TECHNICS AND TECHNOLOGIES FOR CPS

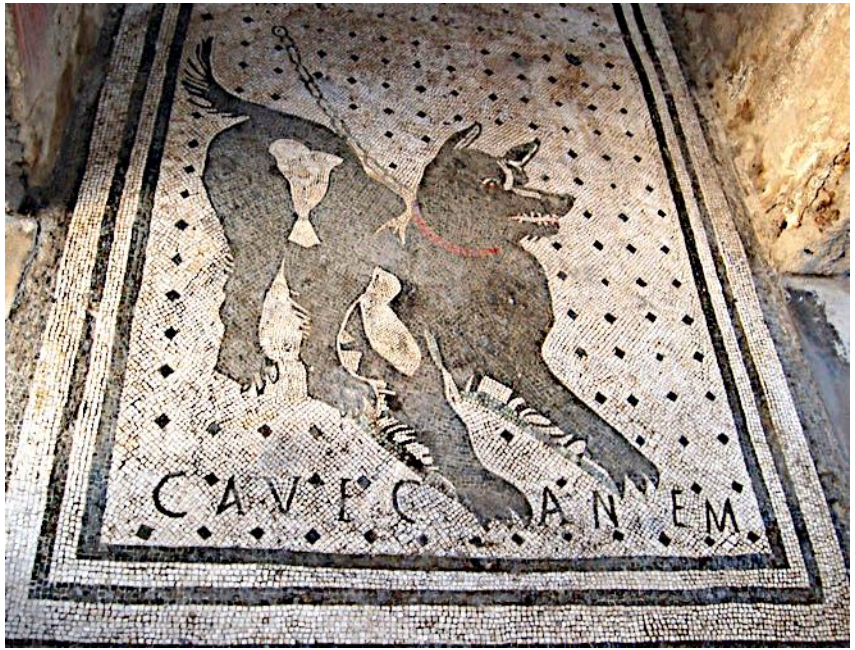
Flavio Frattini

flavio.frattini@consorziosicurezza.com

Burglar Alarm in the I Century

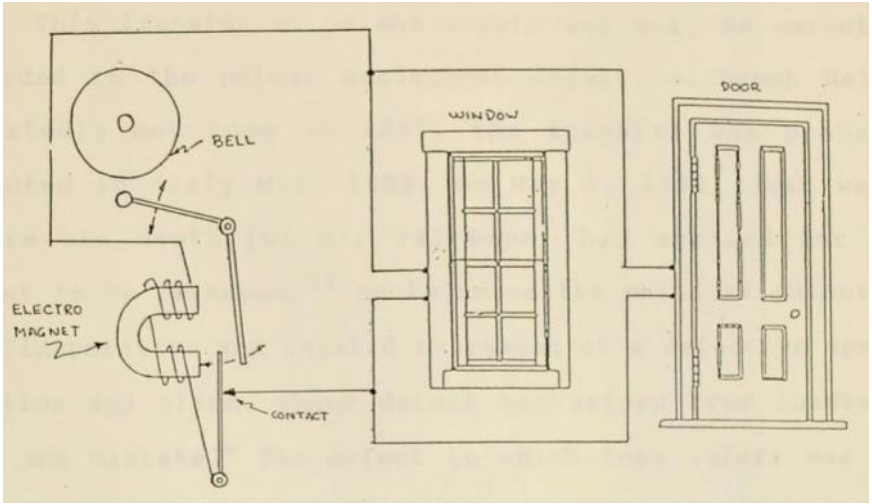
- **A LONG, LONG TIME AGO…**

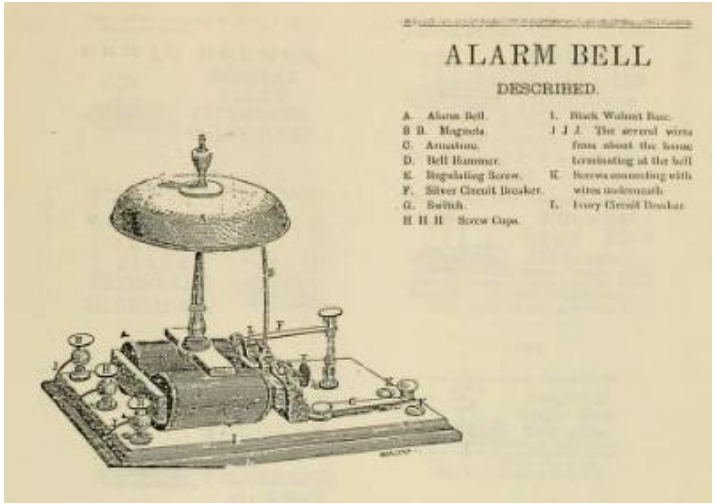
From *Beware of the dog…*



…in the XIX Century

- **A LONG TIME AGO…**

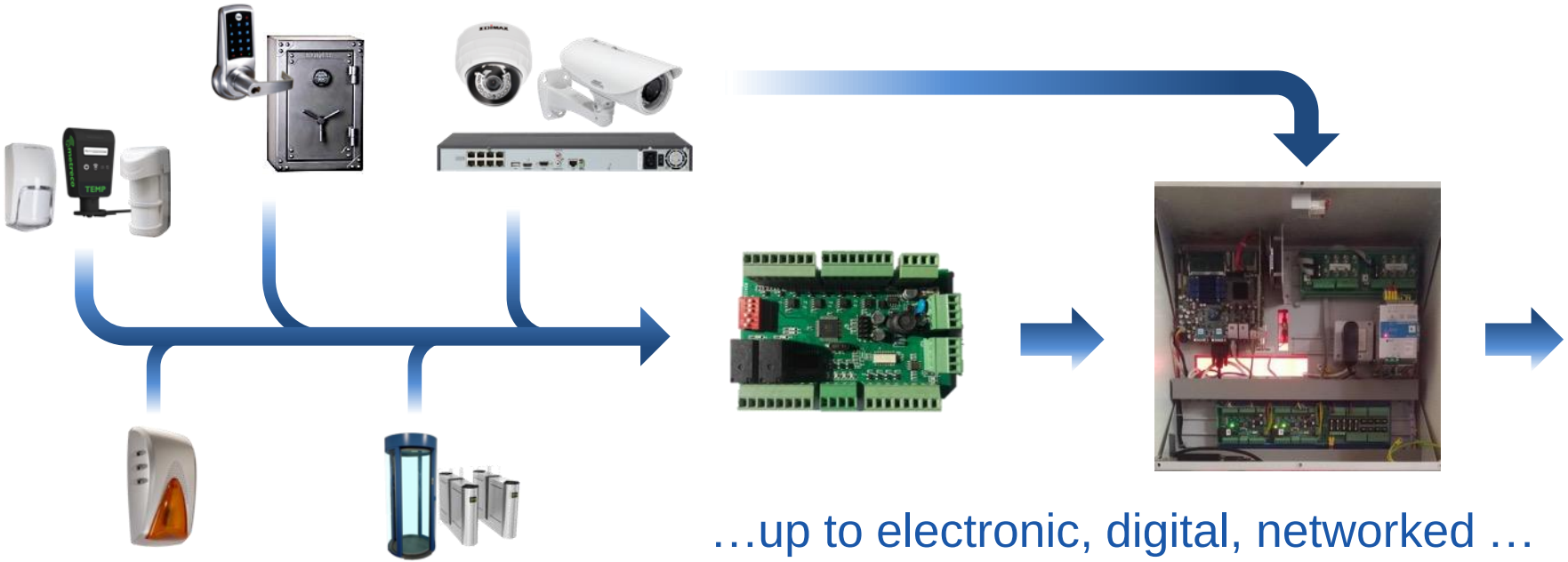




…to electric…

Protection System in the XXI Century

- **NOWADAYS…**



…up to electronic, digital, networked …

Protection System in the XXI Century

Vulnerabilities

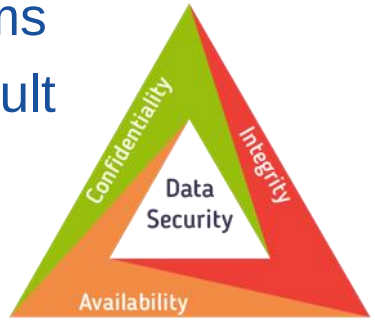
- X Sensor←→IN/OUT Module
- X IN/OUT Module←→Alarm control panel
- X Alarm control panel←→PSIM
- X Alarm control panel
- X PSIM system

Alarm control panel

- Brute force, Footprinting, Scanning, Enumeration, …
- Designed, build and configured for security (**security-by-design**)
- **Selection of hardware and software** (OS and applications)
  - **Avoid dictionary password, reduce open ports, keep the system updated**
  - **Avoid useless services' activation**
  - **Intrusion detection, authentication system**

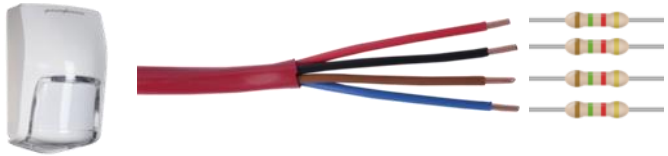
Secure communications

- COMMUNICATION CHANNELS ARE TO BE SECURE:
  - ***Confidentiality*** is enabled by Cryptography
  - ***Integrity*** can be assured by authentication mechanisms
  - ***Availability*** is achieved by using reliable hardware, fault tolerance, …



Sensor←→IN/OUT Module

- A possible attack is to cut the wire and add some resistance with the right tension value



- **Add a module for cryptography**
- **Use secure WSN**
  - Cryptography
  - Key Management Protocol
  - Frequency hopping and Code spreading

IN/OUT Module🡐🡒Alarm Panel

- Issues similar to sensor-module communication
- …but also cyber attacks
- **Symmetric key cryptography**
- **Session keys**
  - These allows making the transmitted data confidential and authenticating the sender of the information

Alarm Panel←→PSIM

- **CEI 79**
  (jointly defined with ABI – Italian Bank Association)
  - 5.1 Communication protocol for security information (alarms) – Transportation layer
  - FEAL-N
    DES-like 64 bit block cipher algorithm (proposed in 1987, last update 2009)

Monitoring and Controlling

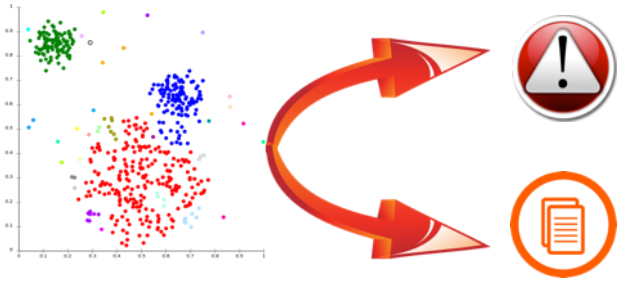
- PSIM systems collect and analyze data on physical security
  - ***What about cyber-security?***

SIEM – Security Information and Event Management

- **Data analytics: log events and network flow data from all the devices (not only of the protection system)**
  - **AI, statistical approaches, fuzzy algorithms, etc.**

Monitoring and Controlling

- ✓ Anomaly detection (near real-time)
- ✓ Uncovering threats
- ✓ Reduction of false positives
- ✓ Reduction of incidents/threats list for security analysts
- ✓ Fault forecasting and failure detection



Conclusion

- **Systems are now cyber-physical, and have specific security issues**
  - New vulnerabilities, further threats
- **But research paved the way towards the solution**
  - Some issues are still to be solved,
  - For the others, we have the means to face them

THANK YOU!

SOLUZIONI PER LA CPS

SENSORE-CONCENTRATORE
Comunicazione sicura tra sensori di allarme e concentratori

CONCENTRATORE-CENTRALE
Comunicazione sicura tra concentratore e centrale

CENTRALE-PSIM
Comunicazione sicura tra centrale e sistema di centralizzazione

CENTRALE
Robusta rispetto agli attacchi cyber

CPSIEM
Realizzato in collaborazione con IBM, è il primo sistema che integra le funzionalità di un PSIM con quelle di un SIEM fornendo una visione completa di physical security e degli aspetti di cyber security ad essi collegati