

PROGETTO 2.1 CYBERSECURITY DEI SISTEMI ENERGETICI

ITASEC, 9 Febbraio 2026

Damn Vulnerable Infrastructure Are you ready for the next StuxNet?

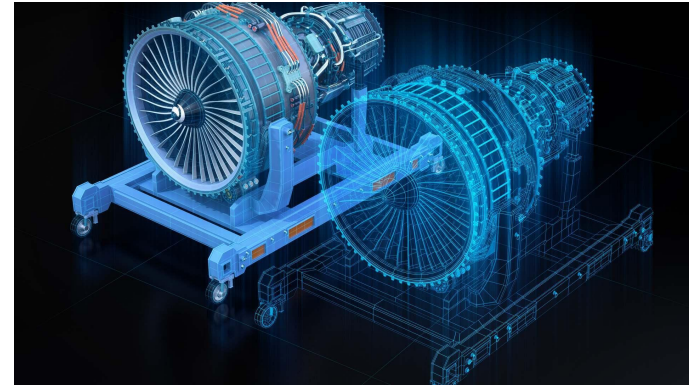
Gabriele Costa, IMT Scuola Alti Studi Lucca

Digital twin (DT) frameworks are often focused on one or few, specific levels of abstractions

- OT fragment, networking, performance, ...
- For this reason the term DT often refers to simulators of a single object

Problem: security operations, e.g. VAPT, are only effective if DT accurately model the entire infrastructure

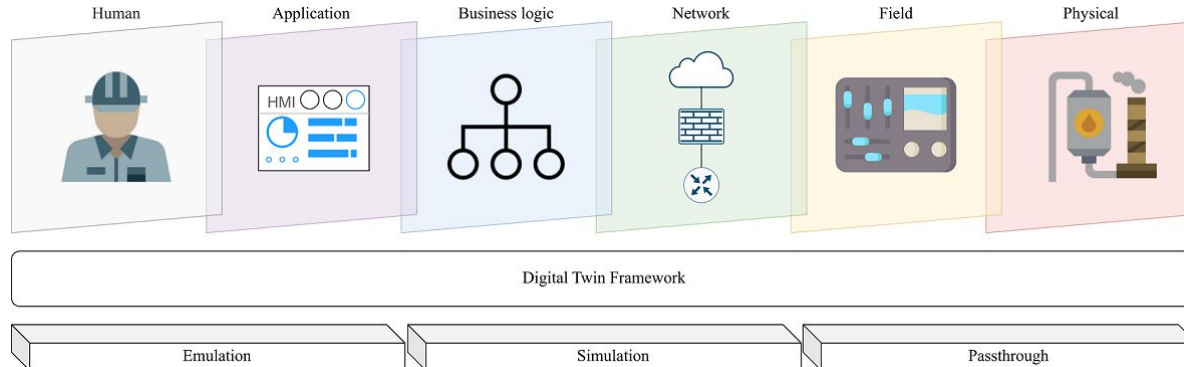
- E.g., since real attackers may rely on every part of it (lateral movements)



A framework based on the **Infrastructure-as-Code (IaC)** paradigm

Every element of an infrastructure is modelled and replicated through either

- **Emulation**, e.g., software is executed on virtual machines
- **Simulation**, e.g., data is generated by equations or taken from datasets
- **Passthrough**, e.g., a real system is connected via VPN

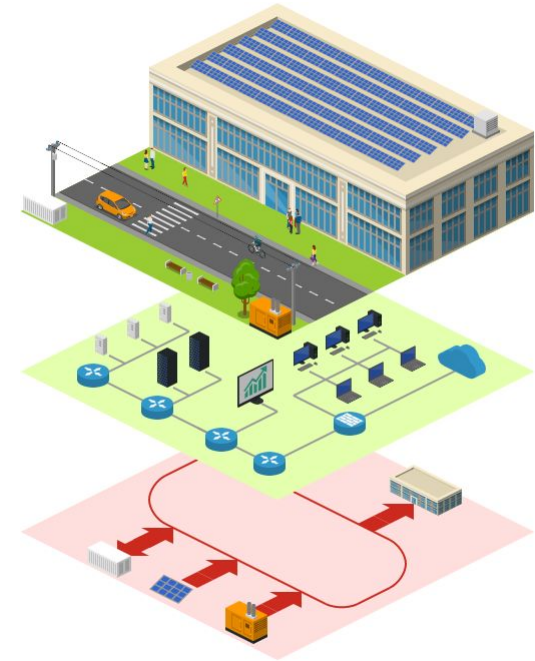
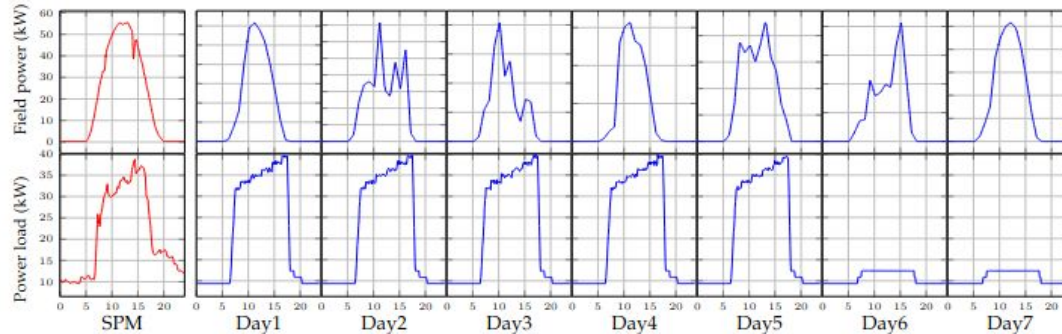


Entire infrastructures can be reproduced in detail using limited resources

Already applied to a real energy infrastructure: SV Polygeneration Microgrid (SPM)

SPM includes: solar panels, gas turbines, batteries, ...

- A real microgrid with its IoT/SCADA system
- Hosted in a university campus with its IT services



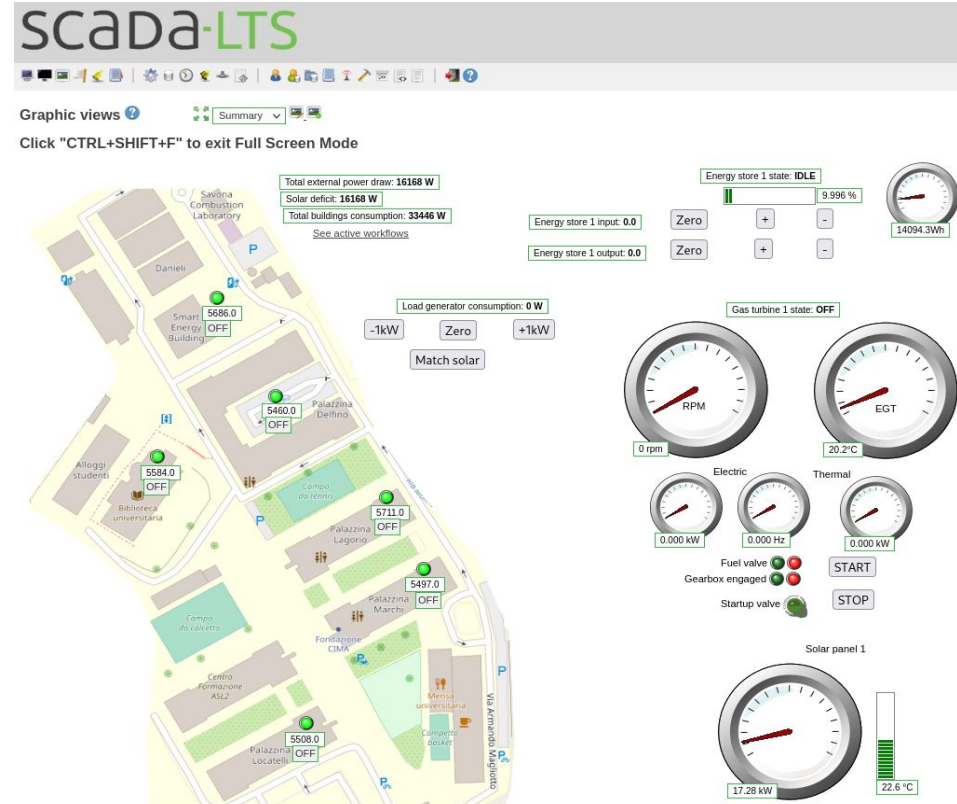
Physical processes are simulated (mainly through ODE modeling and custom code)

Field devices are emulated (via software PLC and Ditto APIs)

Networks are emulated via Docker networks

Business logic and humans are simulated via Camunda/BPMN

Applications are emulated via docker



Idea: populate SPM with intentionally vulnerable technologies/service

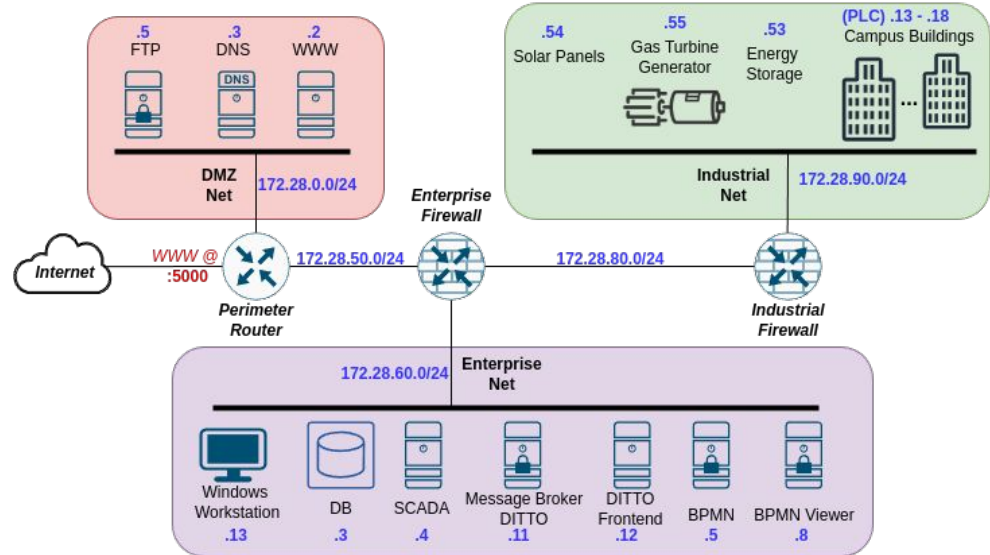
- Not just randomly placed, but intended to simulate attack scenarios (with lateral movements)

Multiple difficulty levels for demonstration and training

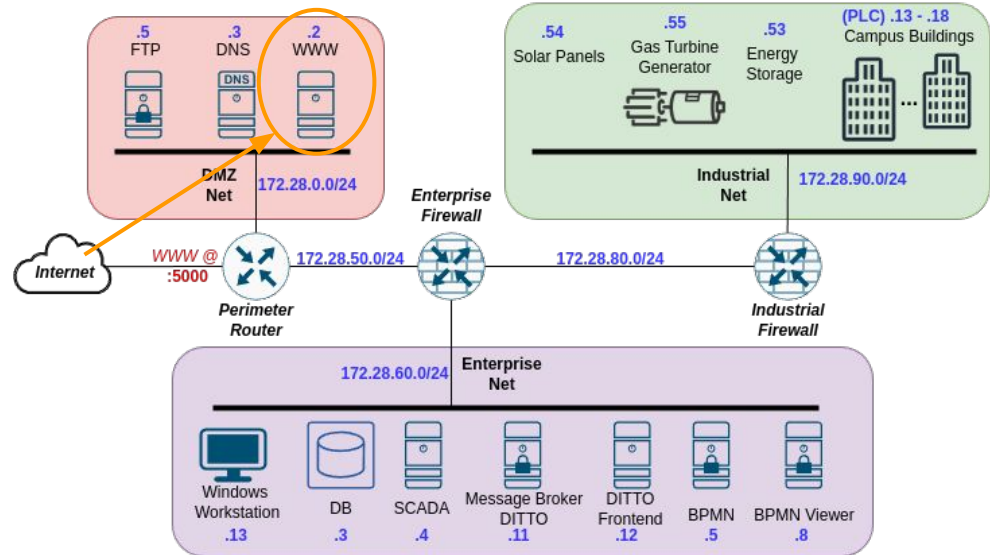
- **Very easy:** network schema, detailed informations, sub-goals
- **Very hard:** no information at all, a single IP entry point

Accepted as part of the OWASP Vulnerable Web Applications Directory project

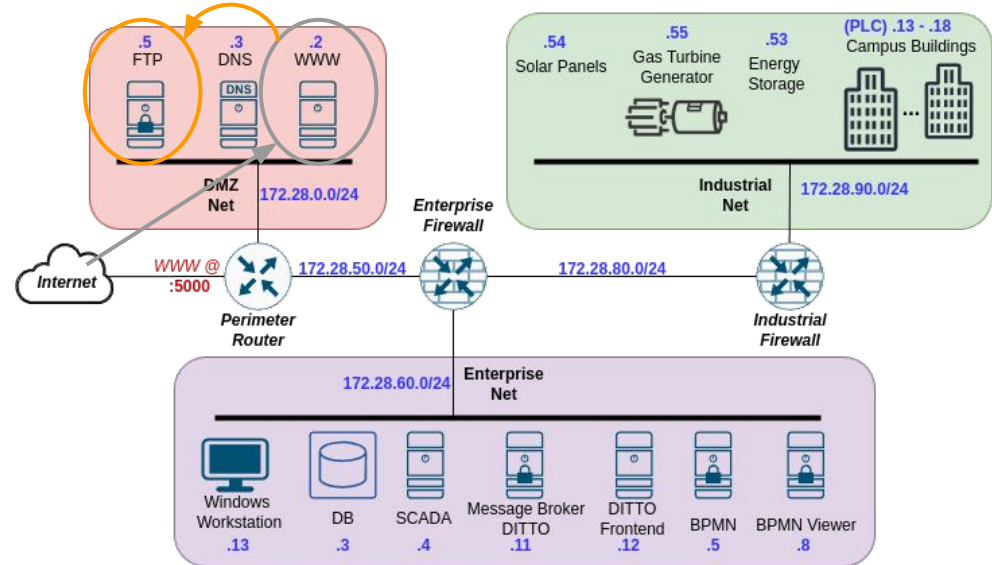




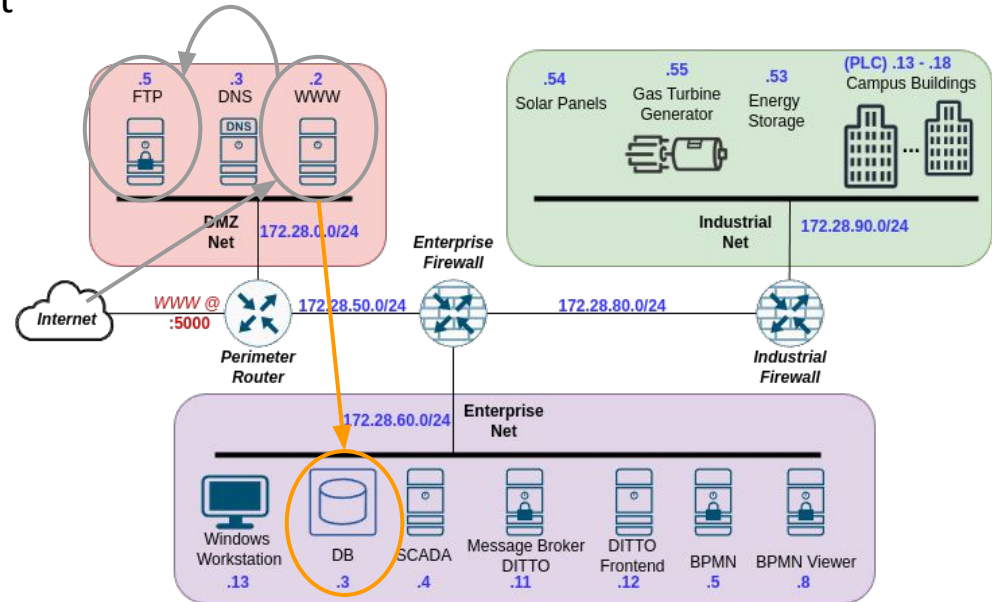
1. **Webserver Takeover:** compromise WWW and open a remote shell



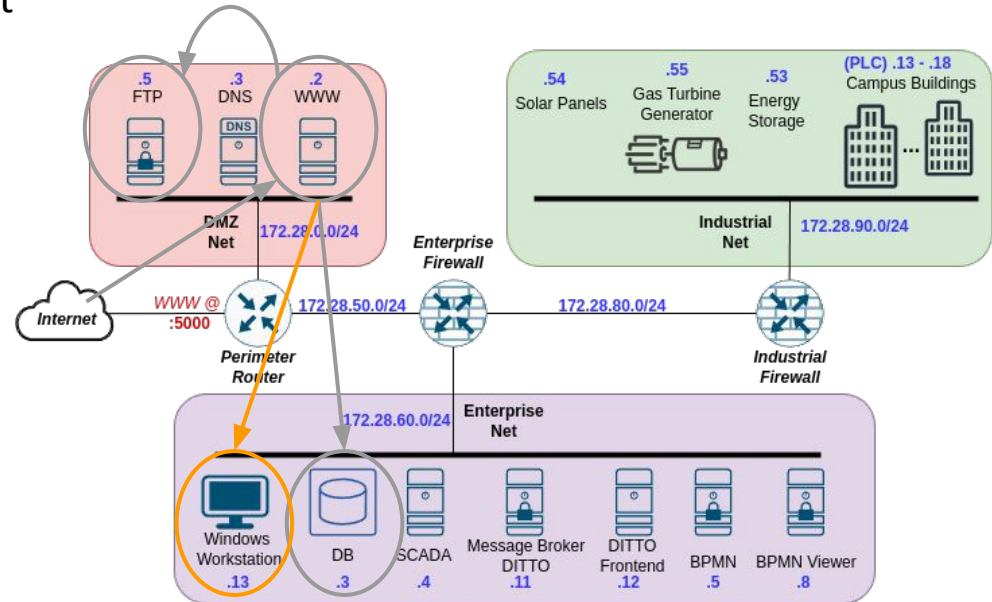
1. **Webserver Takeover:** compromise WWW and open a remote shell
2. **FTP Takeover:** find a CVE and exploit it to bypass authentication



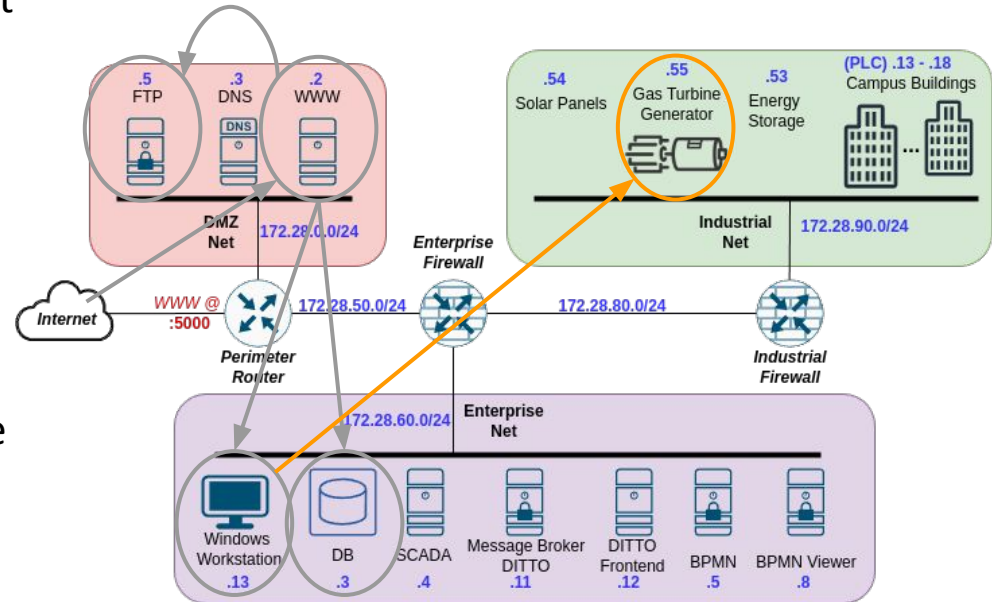
1. **Webserver Takeover:** compromise WWW and open a remote shell
2. **FTP Takeover:** find a CVE and exploit it to bypass authentication
3. **Data Exfiltration:** steal data from DB



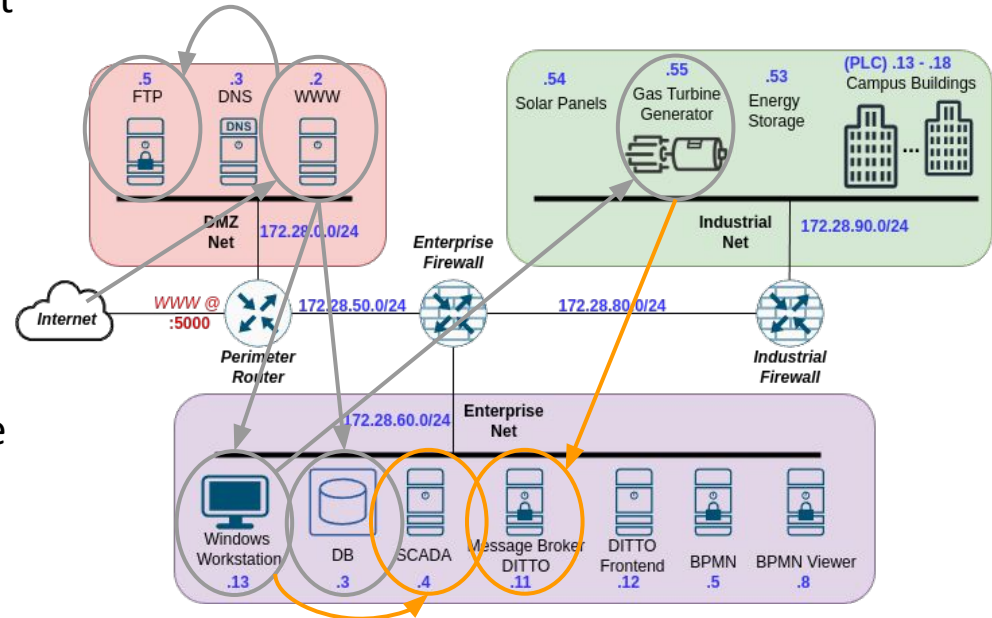
1. **Webserver Takeover:** compromise WWW and open a remote shell
2. **FTP Takeover:** find a CVE and exploit it to bypass authentication
3. **Data Exfiltration:** steal data from DB
4. **Workstation Takeover:** exploit a vulnerable RDP service

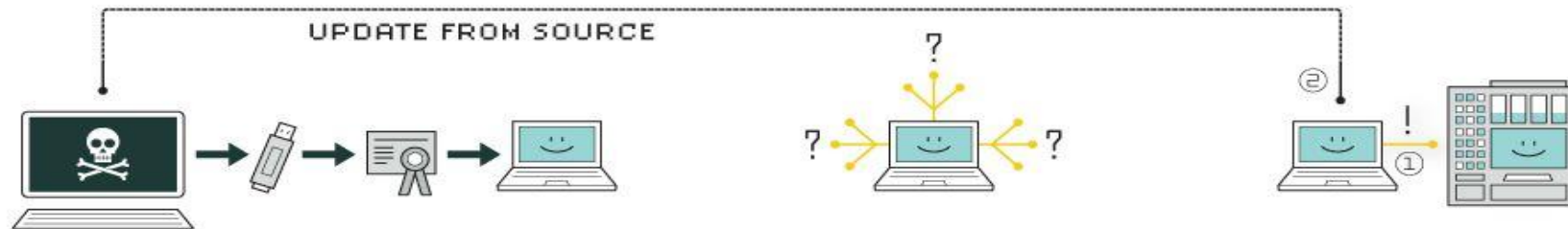


1. **Webserver Takeover:** compromise WWW and open a remote shell
2. **FTP Takeover:** find a CVE and exploit it to bypass authentication
3. **Data Exfiltration:** steal data from DB
4. **Workstation Takeover:** exploit a vulnerable RDP service
5. **PLCs Takeover:** login through insecure credentials



1. **Webserver Takeover:** compromise WWW and open a remote shell
2. **FTP Takeover:** find a CVE and exploit it to bypass authentication
3. **Data Exfiltration:** steal data from DB
4. **Workstation Takeover:** exploit a vulnerable RDP service
5. **PLCs Takeover:** login through insecure credentials
6. **Infrastructure Takeover:** disrupt the EMS logic without the SCADA noticing it





1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

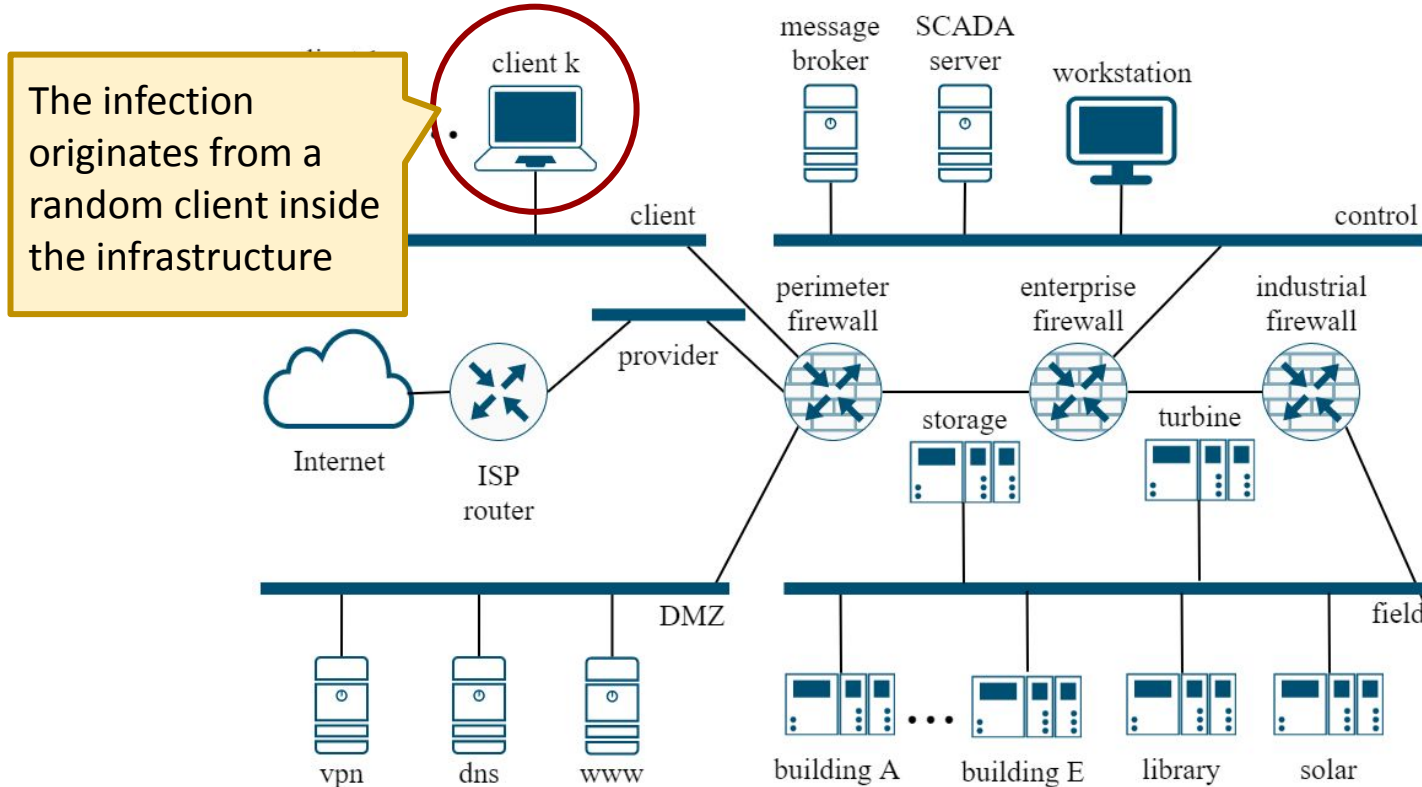
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

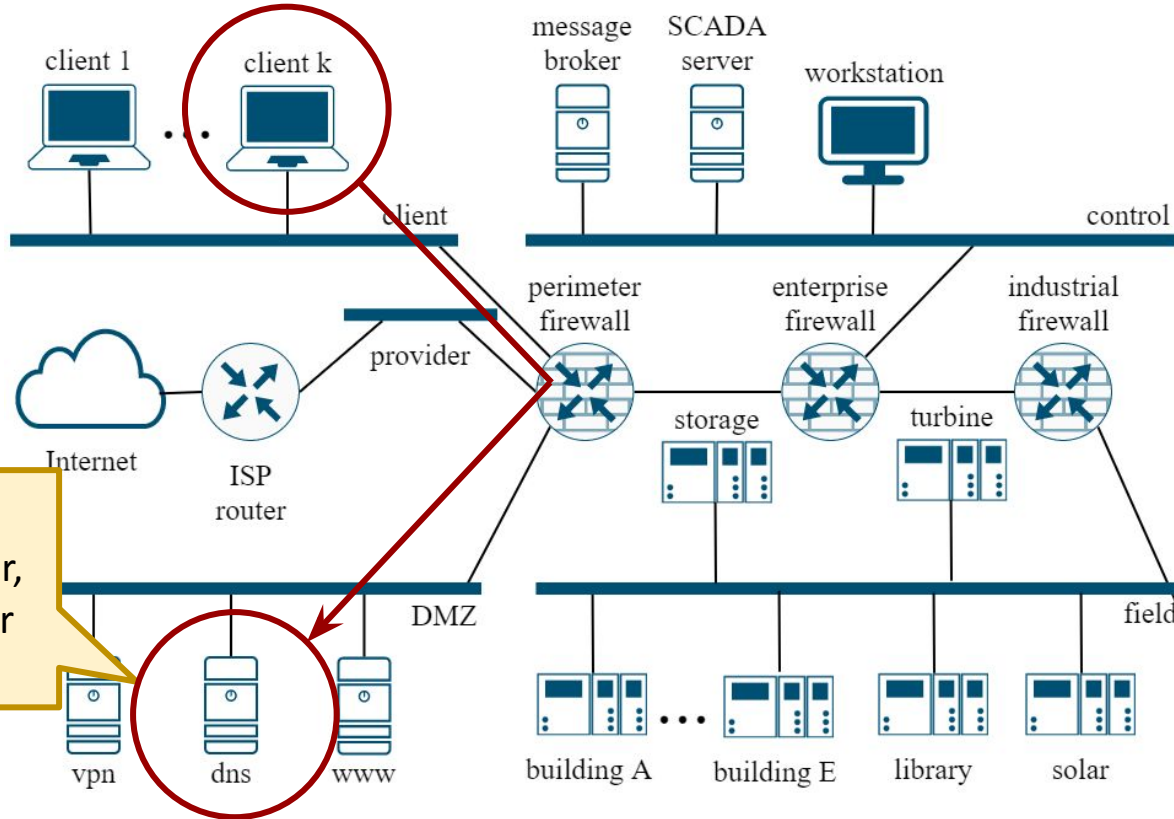
5. control

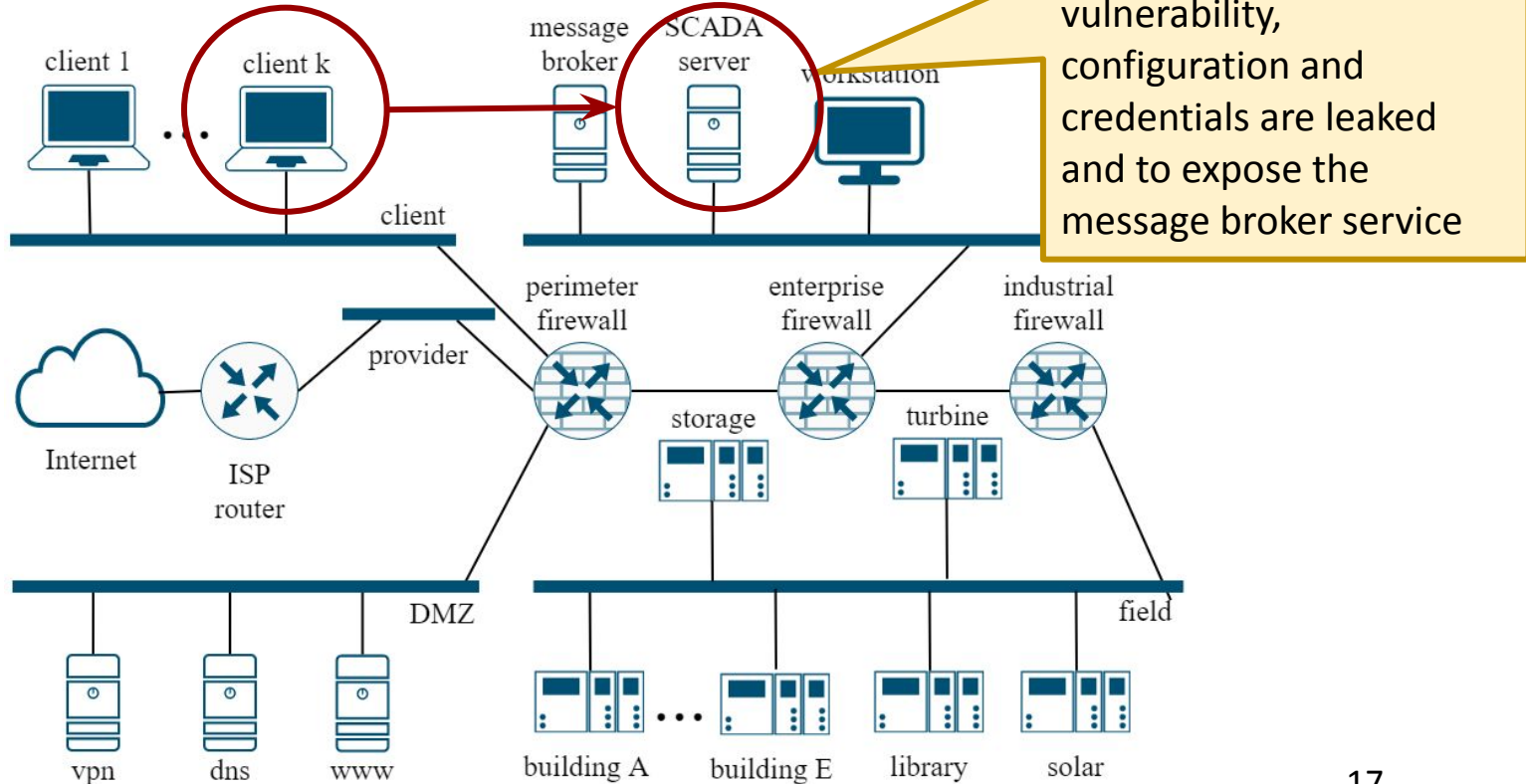
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

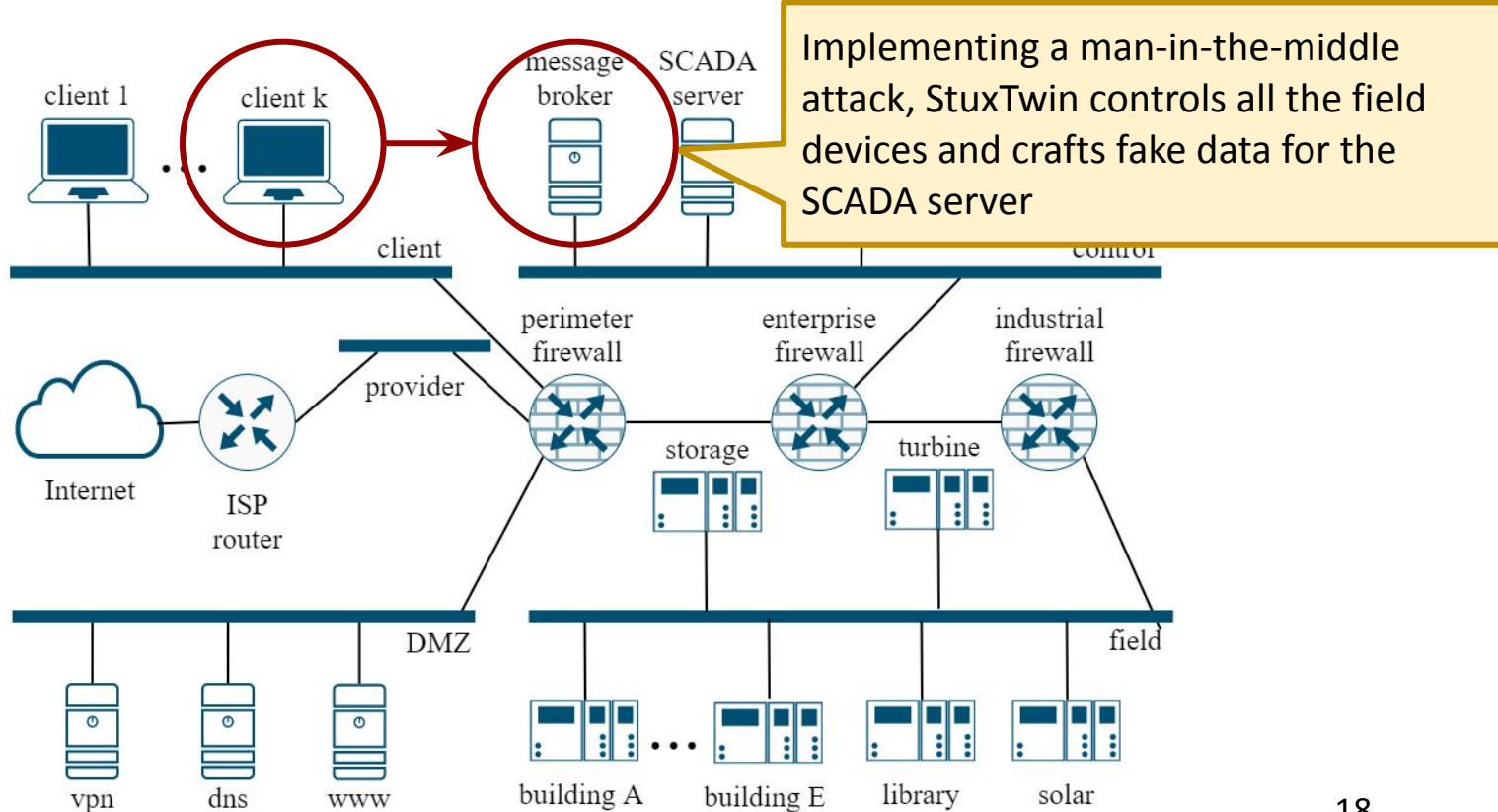
6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.









PROGETTO 2.1 CYBERSECURITY DEI SISTEMI ENERGETICI

ITASEC, 9 Febbraio 2026

<https://github.com/LBartolini/DVI>