Towards Secure Monitoring and Control Systems: Diversify!

Domenico Cotroneo, Antonio Pecchia, Stefano Russo

Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI)
Federico II University of Naples
Via Claudio 21, 80125, Naples, ITALY

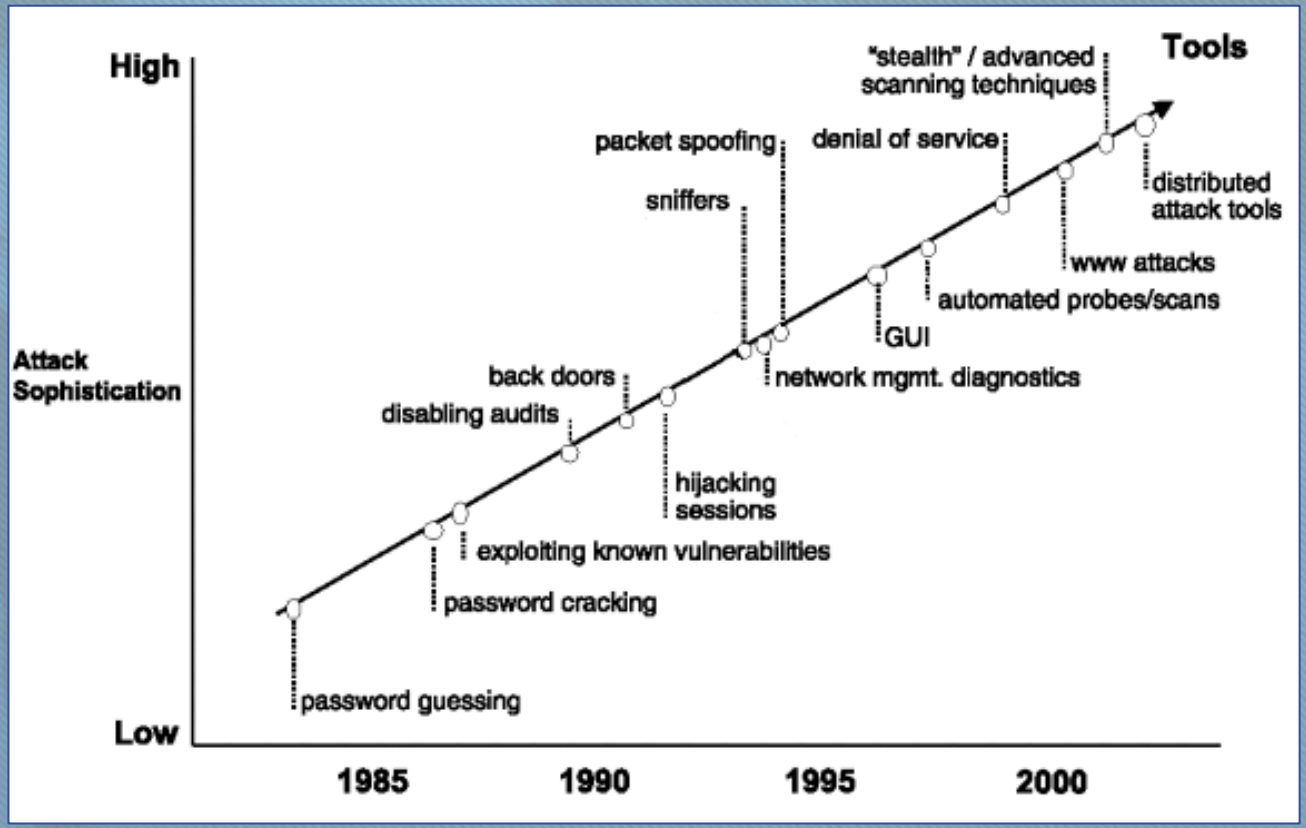
The 43rd Int'l Conference on Dependable Systems and Networks (DSN 2013)
Session: Fast Abstracts 2
Budapest, HUNGARY June, 27

Meeting TENACE, Tropea, 25 Settembre 2014

www.mobilab.unina.it antonio.pecchia@unina.it

Trends in security attacks

- Security attacks have become more and more sophisticated.



What's next?

- Stuxnet?

Impairment of the supervisory control and data acquisition system!

Shall we still care?

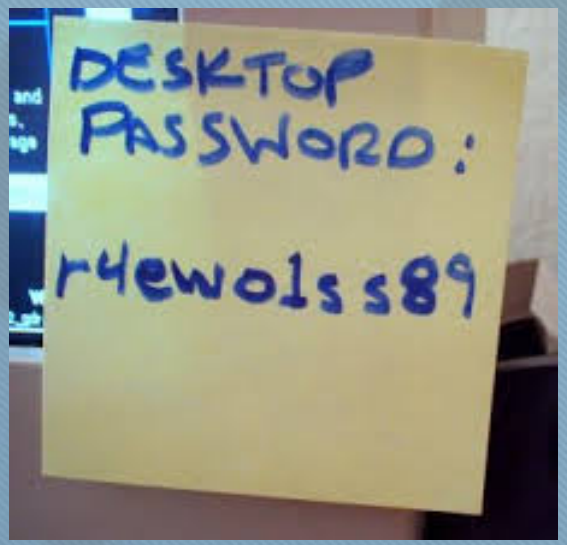
www.mobilab.unina.it antonio.pecchia@unina.it

Some examples

- **Gasoline Pipeline Explosion, US, 1999**
  - poor personnel training, faulty pressure relief valve;
- **North Eastern US-Canada Power Failure, 2003**
  - bug in the control program;
- **Maroochy Shire Waste Water Attack, 2000**
  - stolen equipment being used to remotely control the system.

What it can be done?

- Many failure causes, either accidental or malicious:
  - monitoring/control equipment, OSs, software components.
- Bad operator practices, insider threats.



A diversity-based approach?

- Combining different technologies and protection means to increase the attack effort

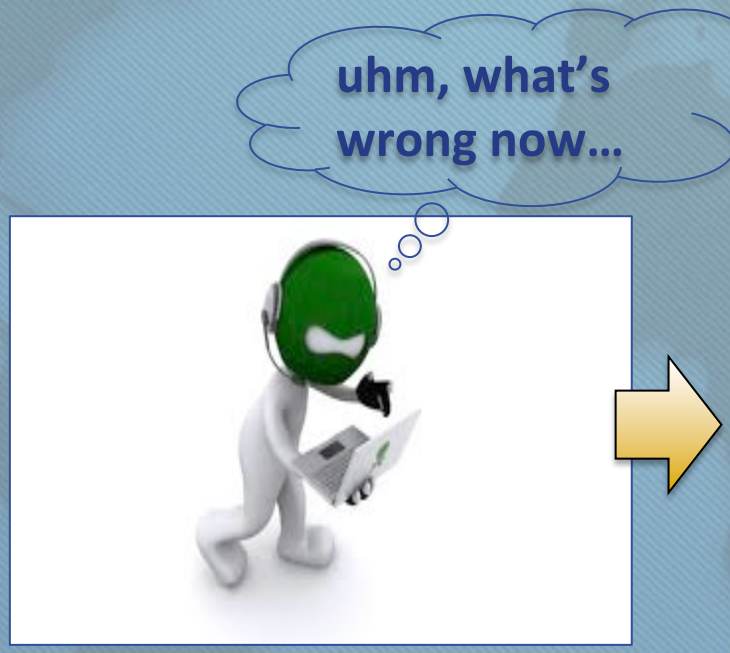
same machine

M_1 M_2

$P(A) \approx P(M_1)$

A diversity-based approach?

- Combining different technologies and protection means to increase the attack effort



different machines

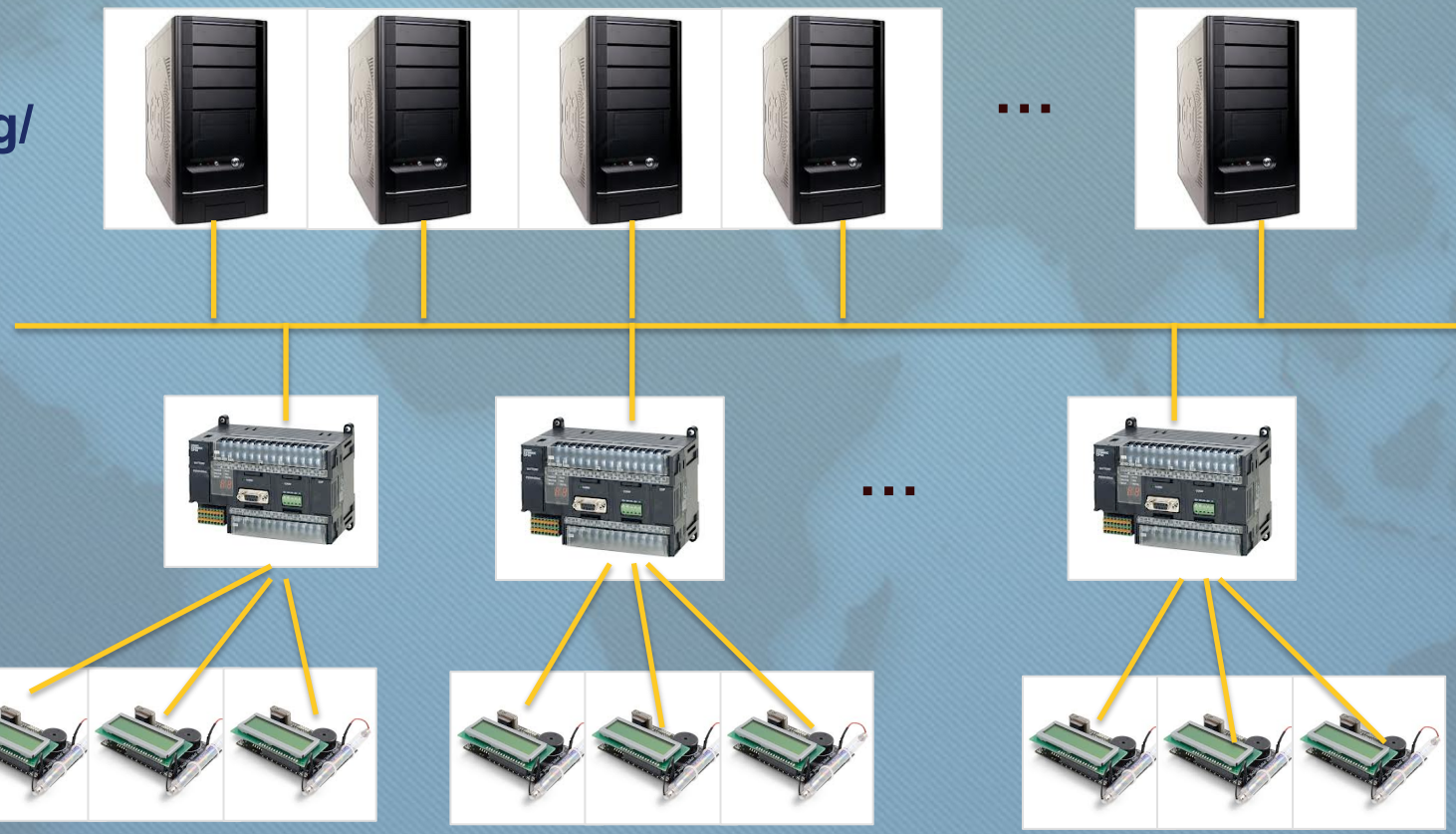
M_1 M_2 $(M_2 < M_1)$

$$P(A) \approx P(M_1) \times P(M_2)$$

www.mobilab.unina.it antonio.pecchia@unina.it

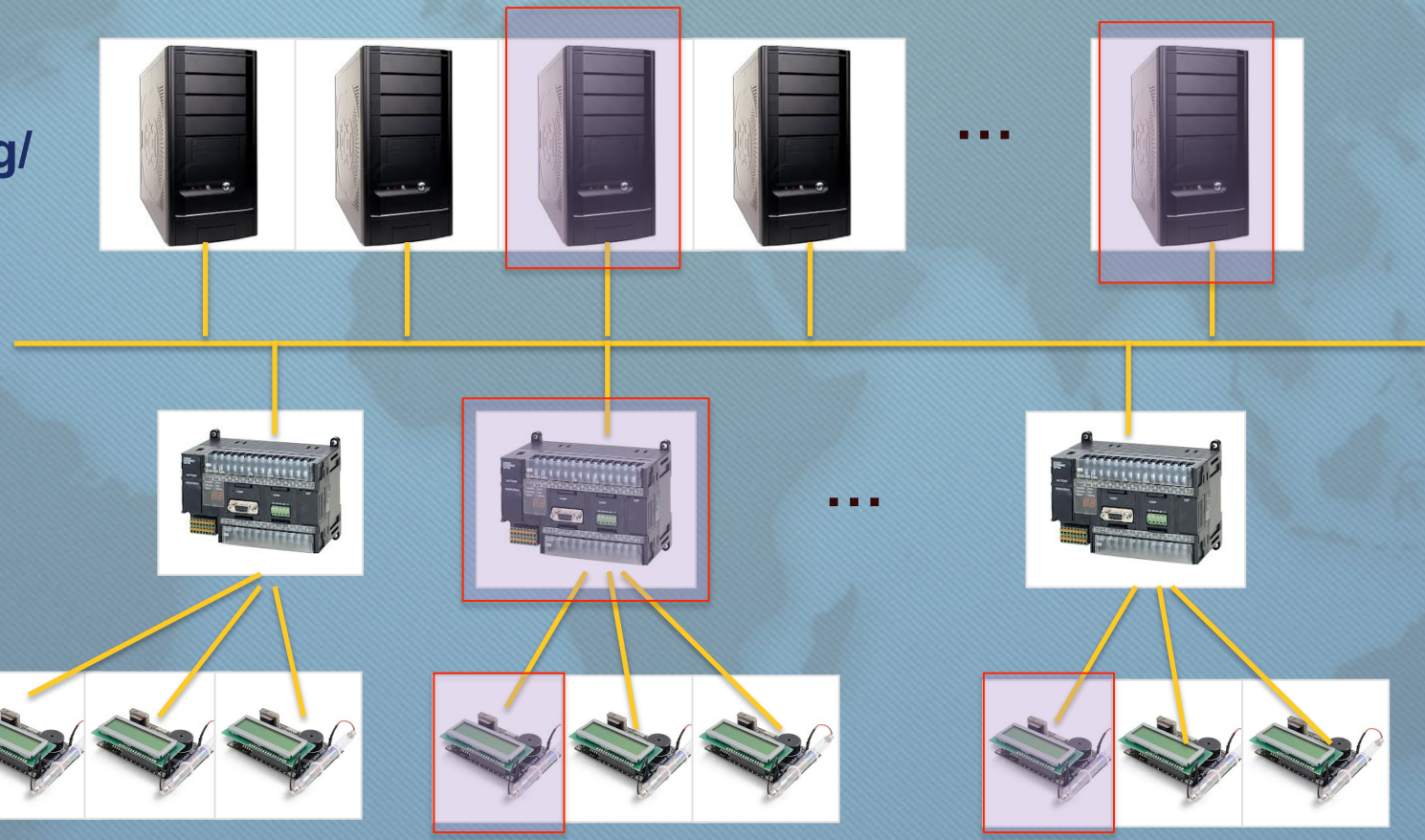
How does it work?

- SCADA systems have an inherent degree of replication



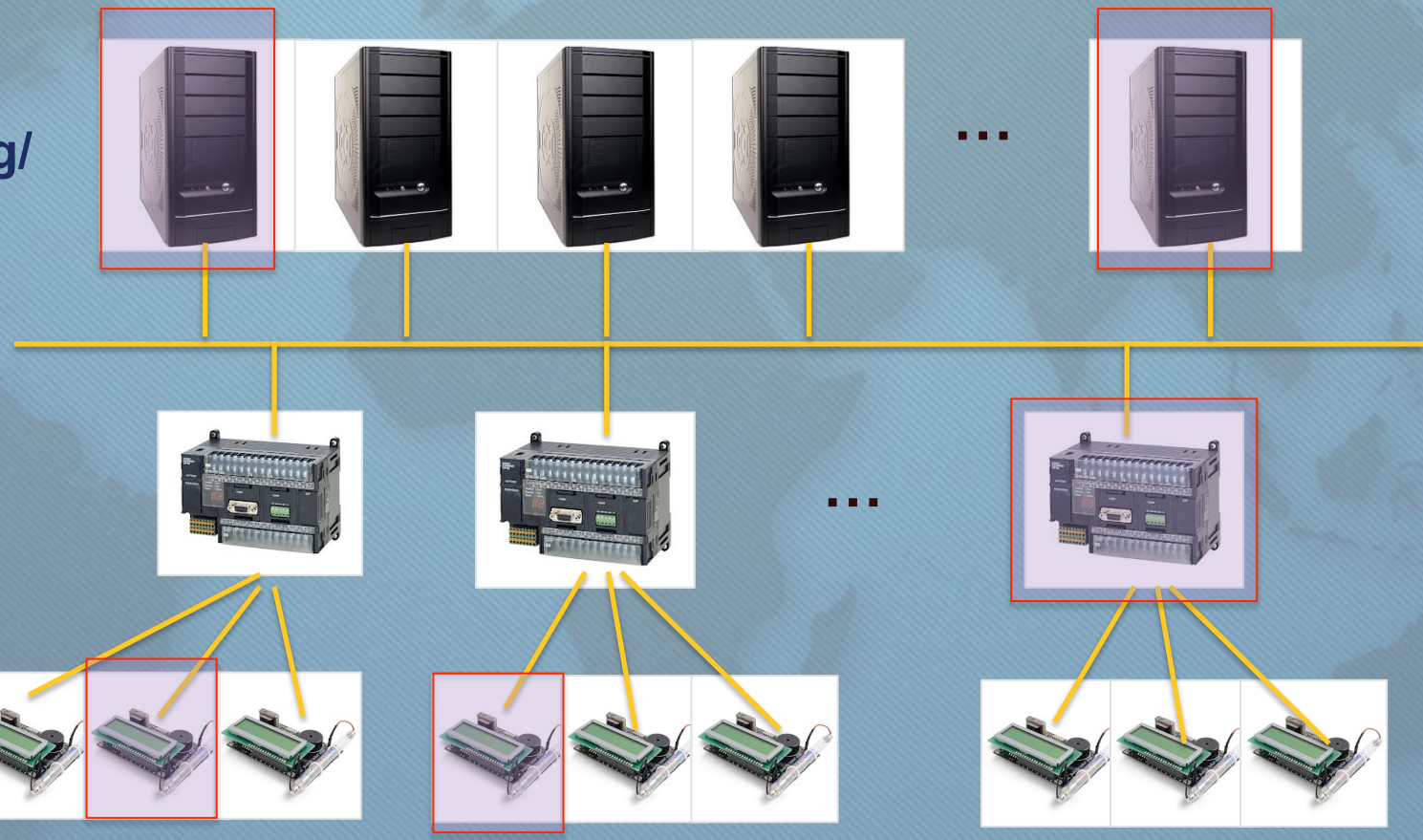
How does it work?

- SCADA systems have an inherent degree of replication



How does it work?

- SCADA systems have an inherent degree of replication



Secure monitoring and control

- A three-step modeling approach.

Attack Modeling

- identification of attack phases
- mapping onto system equipment

Secure monitoring and control

- A three-step modeling approach.

Attack Modeling

- identification of attack phases
- mapping onto system equipment

Design of Experiments

- inferring meaningful “diverse” system configurations

www.mobilab.unina.it antonio.pecchia@unina.it

Secure monitoring and control

- A three-step modeling approach.

Attack Modeling

- identification of attack phases
- mapping onto system equipment

Design of Experiments

- inferring meaningful “diverse” system configurations

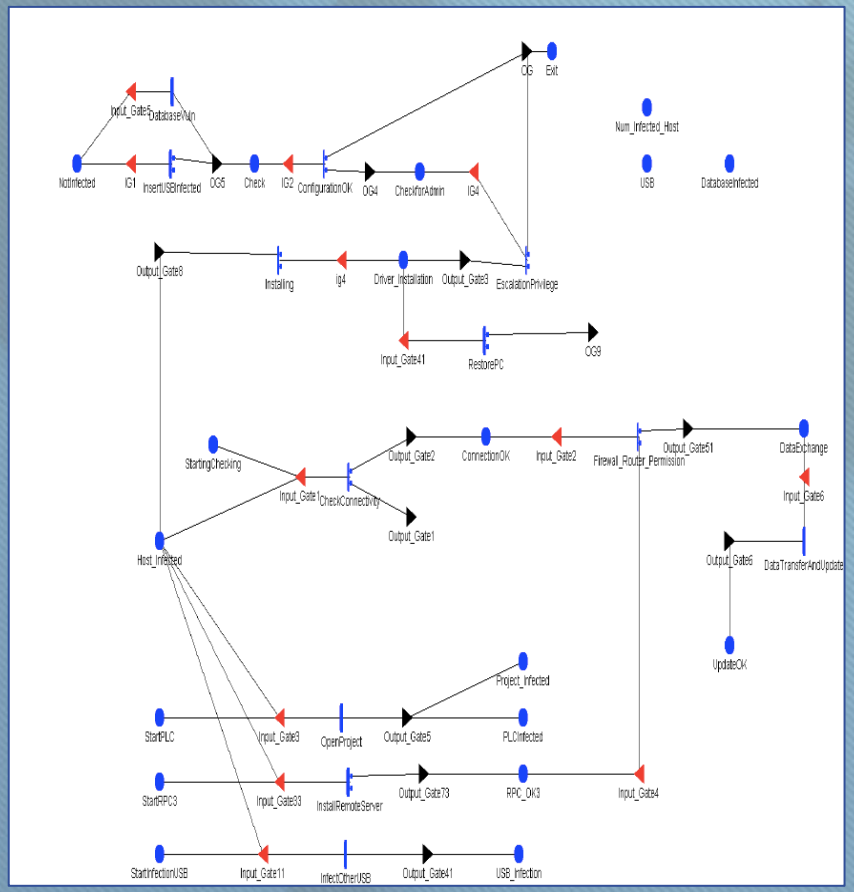
Assessment

- how security metrics have been impacted?

www.mobilab.unina.it antonio.pecchia@unina.it

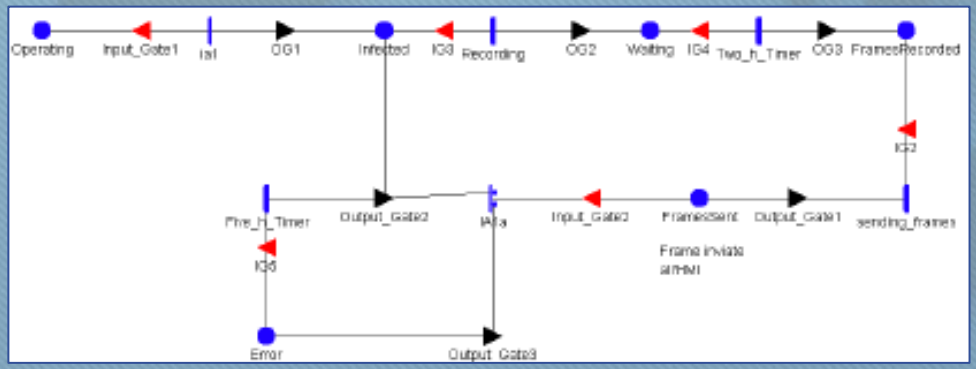
A case study: Stuxnet

Engineering station model



Timed Activity	TTS
Recording	1 *mounth*
Two_H_Timer	2 *hours*
Sending Frames	50 *mins*
Five_H_Timer	5 *hours*

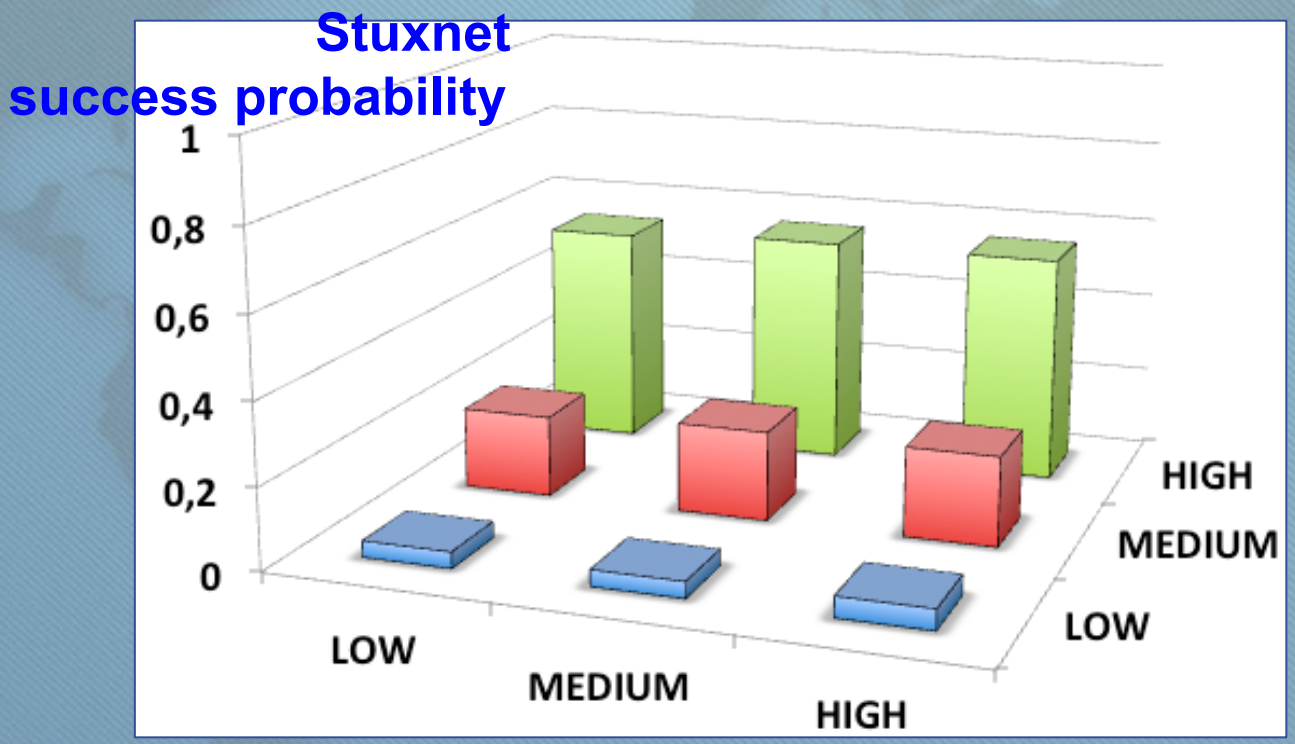
PLC model



www.mobilab.unina.it antonio.pecchia@unina.it

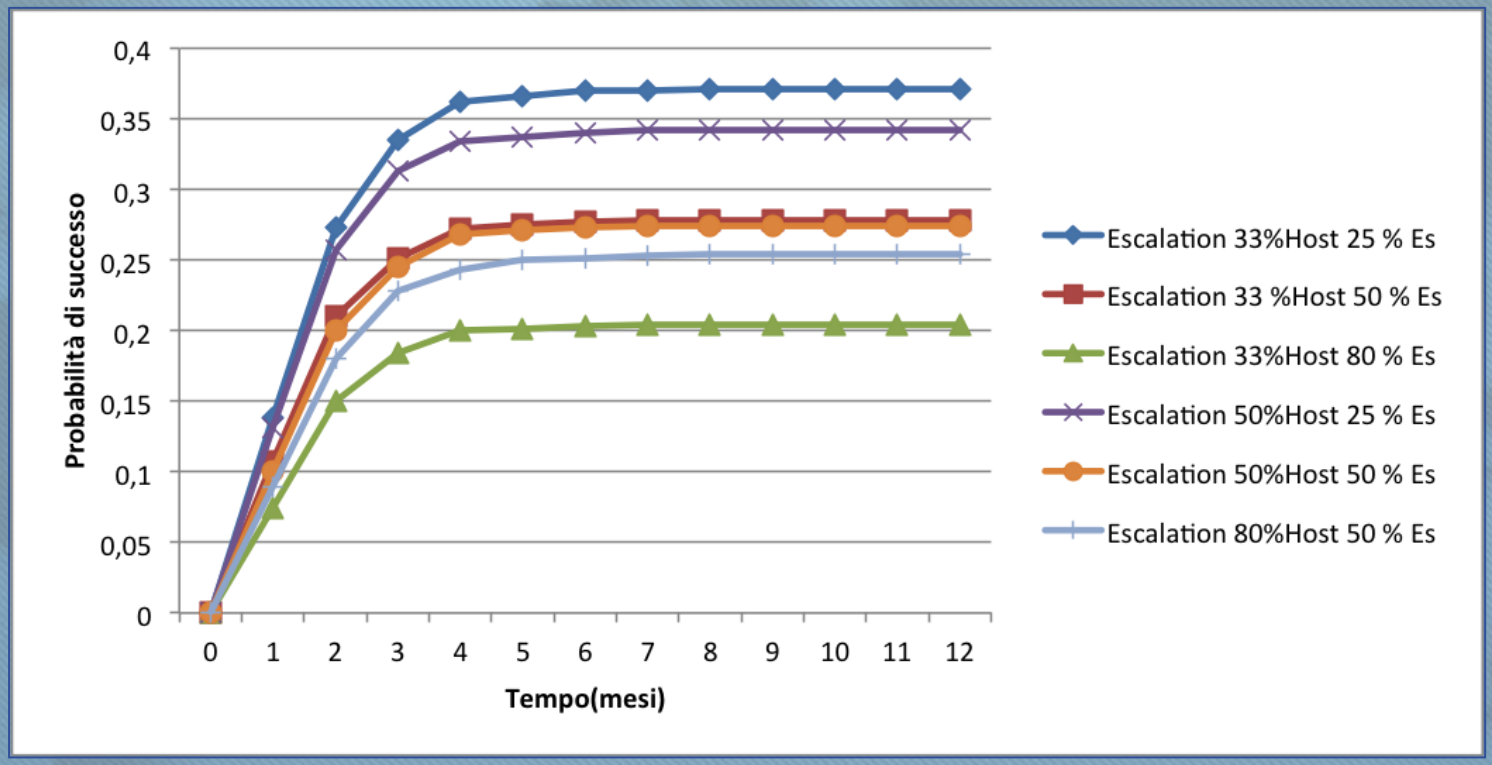
Preliminary results: example

- Protecting the network is not as worthy as protecting a node!



Preliminary results: example

- How much diversity?



Future work

- Improving the assessment framework:
  - bringing in further modeling elements (sensors, actuators);
  - supporting more attack types.
- Applying the approach to real critical infrastructures.
- Moving to other domains: data-centers, cloud computing infrastructures.

Thank you for the attention …

… any question?

antonio.pecchia@unina.it

http://wpage.unina.it/antonio.pecchia