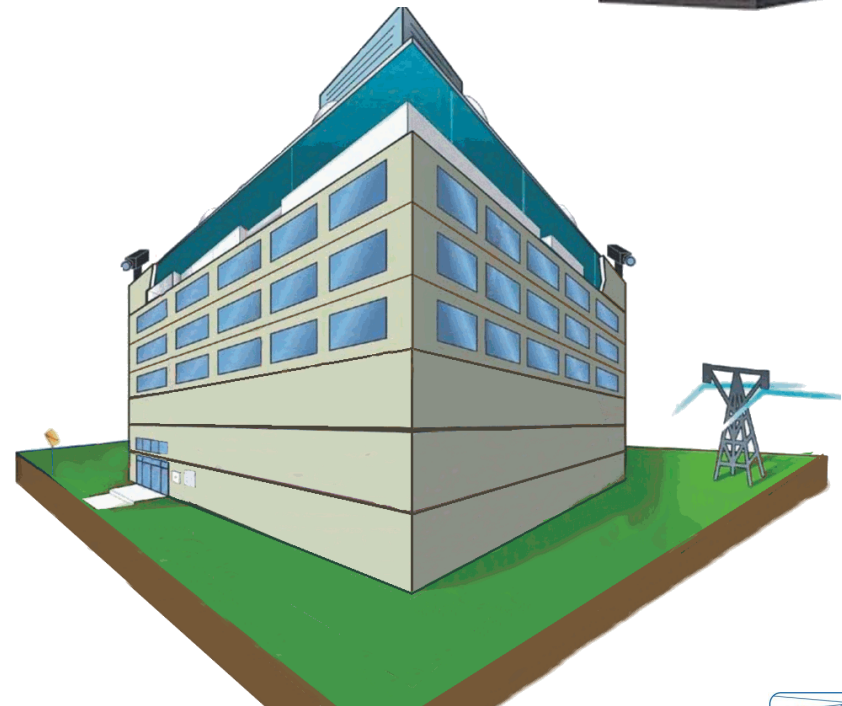


BMS: Building Management System

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





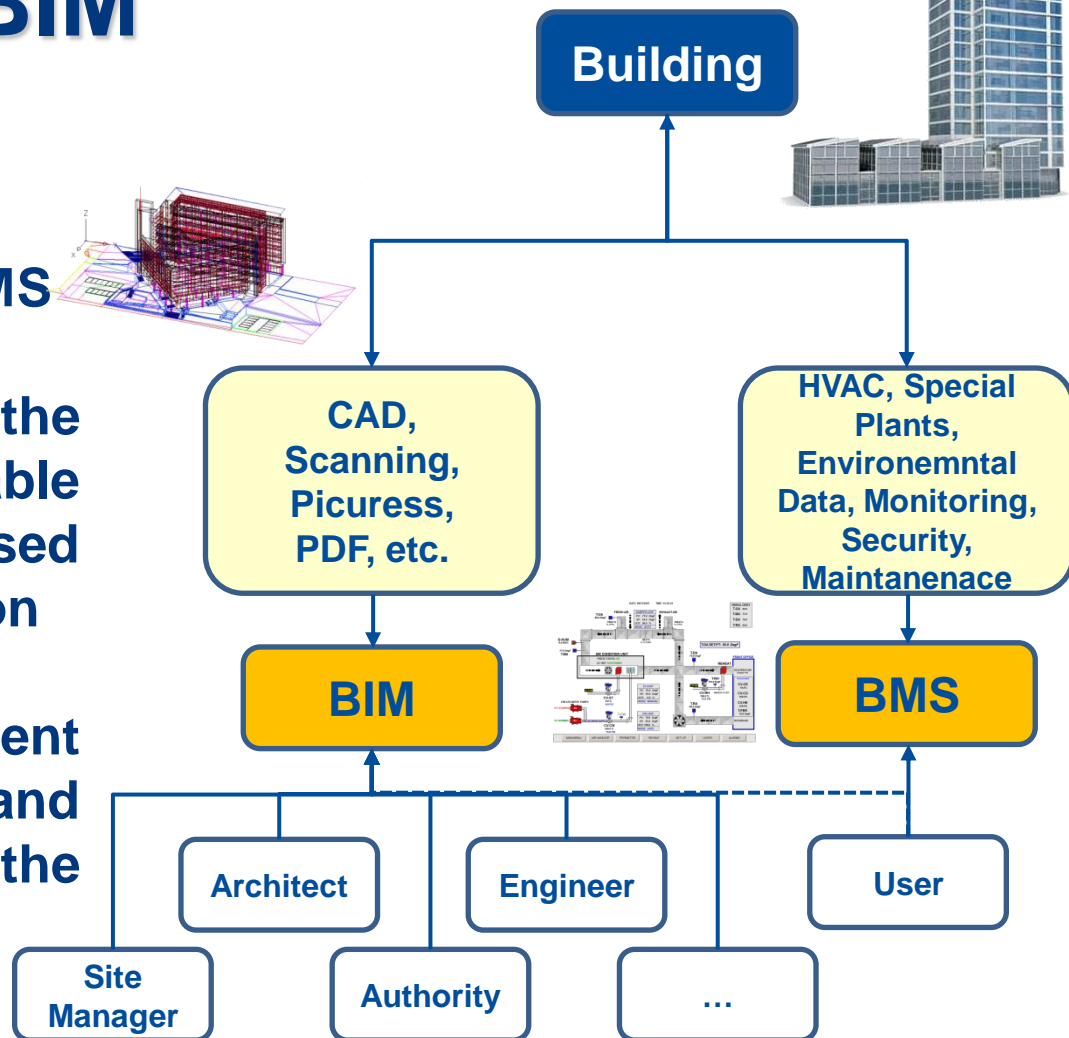
BMS & BIM

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 Savings & Comfort... but a New 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

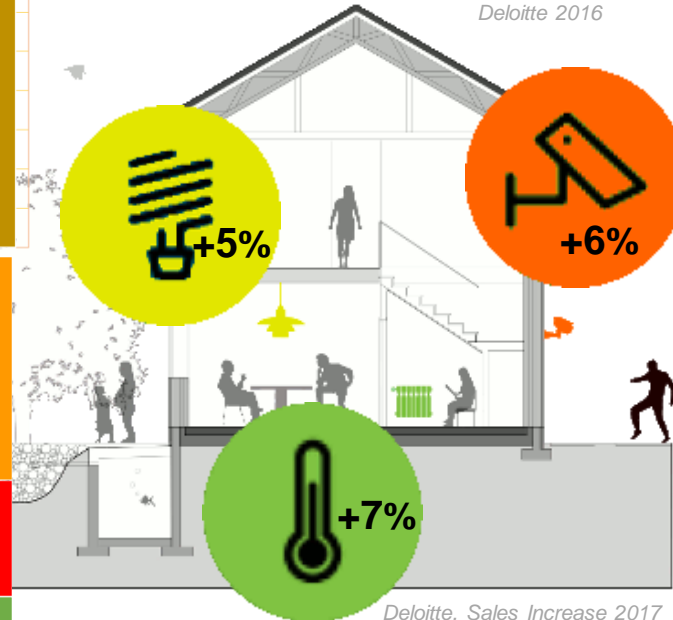
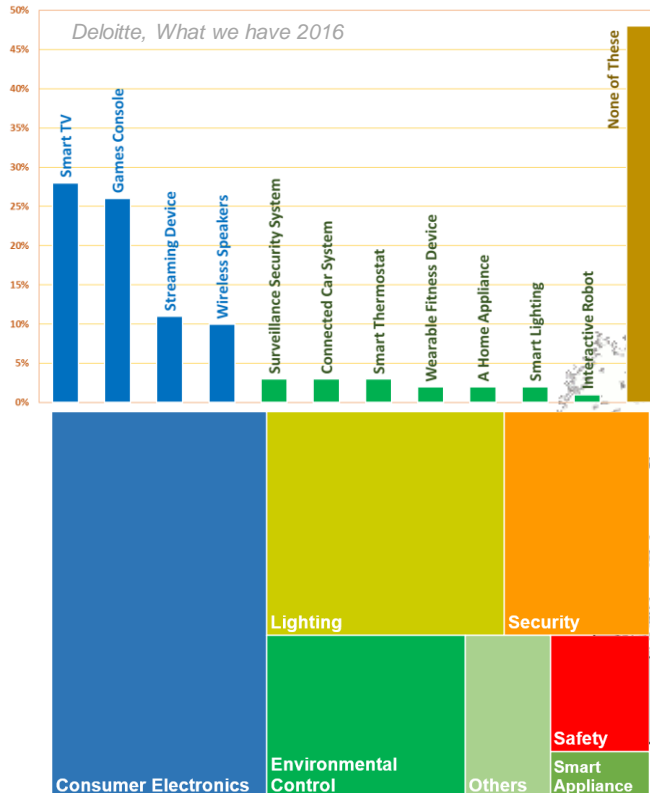
92% Installers say Home Automation is growing and works on:
81% IP CCTV
74% Alarms
72% Smart Locks
54% Electric Blinds
48% HVAC
47% AV

IFSEC Global Research

Barriers to Adoption

Price Barrier 48%
Technology Limits 26%

Deloitte, UK 2016



Deloitte, 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**

TOP COUNTRIES



United States	20,460
Canada	1,680
United Kingdom	948
Netherlands	873
Australia	734



TOP SERVICES

HTTP	20,917
HTTP (8080)	1,770
HTTP (81)	1,400
HTTPS	1,033
8081	382



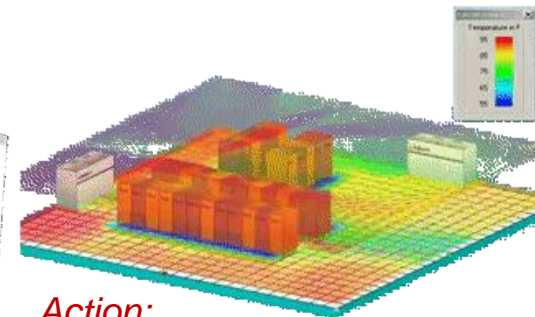


Cyber & Smart Buildings

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



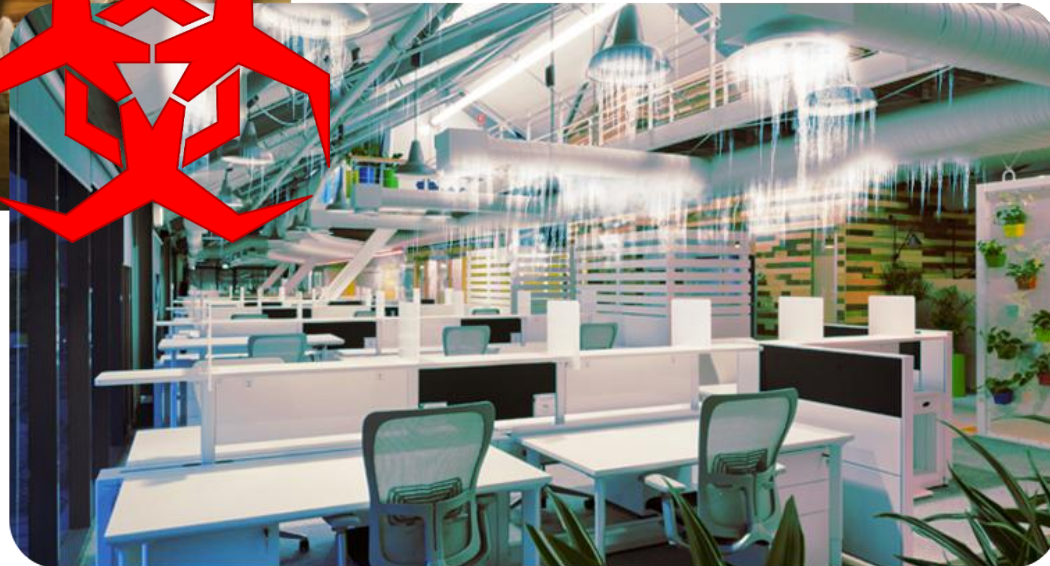
Action:
Overheating Data Farm Room
Shutting Down Key Servers



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



Traffic Jam... is it Real... ...or Cyber?

Two Students from Technion, the Israel Institute of Technology, proposed a Real Traffic Jam attacking phony Waze GPS Apps (Google owned) by creating a massive Fake Traffic jam by Fake Users forcing the system to reroute people within same area (2014)

Carmel Tunnels were blocked creating an Huge Block in Haifa Car Traffic by hacking Camera Systems that put the tunnel in lockdown mode (2013).

The Attacks were based on two phases:

● Traffic Block of 20' on "day 1"

● Traffic Block of 8 h on "day 2"



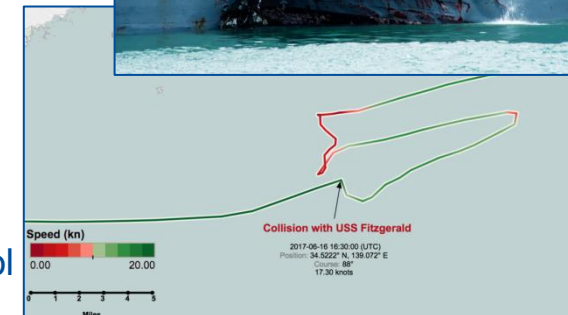


Just Data & Money? Safety?

University of Texas compromised
GPS of a 80MUSD Yacht by spoofing
using a 2k\$ device...



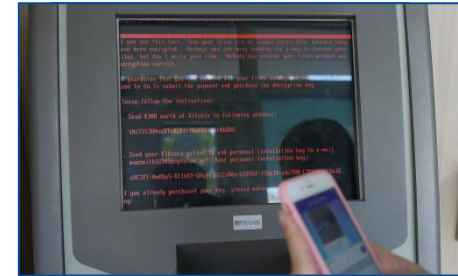
*Italian Coast
August 2013*







-  18/11/2017 **Aegis DD** USS Benfold vs. **Tugboat**
Sagami Bay: Minor Damages, Side Scratches
-  21/8/2017 **Aegis DD** USS John S. McCain vs. **MC Ship** 50000DWT
East of Singapore: 10 Casualties, 3 Injured, Severe Damage
-  17/6/2017 **Aegis DD** USS Fitzgerald / **MC Container Ship** 40000DWT
East of Singapore, 7 Casualties, 3 Injured People, 10 MUSD Damages
-  9/5/2017 **Aegis CG** USS Champlain / **South Korea Fish Boat** (20m)
Sea of Japan, No Injuries, light Damages
-  31/1/2017 **Aegis CG** USS Antietam, **Anchor Daggging, Prop.Out Control**
Tokio Bay, No Injuries, 4 m³ oil spill, **Propellers Damages**



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.
- 
Kyrgyzstan, 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
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



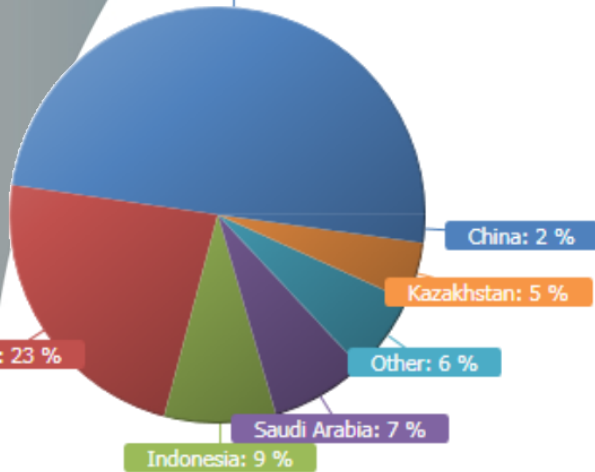
STUXNET 36 Months Later



Geographical distribution of Stuxnet infections 2013-2014.

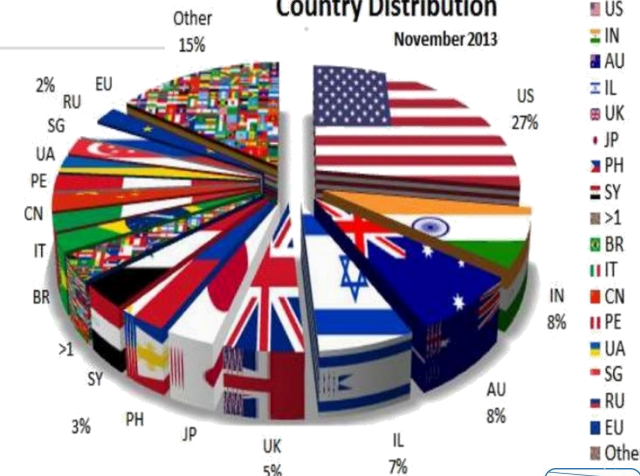
Discriminating Targets and adopting Deception and Sabotage on Hardware
Country Distribution

Iran, Islamic Republic of: 48 %



Country 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



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





Cyber & Safety in a Steel Mill!

Industrial Plants are plenty of Automation and extremely exposed to Cyber Attacks as much as turn to be distributed Systems (e.g. DCS, ICS, SCADA Systems)

It is not only about stealing data or strategic attack to nuclear facilities

A Steel Mill has been attacked in Germany with severe damages to the Plant, potentially with high risks for Human Safety

DCS Digital Control Systems
ICS Industrial Control Systems
SCADA Supervisory Control And Data Acquisition



BSI, December 2014 APT Attack to Steel Mill



Oil should keep going...

Unleaded	0.00	0/10
Plus	0.00	0/10
Super Unleaded	0.00	0/10

Simulation Team



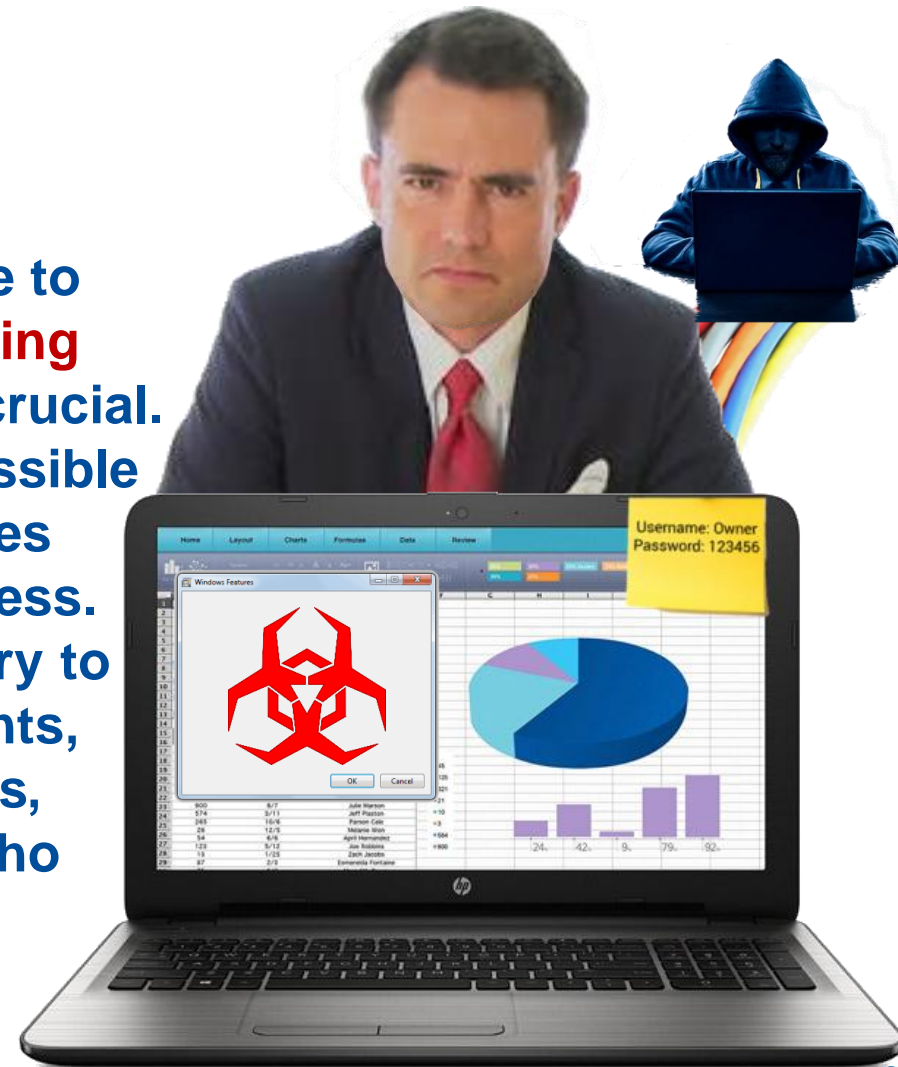
⦿ Middle 2012, Ramadam month, Aramco Saudi Offices: a click on a scam email injects a Virus... August 15, the Virus turn on:

- ⦿ 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 \$



Risks from Outside... and **Inside!**

BMS vulnerability is not only due to external attacks: **Social Engineering** and safeguarding from within are crucial. BMS are often multi-user web accessible. This provides additional functionalities and use but introduces cyber weakness. To secure the systems it is necessary to reengineer processes, 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.





Domotics as Backdoor?

There are many reports of hacking activities successfully compromising thousands of gadgets, for instance to launch malicious email attacks.

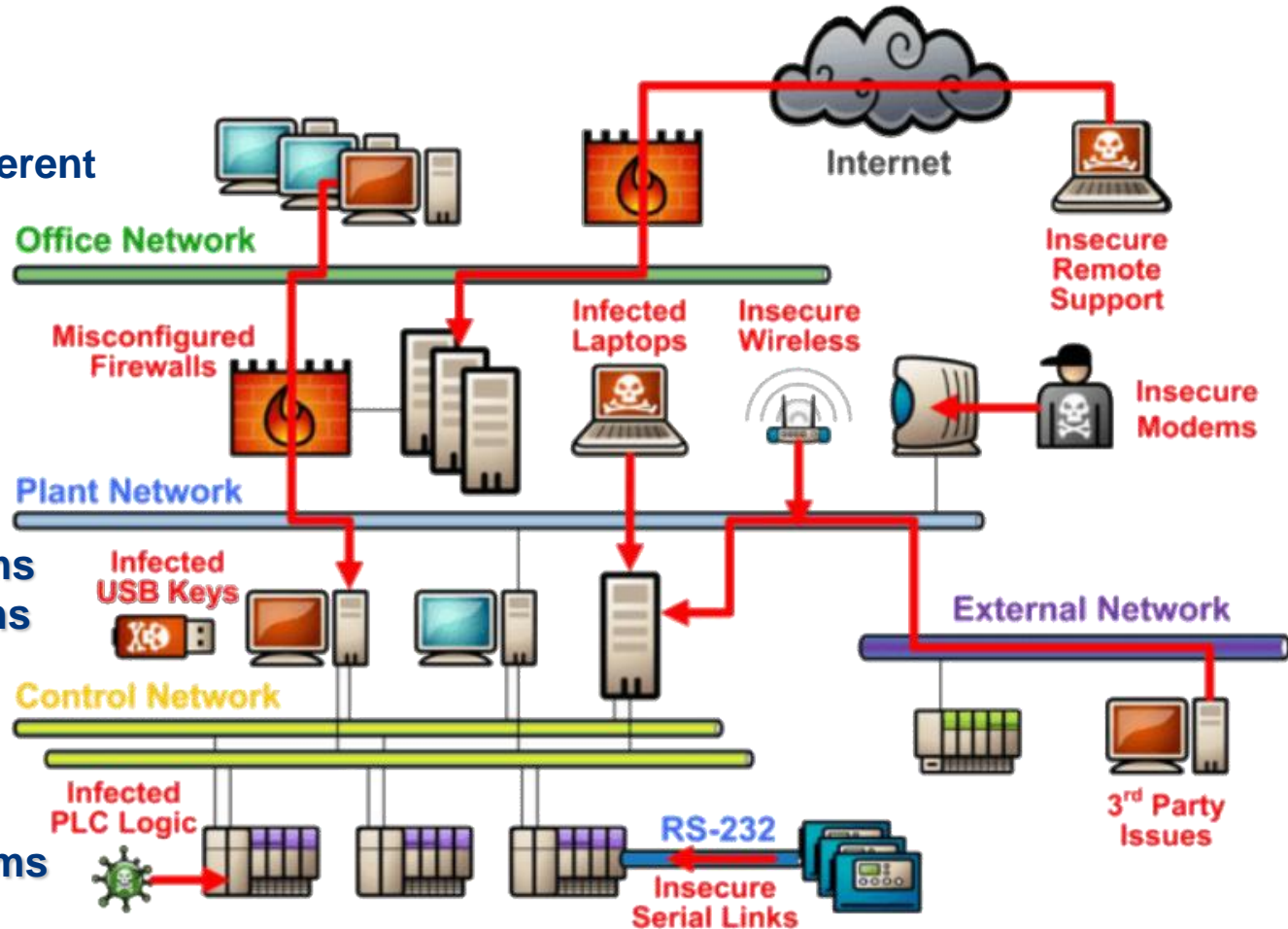
Today Surveillance Cameras, Smart TVs, Garages, Refrigerators and Thermostats are offering connectivity and represent example of IoT for Domotics, therefore most these devices are pretty vulnerable and not protected by anti-virus, nor adequately regularly monitored to update patches resulting as Back Door to entry in your Buildings, Plants and Homes





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



Watching Your Offices

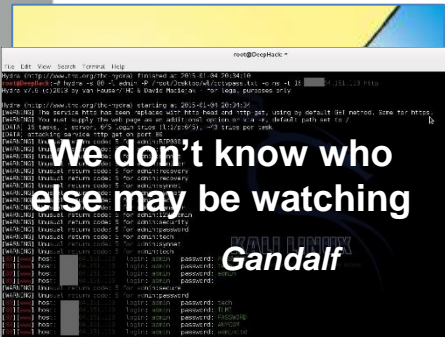
... and even more!



Watching Your Home

Since several years (Houston, 2013 & Cincinnati, 2014) there are

1. **Download** reports of baby monitor hacking. Hackers yelled at child in the
2. **Choose** middle of night: "Wake up!" plus obscenities. The monitor maker (le)
3. **Configure** claimed vulnerabilities were due to lacks in firmware updates, by
4. **Search** families, of devices dating over 6 months.
5. **Start IP Range Scanning** and access detected CCTV through Browser
6. **Use Default Usernames & Passwords** (e.g. admin, none, 12345, 9999)



We don't know who else may be watching

Gandalf

~~CONGRATULATIONS! 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)



Secured by Producer Smart Design

Smart Lamps **HACKED** by accessing through 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 downloads, cause 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 take control of other vulnerable systems on WiFi Network

SOS Message on the Lamps imposed by Hacking from UAV



HomeKit as a platform because HomeKit accessories communicate directly 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 crack, plus if attackers gain control of an iOS device he could just spread malware to this bluetooth standard energy light switch.

not as a platform because HomeKit accessories communicate directly 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 crack, plus if attackers gain control of an iOS device he could just spread malware to this bluetooth standard energy light switch.

AES Advanced Encryption Standard
DD Denial of Service
QR Quick Response Code
RSA Rivest-Shamir-Adleman
TLS Transport Layer Security





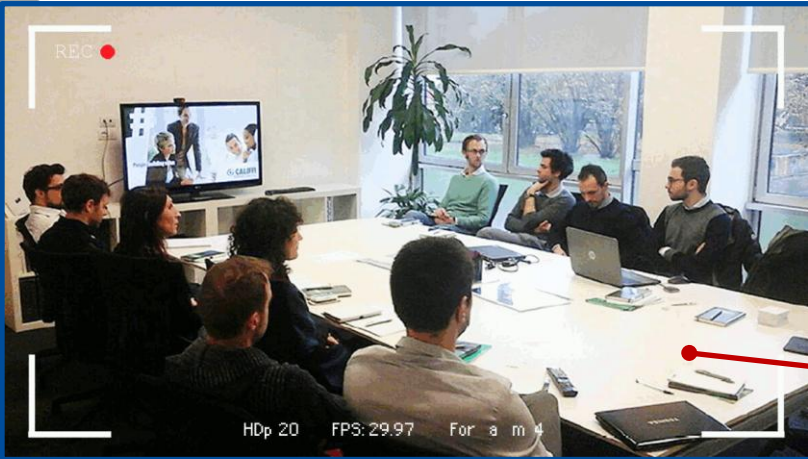
Thinking bad...



HVAC
overheating
Server
Room



Fake Alerts
on Speaker
& Panels
create Panic



Fire Control
& BMS
blinded
during Fire



Intrusion via
BMS In
Company
Tlc System



Seeing through Walls

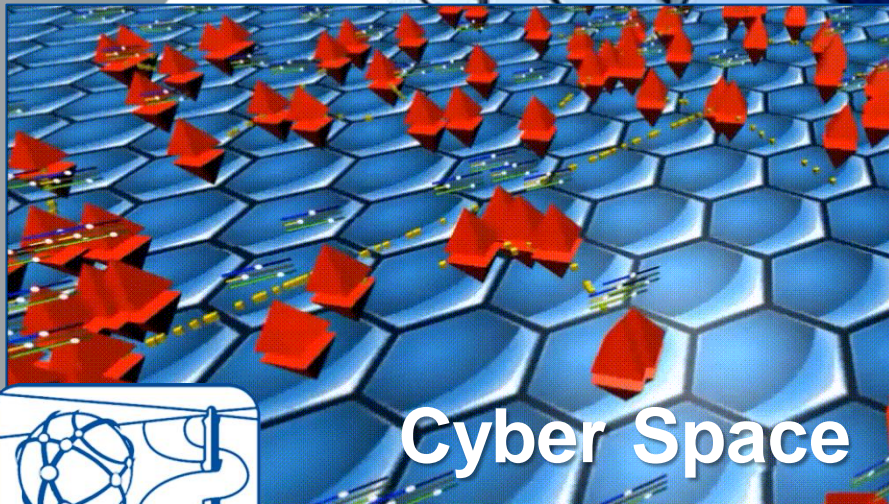
**Buildings & Plants
are plenty of devices
that live concurrently
in Physical World
and Cyber Space**



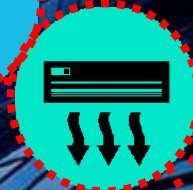


...Prevention by Simulation

Simulation of Cyber Space is fundamental to Improve Security



Cyber Space



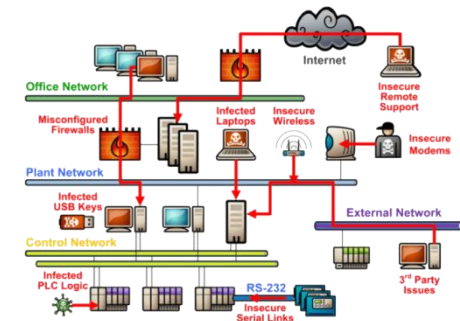


Improving Security of BMS

Password Mngt.

Network 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.

Vulnerability	Reason	Best Practice
Web interface	SQL injection	Install firewall
USB port		Disable Auto-Run

Vulnerability	Reason	Best Practice
Default credentials	Available in online databases	Change before
Simple passwords	Easily cracked	10- to multi-passw
Demonstration systems	Hard-coded credentials	Change before

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.





You don't need to Blow a Bomb... just a Fake New



- 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



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,...



Virtual Assistants based on ICT & IoT





Computers are more efficient than human beings, not better

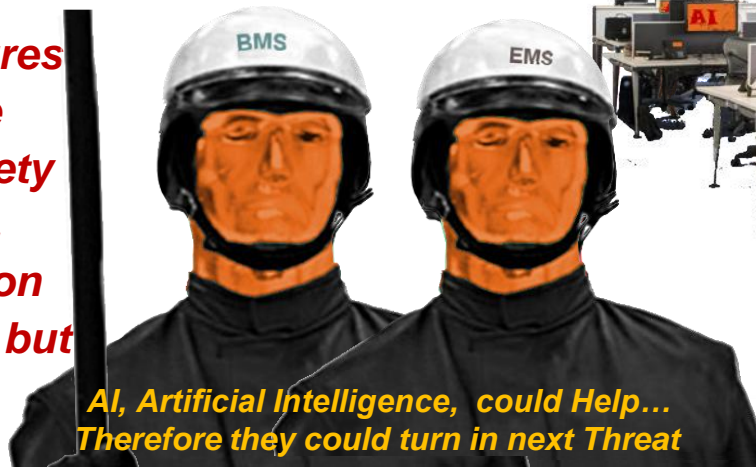
Spock, Ultimate Computer

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



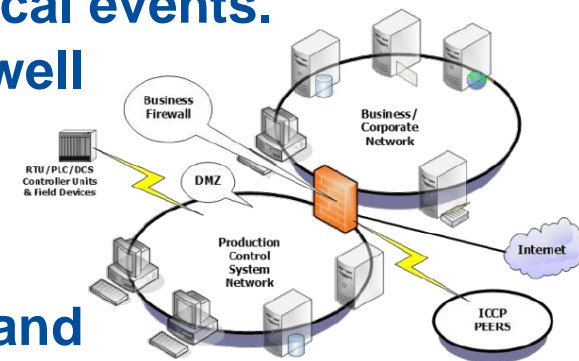
AI, Artificial Intelligence, could Help... Therefore they could turn in next Threat





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



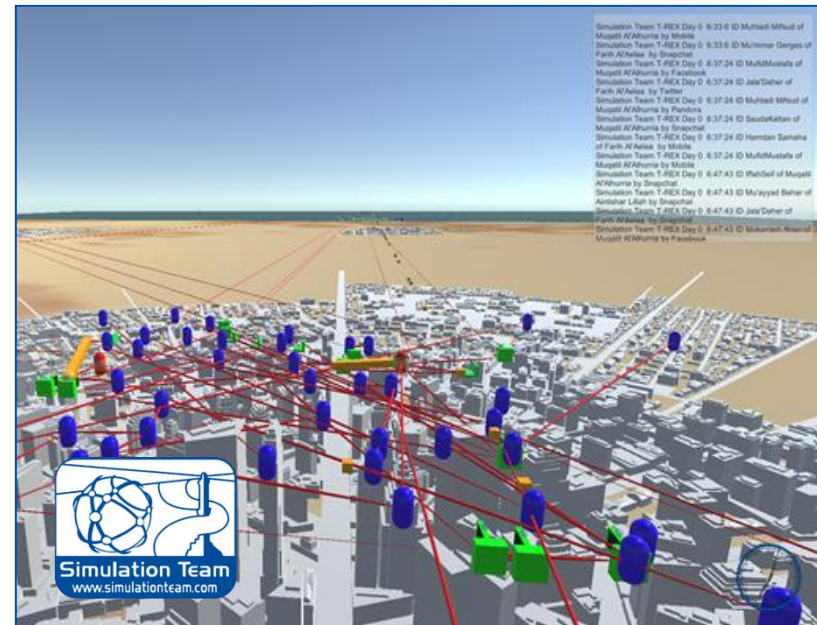
De Docta Ignorantia... Periculi et Ingenio Simulatoris

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

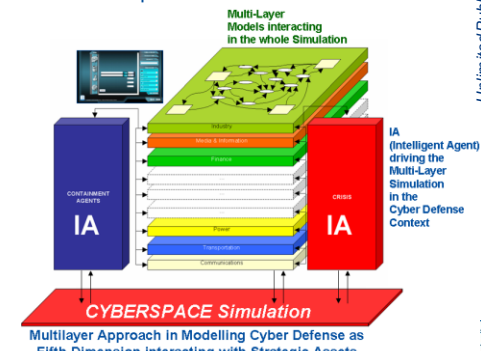
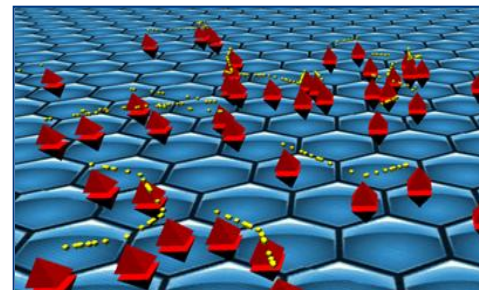
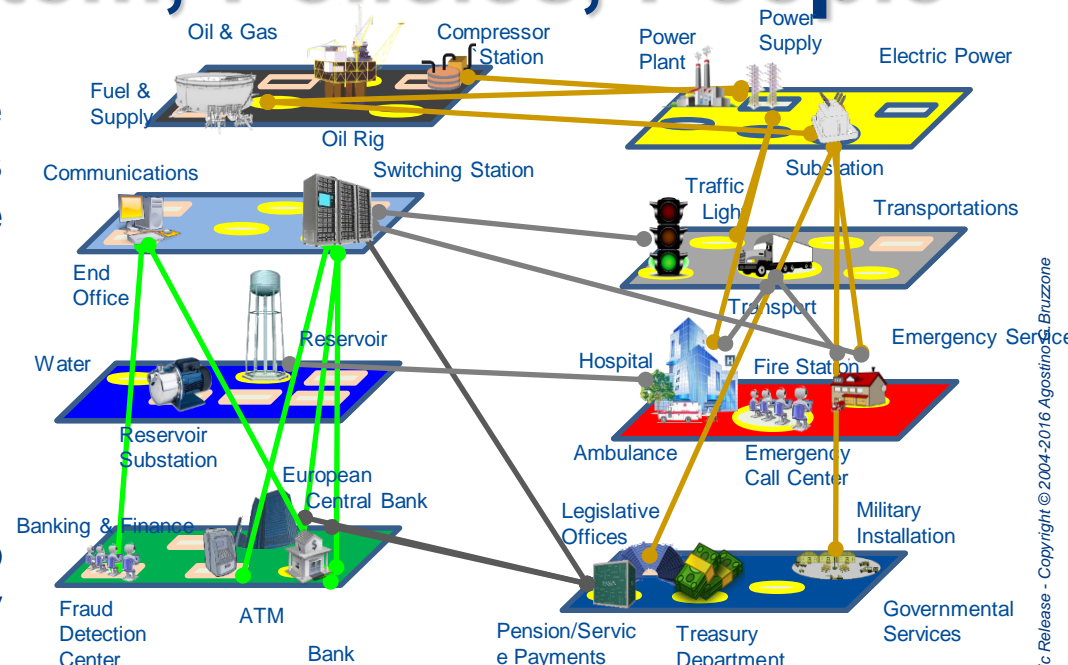


Multi-Layer Simulation for New System, Policies, People

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

- New System Design
- 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 Players

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



Unlimited Public Release - Copyright © 2004-2016 Agostino Bruzzone





Interoperable Virtual Simulators & Models



The Smart Simulators represent the crucial element to support advance and revolution in Engineering, Management and Training. 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.



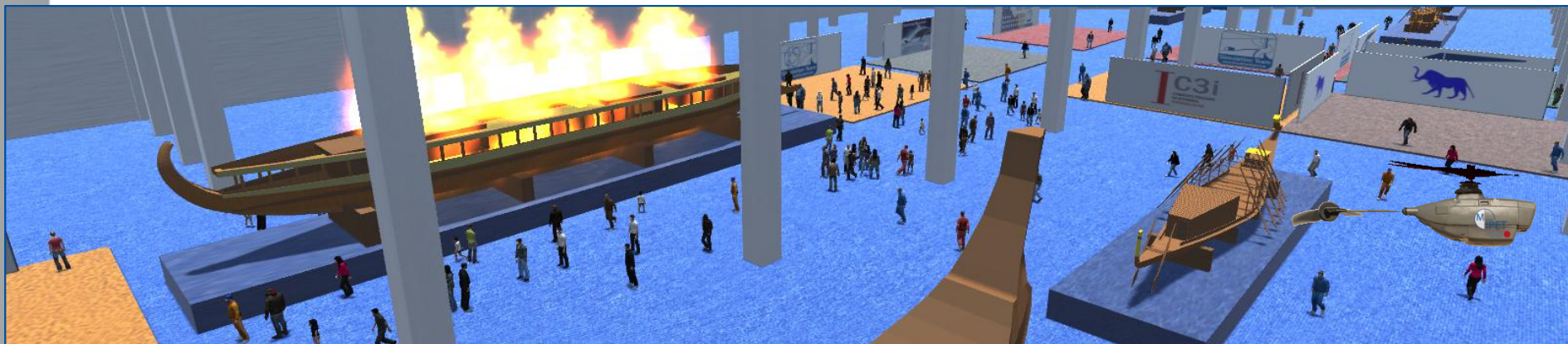
Simulation Team have very long experience in Project with major Industries and leading International Agencies and Institutions



Multi-Layer Engineering Approach at Work: the Blue

Blue Exhibition Hall is the latest infrastructures at the major Italian Boat & Yacht Show: up to 350'000 visitors, indoor and at sea exhibitions

Multi-Layer Engineering Approach is applied by **Simulation** respect **Ancient Ships: a Humankind's Heritage** Exhibit





Fire Safety Engineering... Cyber Security... Drones & *much more!*




Human Behavior



Cyber & Physical Actions



Fire Safety Engineering

Simulating: **Joint Threats, WiFi & Speakers** hacking, **Fake News**, attracting People in most critical area, **Blocking Doors** by **Cyber**, using **Drones** to disable , igniting **Fire**, using **Trucks** to **block Exits** and to create **Panic**



Fire Safety Engineering... Cyber Security... Drones & *much more!*



Blocking Doors by Trucks



Cyber & Physical Actions



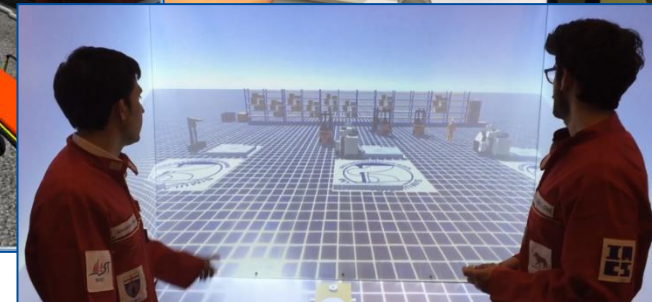
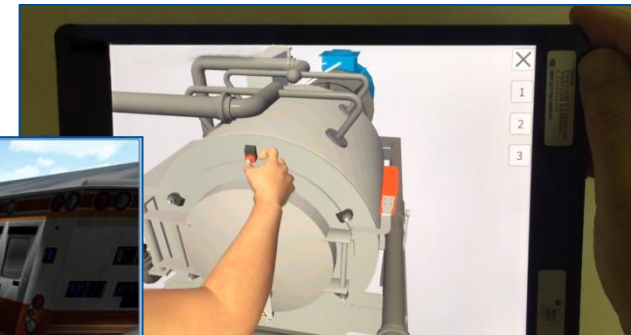
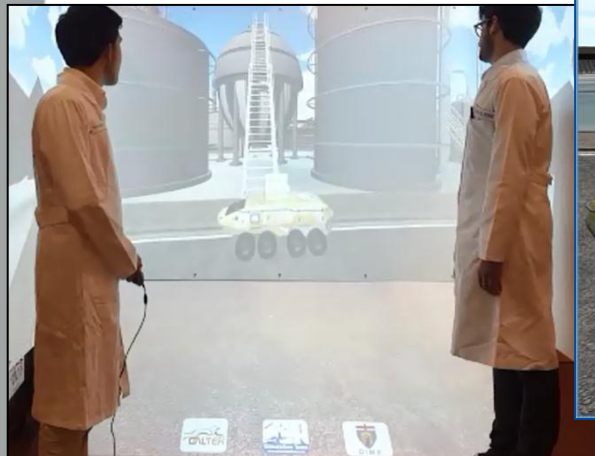
Fire Safety Engineering

Simulating: Joint Threats, WiFi & Speakers hacking, Fake News, attracting People in most critical area, Blocking Doors by Cyber, using Drones to disable Fans, igniting Fire, using Trucks to block Exits and to create Panic



MS2G Paradigm as new Enabler

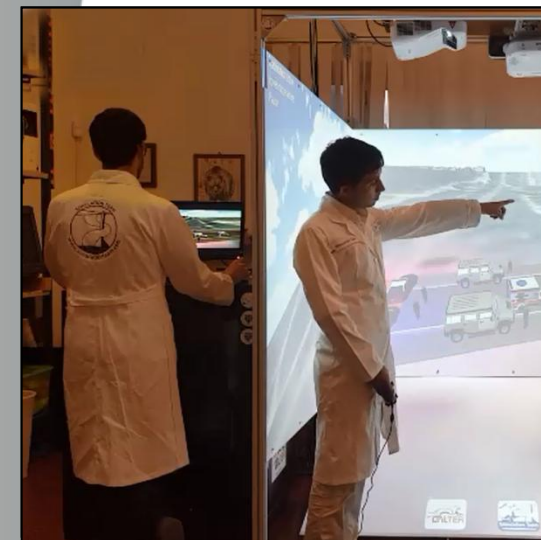
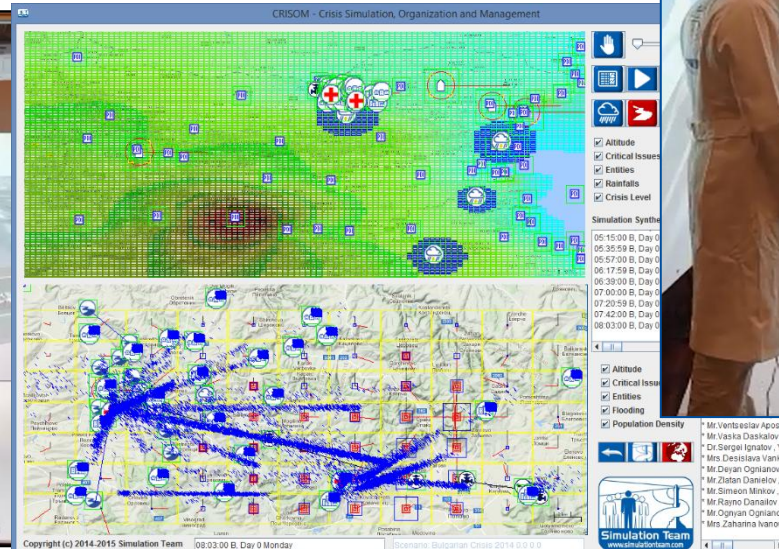
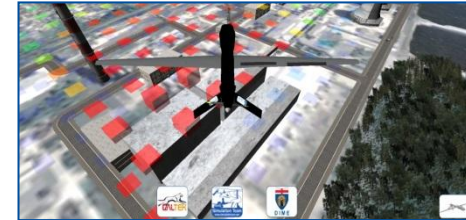
The innovative concept of MS2G (Modeling, interoperable Simulation and Serious Games) allows to develop interoperable scalable and reusable simulators with benefits of new Immersive Solutions. MS2G is very flexible and enable use from different platforms: regular laptops, computers, CAVE (Computer Automatic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



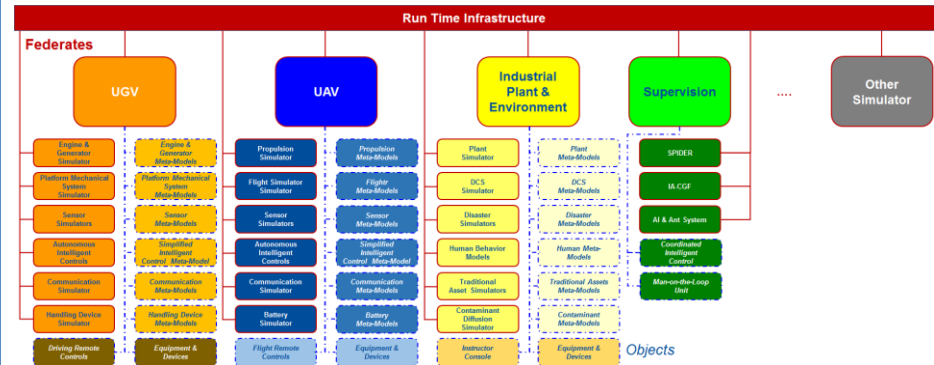


MS2G and IA-CGF

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



UxV & Plants...



UxV Unmanned any domain Vehicle

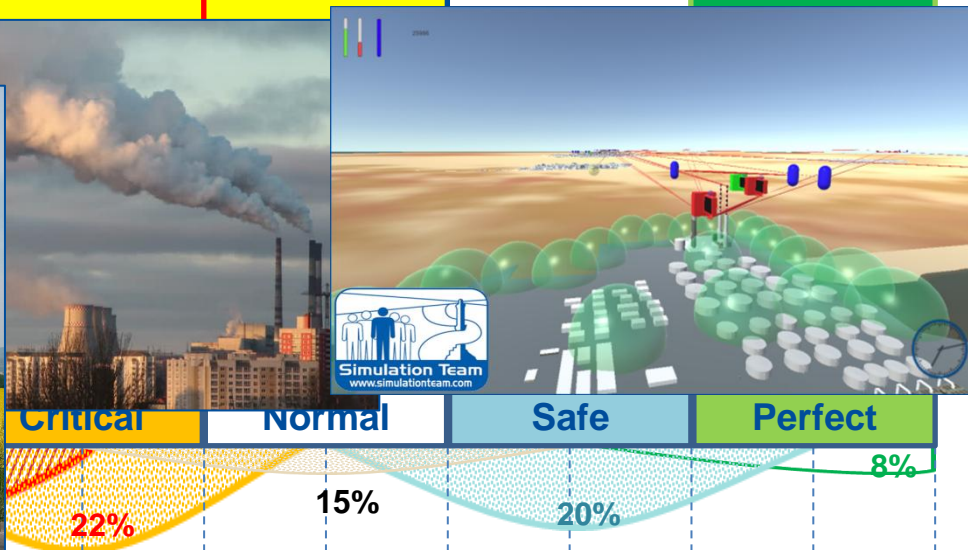
AI... Artificial Intelligent for Awareness driven Initiatives



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

General Situation on the Plant

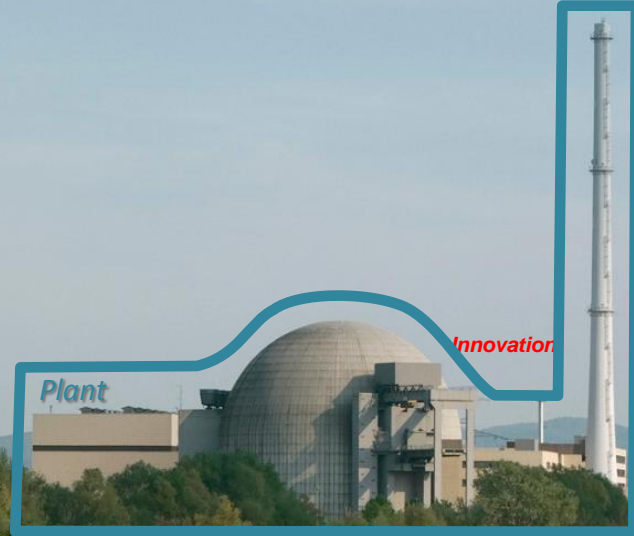
Activating "Very Strong" at 10% Symptoms From Sensor Ref Values Activating "Strong" at 90%	Very Strong	Alarm 31.5%	Inspection 19.8%	Monitor 13.5%	Monitor 18.0%	Sand by 7.2%
	Strong	Inspection 3.5%	Monitor 2.2%	Monitor 1.5%	None 2.0%	Sand by 0.8%



Mutual Relationship among Sensors & UxV



Emissions



Plant

Innovation



Sustainability



People



Environment



Drone

New Engineering

Market Evolution

New Regulations





Sustainability

New Threats

New Technologies

Innovation

Market Evolution

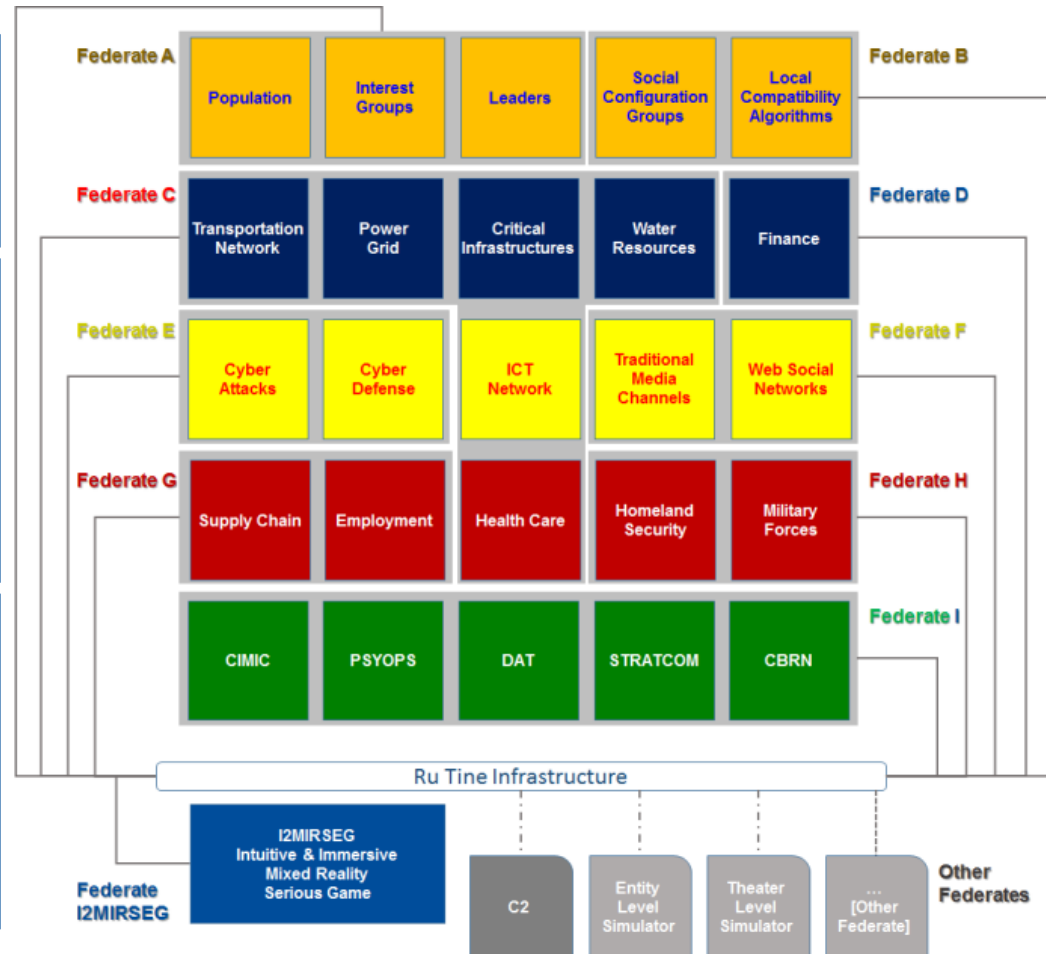
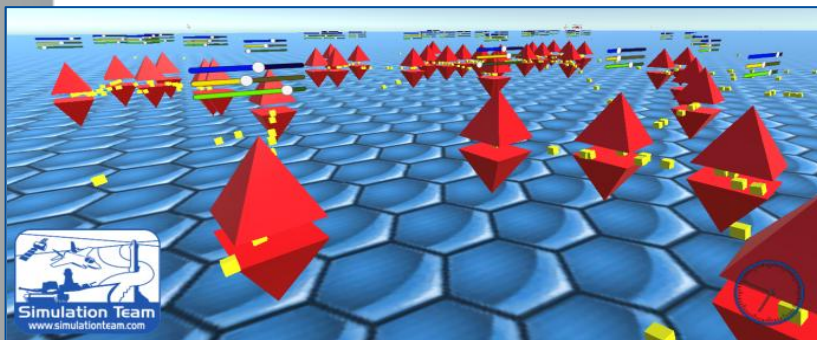
New Regulations

We need Smart Simulation in Engineering ...because things are Changing!



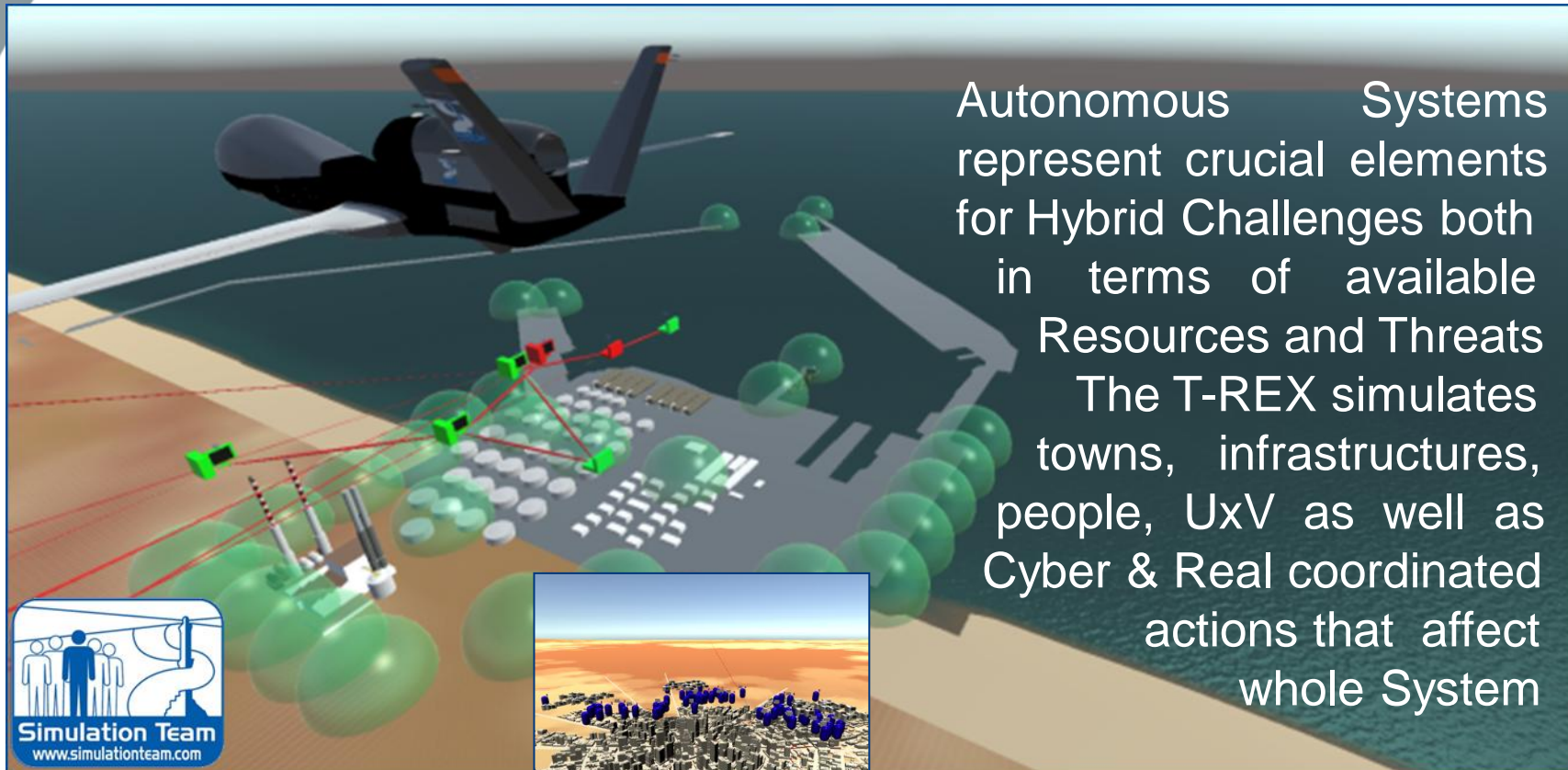
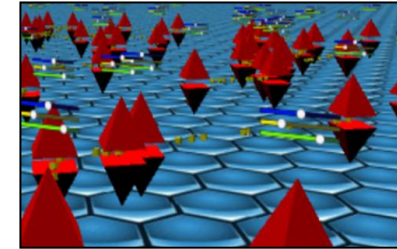


Creating Comprehensive Environments

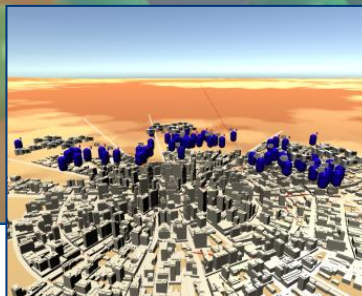




Hybrid Challenges & Autonomous Systems



Autonomous Systems represent crucial elements for Hybrid Challenges both in terms of available Resources and Threats. The T-REX simulates towns, infrastructures, people, UxV as well as Cyber & Real coordinated actions that affect whole System.





T-REX

Threat network simulation for REactive eXperience

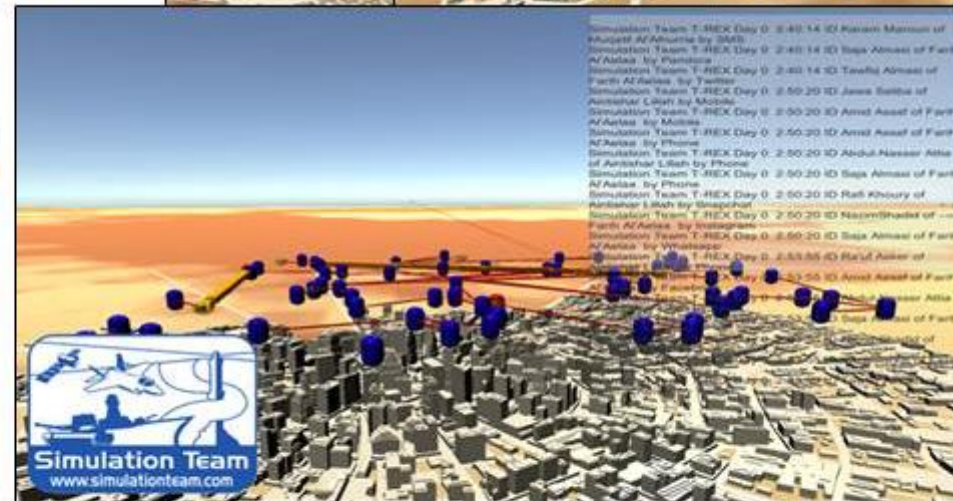
Simulation Team



T-Rex (Threat network simulation for REactive eXperience) is a MS2G (Modeling, interoperable Simulation & Serious Game) devoted to reproduce Hybrid Warfare and to be federated with other elements to evaluate the impact of these actions.

T-REX reproduces urban, as well as extra urban contexts over multiple domains including land, air, sea, space and cyberspace. The models allows to consider media communications and

possibility to use different assets and to experiment virtually the different decisions in terms of COAs (Courses of Actions)





T-REX Cyber Layer



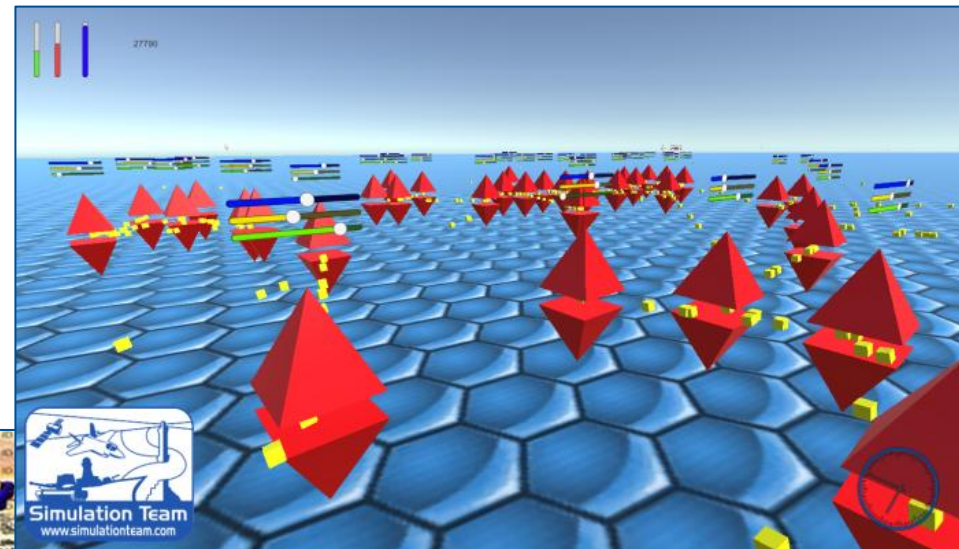
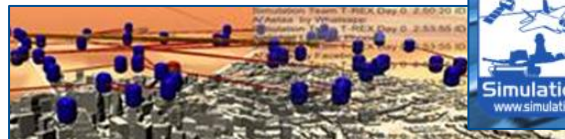
-  T-REX and IA-CGF (Intelligent Agents Computer Generated Forces) drive actions on the Cyber Layer where it is mapped the ICT domain and related levels of **Confidentiality**, **Accessibility** and **Integrity** for *each node and link*

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

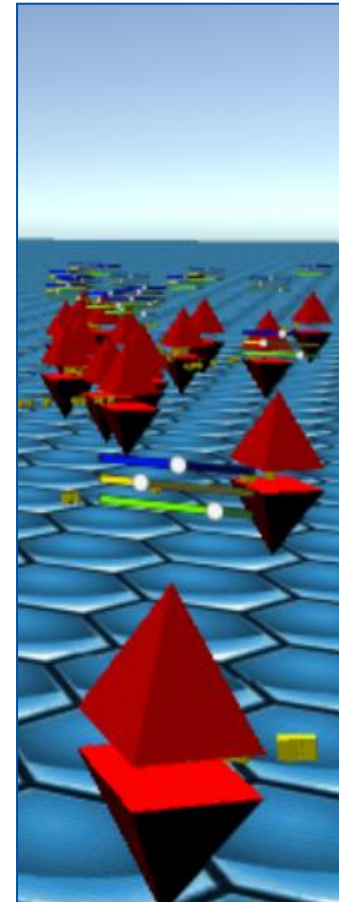




CIAP: Confidentiality, Integrity, Availability, Privacy

CIAP are concepts which have vast goals in Information Security:

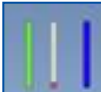
- 
Confidentiality: Ensures that data or an information system is accessed by only an authorized person. User Id's and passwords, access control lists (ACL) and policy based security are some of the methods through which confidentiality is achieved
- 
Integrity: Assures that the data or information system 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.



duced
list



Simulation Team T-REX Day 0 6:33:6 ID Muhsin Mhsud of Muysil A'Alhuria by Mobile
 Simulation Team T-REX Day 0 6:33:6 ID Mu'ommar Gergas of Farh A'Alaa by Snapchat
 Simulation Team T-REX Day 0 6:37:24 ID MuhsinMustafa of Muysil A'Alhuria by Facebook
 Simulation Team T-REX Day 0 6:37:24 ID Jara'Deher of Farh A'Alaa by Twitter
 Simulation Team T-REX Day 0 6:37:24 ID Muhsin Mhsud of Muysil A'Alhuria by Pandora
 Simulation Team T-REX Day 0 6:37:24 ID Saubkhaten of Muysil A'Alhuria by Snapchat
 Simulation Team T-REX Day 0 6:37:24 ID Hamdan Samaha of Farh A'Alaa by Mobile
 Simulation Team T-REX Day 0 6:37:24 ID MuhsinMustafa of Muysil A'Alhuria by Mobile
 Simulation Team T-REX Day 0 6:47:43 ID Wahid of Muysil A'Alhuria by Snapchat
 Simulation Team T-REX Day 0 6:47:43 ID Mu'ayyid Behar of Anshar Lillah by Snapchat
 Simulation Team T-REX Day 0 6:47:43 ID Jara'Deher of Farh A'Alaa by Snapchat
 Simulation Team T-REX Day 0 6:47:43 ID Mkaamir Awan of Muysil A'Alhuria by Facebook



ation Team T-REX Day 0 2:27:1 ID Anbarin Toma of nar Lillah by Email
 ation Team T-REX Day 0 2:31:30 ID Shahd Bitar of nar Lillah by Phone
 ation Team T-REX Day 0 2:31:30 ID Adara Gaber of Al'Aelaa by Instagram
 ation Team T-REX Day 0 2:31:30 ID NafisahHadam of Al'Aelaa by Mobile
 ation Team T-REX Day 0 2:31:30 ID Muhsinah Essa of Al'Aelaa by Mobile
 ation Team T-REX Day 0 2:34:57 ID Adara Gaber of Al'Aelaa by Phone
 ation Team T-REX Day 0 2:34:57 ID Lubab Essa of nar Lillah by Mobile
 ation Team T-REX Day 0 2:43:42 ID Shahd Bitar of nar Lillah by Email
 ation Team T-REX Day 0 2:43:42 ID NafisahHadam of Al'Aelaa by Facebook
 ation Team T-REX Day 0 2:43:42 ID IsmahDagher of til Al'Alhurria by Instagram
 ation Team T-REX Day 0 2:43:42 ID Lubab Essa of nar Lillah by Snapchat
 ation Team T-REX Day 0 2:43:42 ID Muhsinah Essa of Al'Aelaa by Whatsapp



T-REX: Autonomous Systems

Autonomous Systems, on both sides, are driven by **Intelligent Agents** and interact with **traditional Assets**. **Coalition UxV (Unmanned 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.*

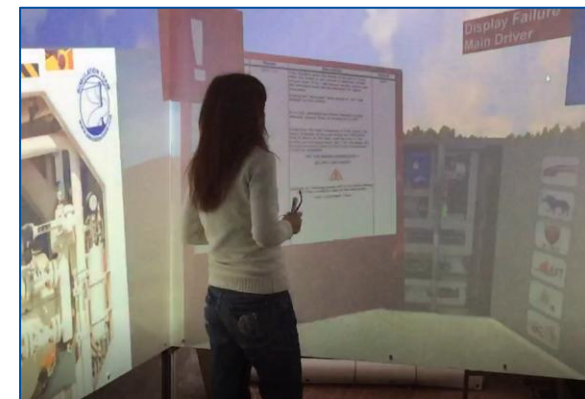
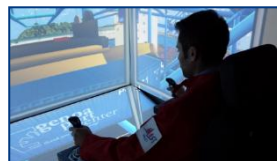
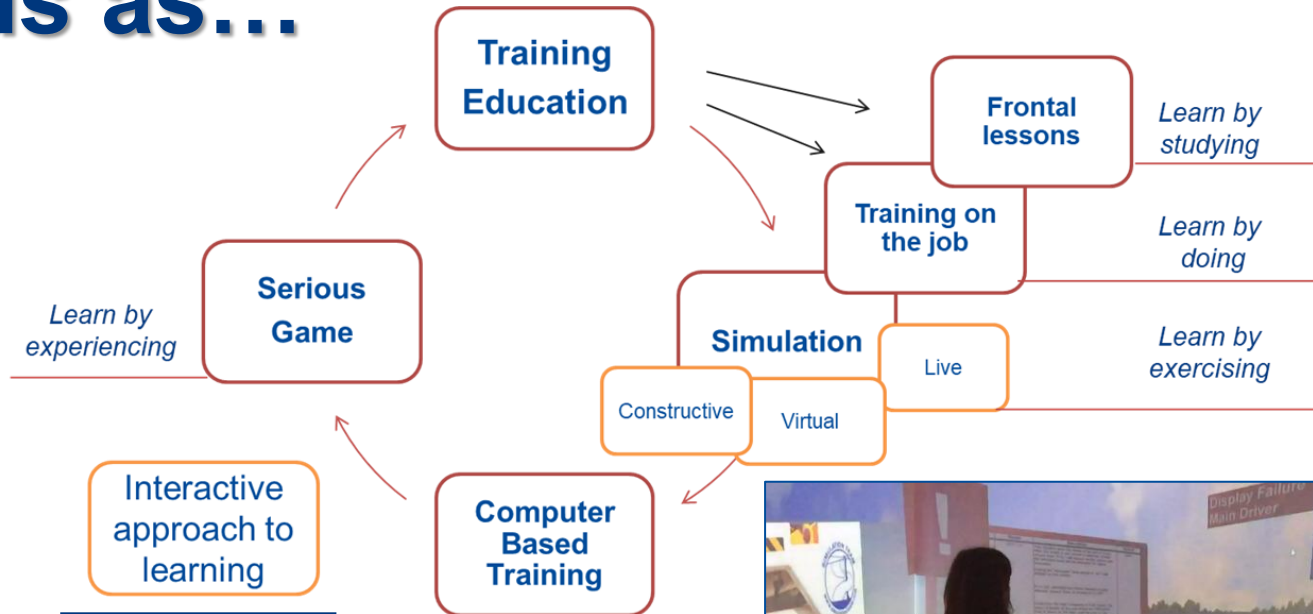


Training Guidelines for Safety, OSHA

OSHA Occupational Safety and Health Administration, USA



Cyber Security & Training Aids as...

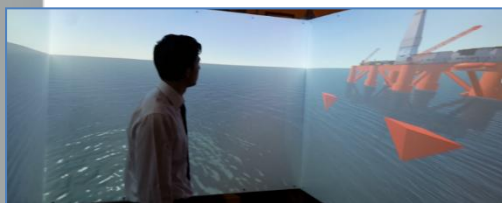


“Tell me and I will forget. Teach me and I will remember. Involve me and I will learn”,

Confucius



... Serious Games Evolve into Simulation Team Roadmap



Training on the Job



Simulation for Training

Experimenting on the Simulator

Many Installations
Many More Users

Serious Games for Training



New Education Modes
New Utilization Modes

Playing while Learning

Experimenting on Games

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





Conclusions



-  **Cyber Security** is a major issue dealing with crucial vulnerabilities addressing not only ICT Systems, but also on real systems such as: Machines, 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.. 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



CALTEK



www.liotech.co.uk



Genoa



CIREM
Università di Cagliari



CentraLabs
Cagliari



CRiCS
Centre for Research
In Complex Systems

CSU
Australia



Mik
Riga TU



Universidad
de la Rioja



AntOptima
we succeed with your business



etea SICUREZZA



Blizzard Srl
Evolution



MSC
LES



LOGIXTICA
Perugia
Perugia Center



DIPMEC

labria



SimCenter Universitat
Autònoma de Barcelona



LSIS
Marseille



SPIRAS Russian
Academy of Science



IMS-LAPS
Univ. Bordeaux



GRVa
LANCE
Rio de Janeiro
Brazil



MITIM
Simulation Team
Genoa Center
McLeod Institute of Technolo
Interoperable Modeling Simu
Genoa

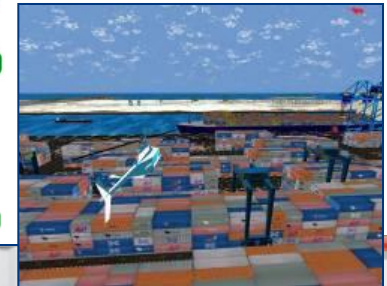


DIME
Università di Genova





References



DIME



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

