UNIVERSITÀ DEGLI STUDI
DI GENOVA

Sicurezza delle infrastrutture critiche: Progetto POR-FESR Regione Liguria

Convegno PARMA Cybersecurity

Armando Tacchella

Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS)

Giovedì 14 novembre 2019

Contesto della ricerca

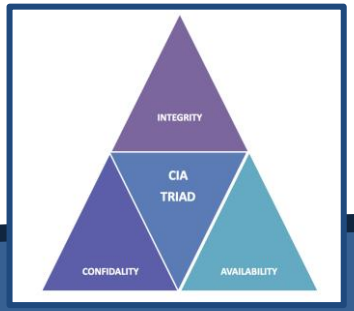
≠

Information Technology (IT)

Operational Technology (OT)

IT cybersecurity ≠ OT cybersecurity

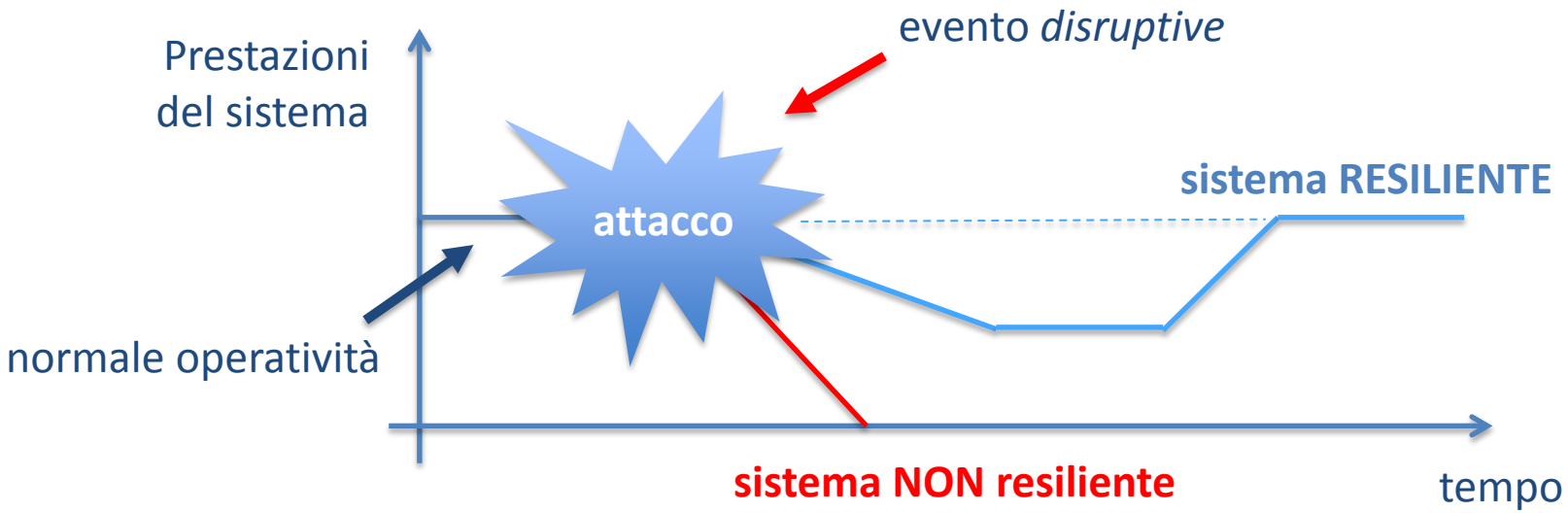
Differenti priorità



La resilienza nella cybersecurity OT

Presidential Policy Directive (*PPD-21*) - President Obama 14/02/2013

defines **resilience** as ***"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."***



Obiettivo della ricerca

Creazione di un framework di valutazione della resilienza dei sistemi cyberfisici

CARATTERISTICHE RICERCATE

1) MODEL FREE

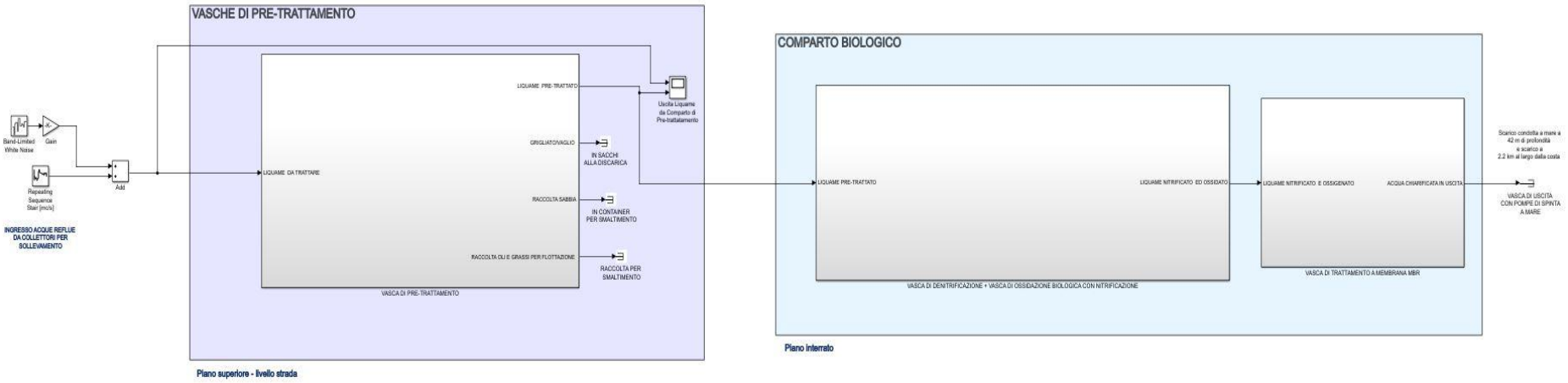
2) QUANTITATIVE

3) GENERAL PURPOSE

Caso di studio (CyCon 2019)

MATLAB® & SIMULINK®

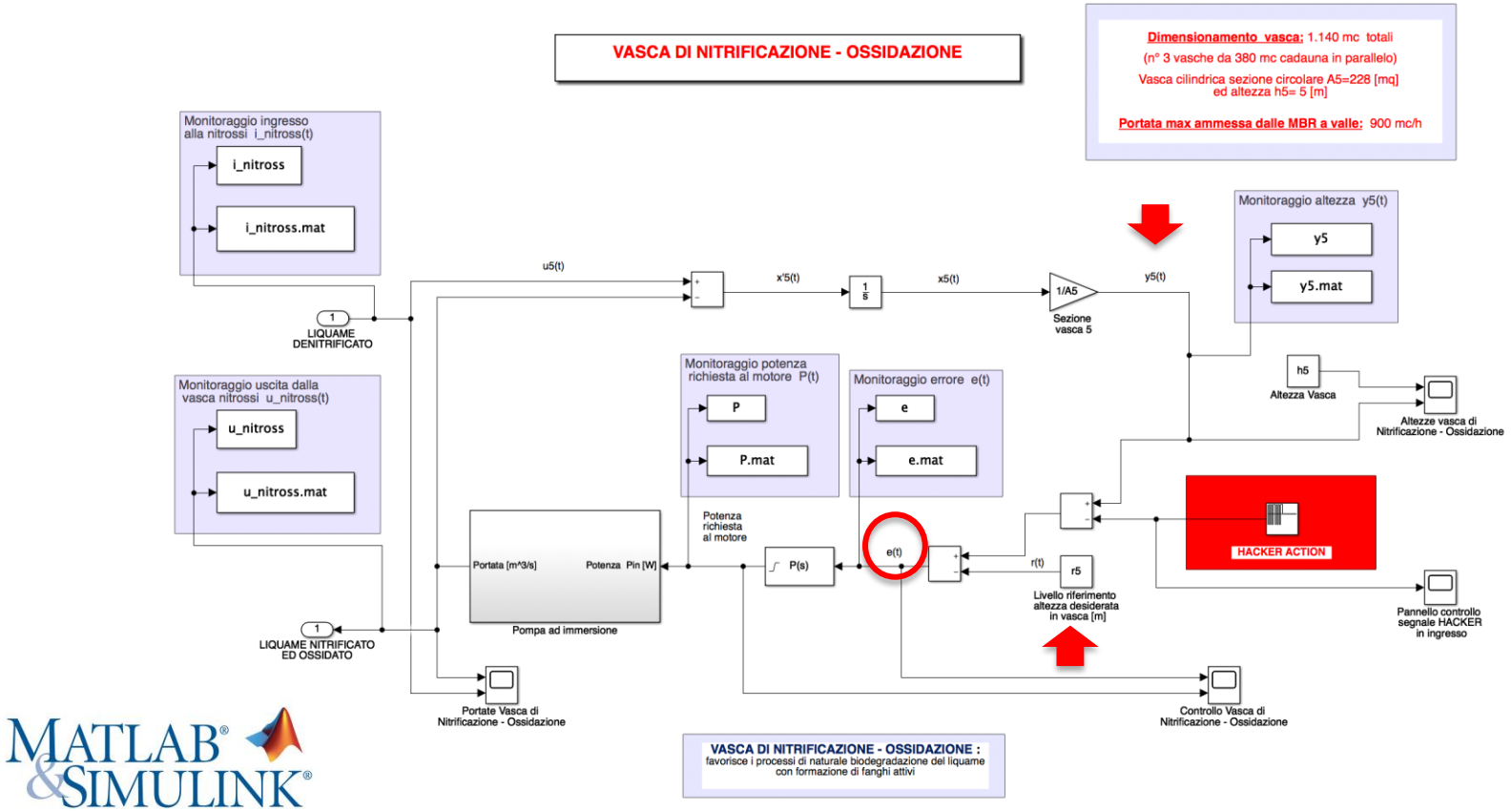
SCHEMA IMPIANTO MBR PER IL TRATTAMENTO DELLE ACQUE REFLUE



- ✓ **Modello basato sui dati reali di un impianto ad elevato livello automazione** (protetto da NDA)
- ✓ **Segnale in ingresso costruito sui dati reali da monitoraggio nel periodo di max portata influente**
- ✓ **Simulazione Montecarlo**

LINEA ARIA
LINEA FANGHI
LINEA ACQUA

La modellazione dell'attacco hacker



MATLAB® & SIMULINK®

Possibili azioni malevole sulla retroazione:

- Cambiamento del ***set point***
- Alterazione del ***segnale in retroazione***
- Cambiamento dei ***parametri del regolatore***

Approccio Metodologico

STEP 1
- Individuazione degli indicatori di performance del sistema

STEP 2
- Identificazione delle misure quantitative *di resilienza* applicabili

STEP 3
- Mappatura dallo spazio delle variabili di stato allo spazio delle prestazioni mediante costruzione delle Figure-Of-Merit (FOM)

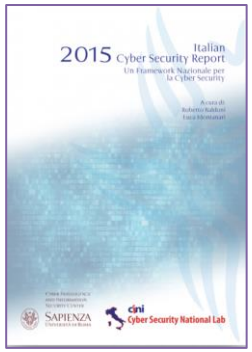
STEP 4
- Calcolo degli indici sulle FOM delle variabili di stato individuate

STEP 5
- Analisi dei risultati ottenuti con i differenti modelli d'attacco

STEP 6
- Individuazione delle configurazioni d'attacco più pericolose
- Compilazione delle relative configurazione d'allerta

Il progetto POR/FESR

FRAMEWORK METODOLOGICO IT/OT NAZIONALE

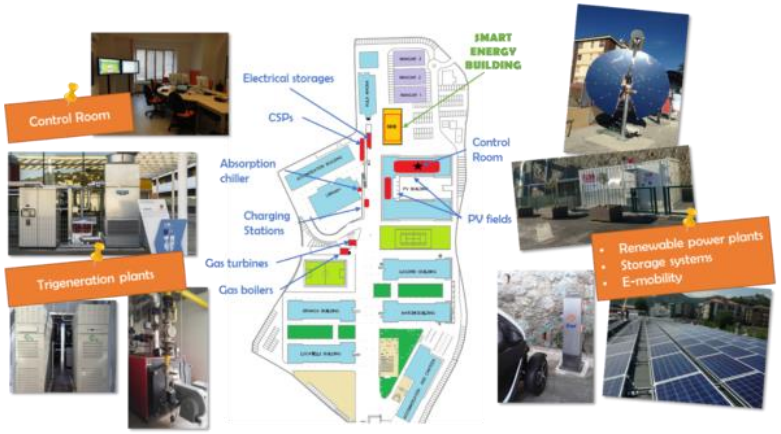


2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019

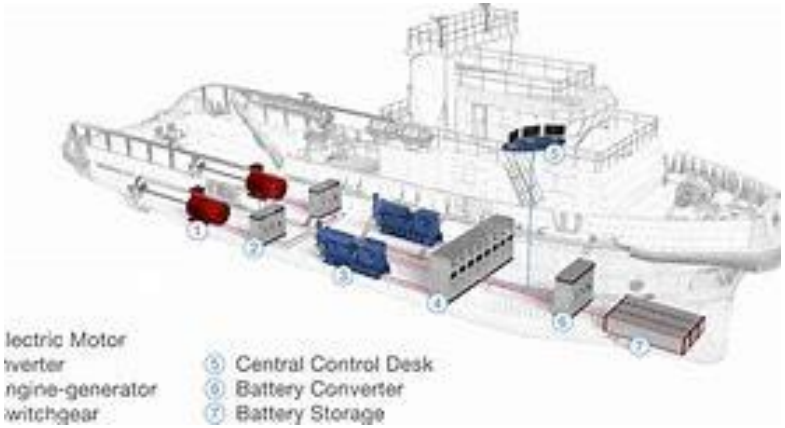
Versione 1.0

Versione 1.1

Il progetto POR/FESR



SAVONA POLYGENERATION MICROGRID



SHIP POWER MANAGEMENT SYSTEM

Ringraziamenti

SEASTEMA

LEONARDO
INGENUITY AT YOUR SERVICE

GFT

ABB

Grazie per l'attenzione !

Circle
Touch your ideas

MAPS
SHARING KNOWLEDGE

CETENA S.p.A.

Consiglio Nazionale delle Ricerche