SECUREWATER

SECUre and REsilient cyber physical systems for SCADA in water systems enhanced by comprehensive analysis capabilities

LUIGI Martino – BVTECH
Gabriele Oliva – NITEL/ Campus Biomedico

CRITIS2017, Lucca 10th October 2017

Intro

Water supply and distribution cybersecurity

SECUREWATER project, presented by BV TECH together with NITEL Consortium and Israeli company IOSIGHT, has been granted funding by the Ministry of Foreign Affair and International Cooperation within the industrial cooperation agreement between Italy and Israel.

The project aims at improving cybersecurity of industrial control system used in the water distribution sector, providing secure communication between SCADA systems and sensors and developing a suite of tools able to detect several type of cyber-attacks on the base of an innovative analysis methodology of data collected from the field.

Intro

ID	Activity name	1° ANNO MESE 01	02	03	04	05	06	07	08	09	10	11	12	2° ANNO MESE 01	02	03	04	05	06	07	08	09	10	11	12
1	**Secure Water project**																								
2	Acceptance of contributions																								
3	**Requirements & Funcional Analysis - WP1**																								
4	Document on State of the Art																								
5	Document on processes and procedures																								
6	Cyber security requirements																								
7	**Design of Technology Solution - WP2**																								
8	SCADA security toolset design																								
9	Data and information fusion																								
10	**Implementation - WP3**																								
11	iGreen installation at NITEL testbed																								
12	Development of Concept for new iGreen Module at NITEL																								
13	Development of secure communication																								
14	**Design and Implementation of Risk**																								
15	Empowerment Procedures																								
16	**System Integration and Release - WP4**																								
17	Engineering of new iGreen Module																								
18	Installation of new iGreen Module and testing at NITEL																								
19	**Demonstration and Validation - WP5**																								
20	Installation of new iGreen Module and testing in Israel																								

Legend:

Attivity

Sub-attivity

Duration: 24 months

What we do - contribution to the project

BVTECH

- Development of Security Layer inside the Cyber Physical Devices through application of ***secure communication*** (including resilient mobile communication) and cryptographic algorithms included and integrated in the Cyber Physical System for critical infrastructure protection.
- Development of Security layer compliant with NIST framework for CPS in Critical Infrastructure, with specific test bed in the water management domain

NITEL (Campus Bio-Medico Unit)

- provide tools and methodologies to ***detect and cope with cyber-physical attack*** or faults.
- Testing the SECUREWATER solution on a water network testbed at University Campus Bio-Medico of Rome.

IOSIGHT

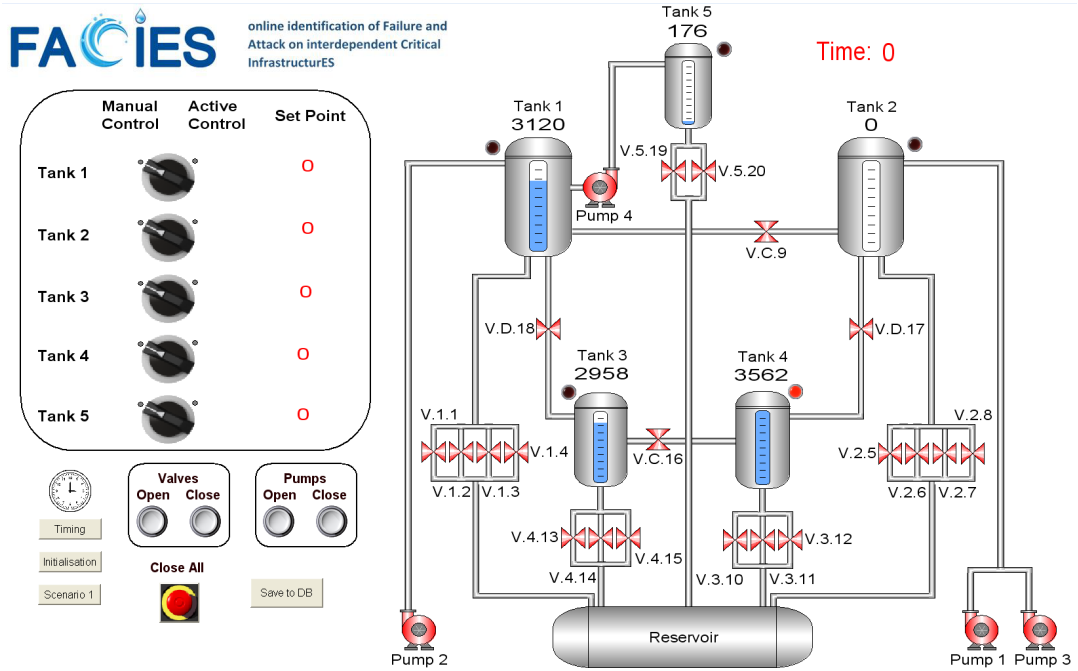
- Improve the data collection/analysis software ***iGreen*** by developing additional modules to provide additional functions at SCADA level for optimizing the water management cycle, e.g., decision support modules, bad data detectors, modules to detect cyber attacks with consequences on the physical process.

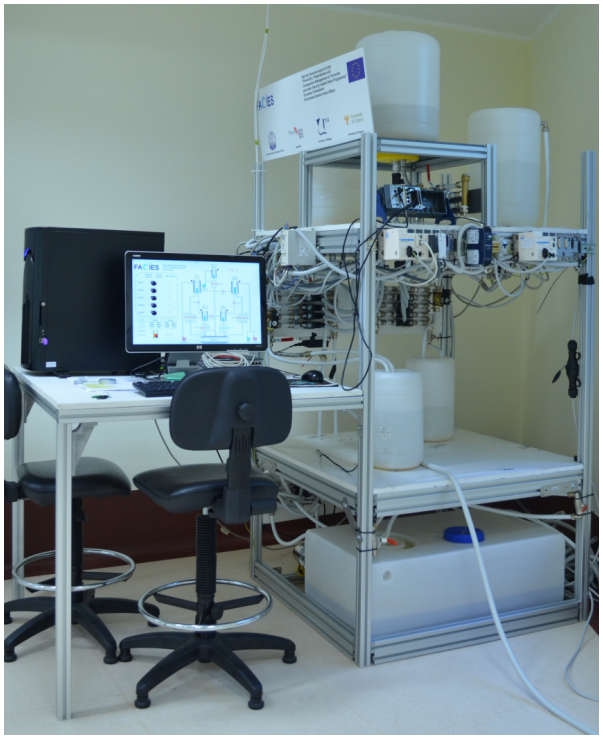
BVTECH/NITEL - Project Highlight

Project Objectives: Develop 3 products

- Tools/Procedures based on BV-Tech secure communication solution, namely **Private Wave**, to secure data exchanged between PLC's and SCADA.
  - Leading Role: BVTech, supported by NITEL and IOSight
- Methodologies to detect and react to man-in-the-middle attacks and malicious data injections in ad-hoc field networks of smart sensors and actuators.
  - Leading Role: NITEL, supported by BVTech and IOSight
- Anomaly detection engine and event management system for operational data above the existing iGreen platform. Leader: IOSIGHT
  - NITEL: Initial Concept Development and support to engineering.
  - IOSIGHT: Engineering of the initial concept into a new iGreen module.
  - BVTECH: support, in particular for the secure communication among the different sub-systems.

Testbed at University Campus Bio-Medico (NITEL)





- Simple water network physical process
- Full functional SCADA system
- Possibility to inject false data and perform several cyber attacks
- Possibility to simulate physical damages by opening manual valves

BV TECH nitel Consorzio Nazionale Interuniversitario per i Trasporti e la Logistica IOSight

iGreen

IOSight
Data Analysis Insightful decisions

- Data collection software (from field, PLC, etc. One way only)
- Possibility to implement decision support systems and real-time indicators based on colelcted data

Testbed in Israel

- The testbed replicates part of Jerusalem water distribution network (in collaboration with Hagion, Jerusalem's water utility)
- The testbed is currently being configured in order to include custom iGreen modules

1 - Private Wave for Secure Water

Secure Communication in Cyber Physical System (CPS)

BVTECH will implement secure mobile communication between the field or peripheral devices connected through mobile network and IACS central modules.

BV TECH engineering staff will evolve and enhance its market leading Enterprise VOIP security suite for secure mobile and fixed voip communication.

Protocols will include:

- SRTP/TLS protocol with 128 bit key length for End to Site encryption with optional point of call registration and interception compliant with local laws.
- ZRTP/S protocol with 256 bit key length for End to End encryption,
- A dedicated server will allow also end-to-end communication, supporting the implementation of secure IoT and CPS devices inside the IACS architecture with specific references to resilience techniques through roaming schemes.

CPS security framework

BVTECH will perform the Identification CPS assets and vulnerabilities of Critical Infrastructures systems and processes, assess risks and develop a specialized frameworks for Security and Risk Management for CPS, with specific reference to CPS for water management and related SCADA systems. This activity will rely on standards such as ISO27001

1 - Private Wave for Secure Water

- Open Source and public technologies, with a security certified and monitored by the biggest worldwide experts in this sector
- EVSS is a secure communications solution for voice and text messages composed by PrivateWave mobile application and PrivateServer
- PrivateWave app, software voice encryption

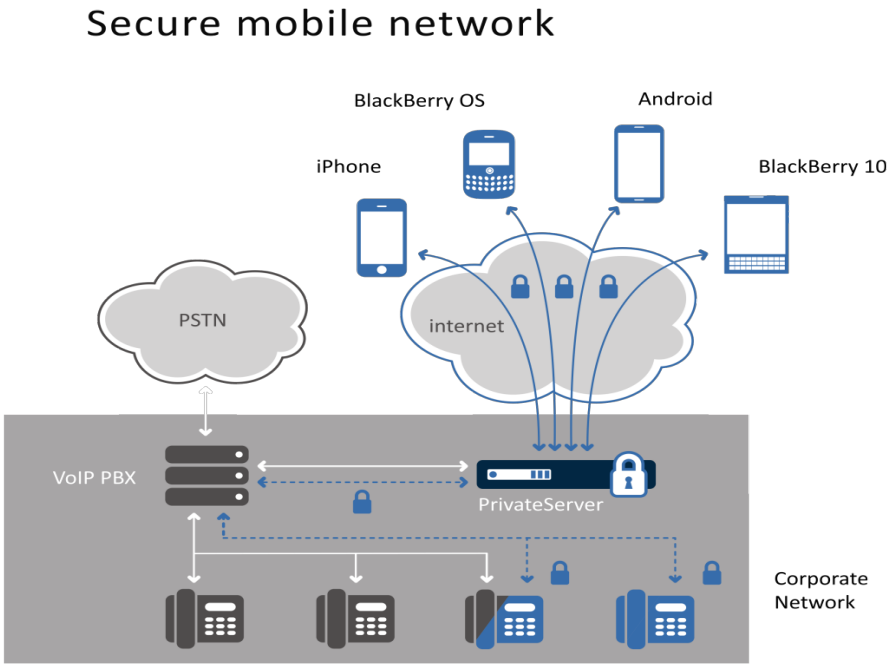
  for Smartphone:
  - Android, iOS, Blackberry
  - VoIP technology on LTE,

    UMTS, EDGE, GPRS, WIFI
- PrivateServer: Linux based secure PBX

  hardened following NSA/Linux guidelines.

  Provided as a virtual appliance to deploy

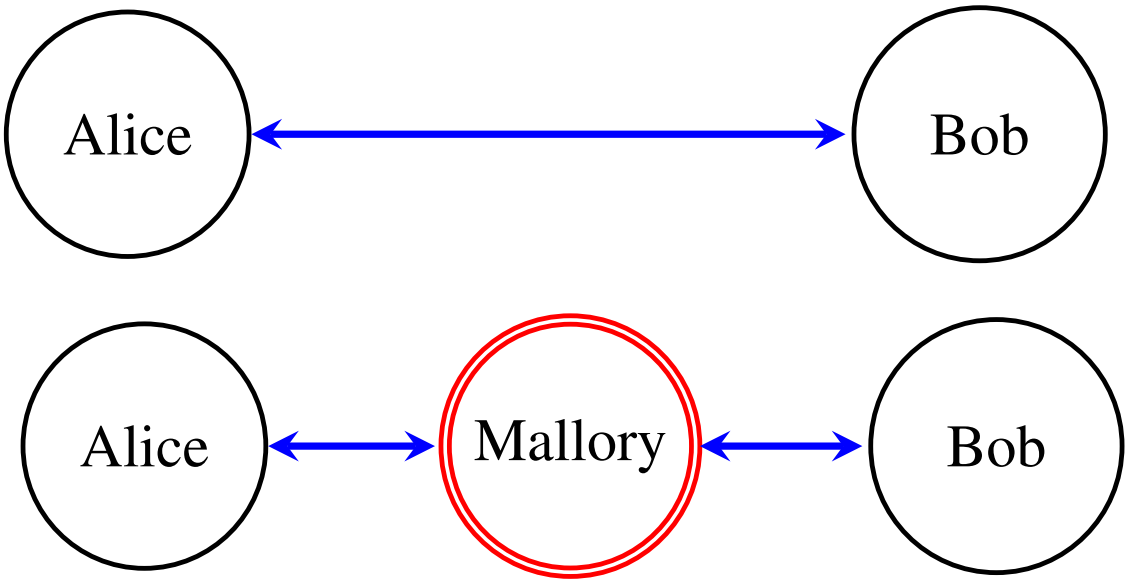
  in cloud or on premise



1 - Private Wave for Secure Water

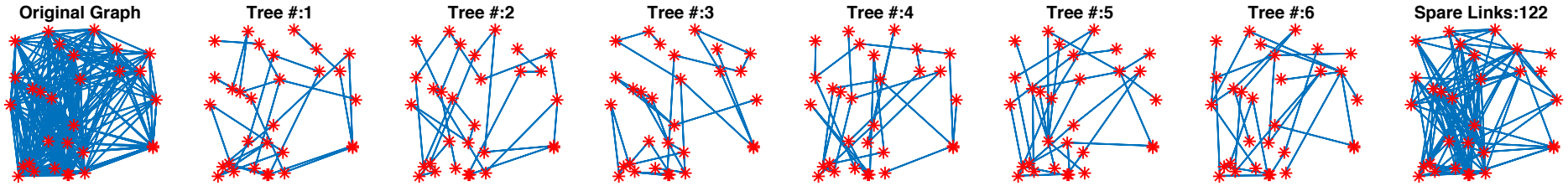
- Two security models for encryption:
  - End-to-Site:
    - between PrivateWave app and PrivateServer, it is available the integration within existing Corporate PBX to extend the secure telephony network
  - End-to-End:
    - Mobile-mobile communications, only caller and callee are able to decrypt voice and messages
- Encryption protocols details:
  - Approved by major standard institutes: NIST/FIPS
  - Key exchange/agreement: RSA, ephemeral Diffie-Hellman (DHE), ephemeral Elliptic Curve Diffie-Hellman (ECDHE)
  - SIP/HTTPS: TLS 1.2 with X.509 certificates
  - Voice and messaging: AES256 with different key exchange method dependent on security model (SRTP/SDES for End-to-Site and ZRTP for End-to-End)

2 – Coping with Man-in-the-middle attacks at field level



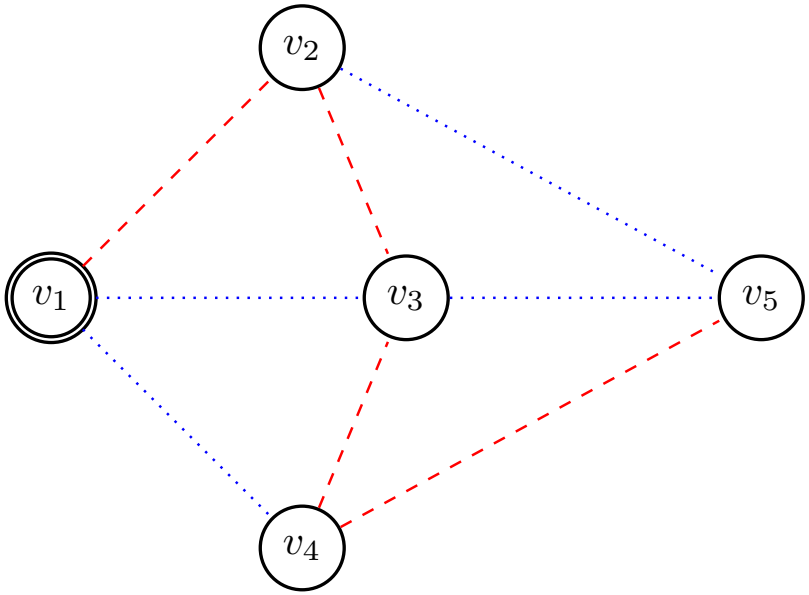
- Ad-hoc network of sensors at field level, no central orchestrator
- Nodes can communicate on a multi-hop basis
- As a consequence of an attack, Mallory becomes the sole interface between Alice and Bob
- Mallory can send false data to Alice and Bob without being noticed

2 – Coping with Man-in-the-middle attacks: Problem



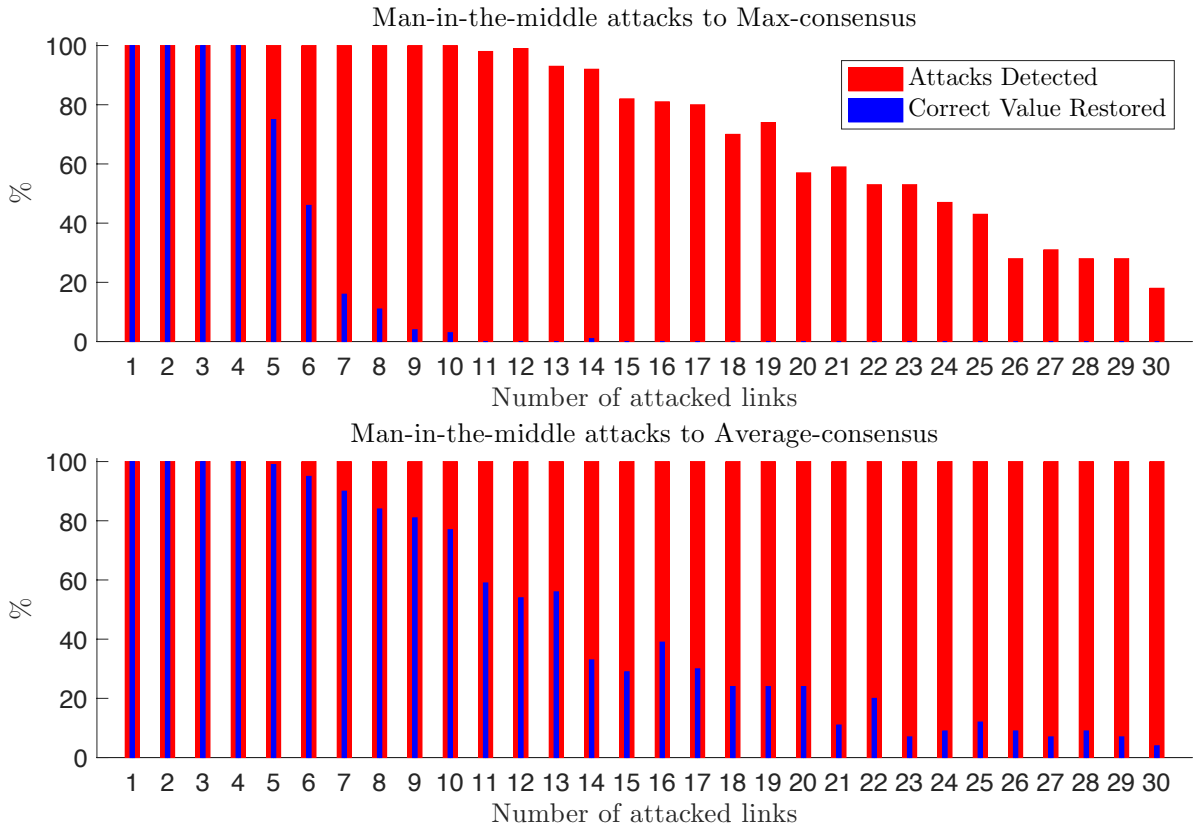
- Partition the network in advance into K edge-disjoint spanning trees
- Nodes communicate in parallel over the K spanning trees
- A single link can compromise at most one spanning tree
- If the majority of spanning trees is not affected the correct message can be identified by majority decision
- We want the nodes to partition the edges in spanning trees with no central coordination → distributed algorithm
- Optimal algorithms to find the maximum number of disjoint spanning trees are not feasible for distributed implementation

2 – Coping with Man-in-the-middle attacks: our algorithm



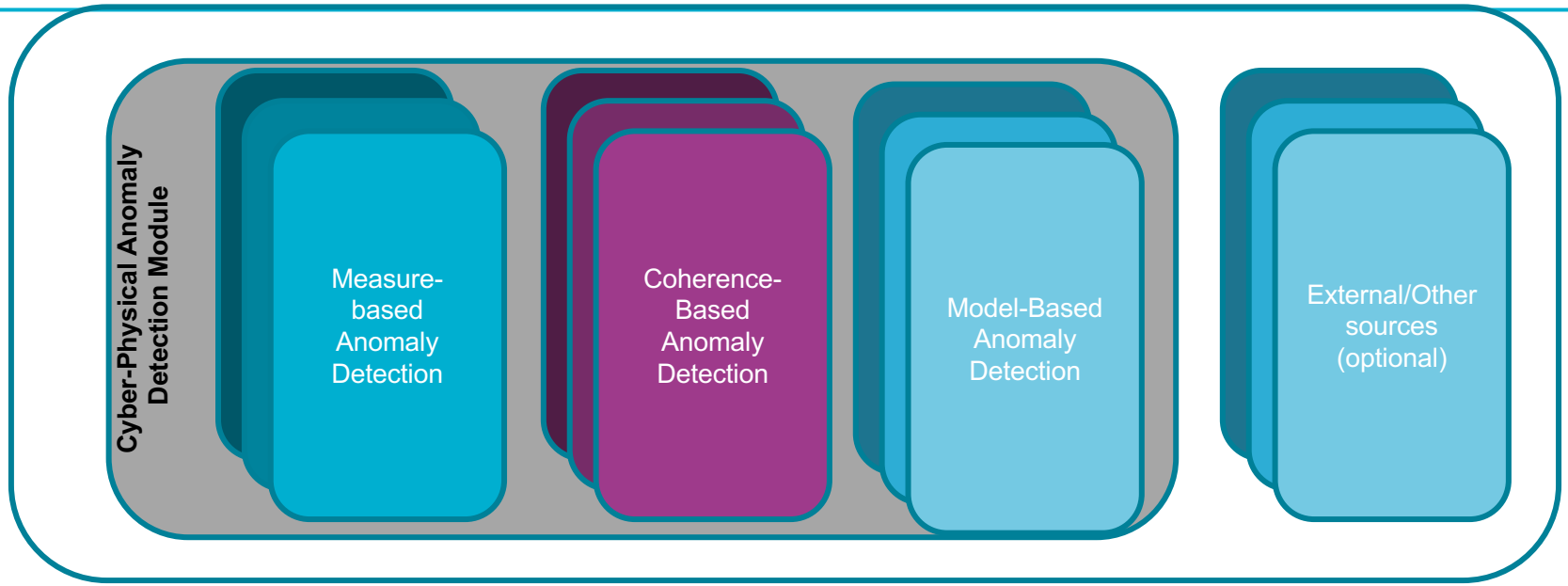
- Construct a spanning tree via depth-first visit
- “remove” the links in the spanning tree
- Construct a spanning tree over the residual graph
- Iterate until the graph is disconnected
- Suboptimal, but finds a good number of spanning trees in practice

2 – Coping with Man-in-the-middle attacks: simulation results



G Oliva, S Cioabă, CN Hadjicostis
Distributed Calculation of Edge-Disjoint Spanning Trees
for Robustifying Distributed Algorithms
against Man-in-the-Middle Attacks
IEEE Transactions on Control of Network Systems, 2017 (in press)

3 - Anomaly detection engine



- Construct a suite of indicators of cyber-physical anomaly
- Measure based (e.g., bad data detector)
- Coherence based (e.g., statistical correlation)
- Model based (e.g., dynamically assessing deviations of the physical model from a real-time dynamic model of the nominal process)

Project's status

- **PRODUCT 1 STATUS**: currently under development, the Private Wave suite is being customized for the testbed at University campus Bio-medico
- **PRODUCT 2 STATUS**: methodology developed and tested in simulation. Ad-hoc sensor network to be interconnected to the testbed is currently under deployment
- **PRODUCT 3 STATUS**: first simple measure-based indicators being tested and incorporated in iGreen framework

Thank you for your attention!

BV TECH nitel Consorzio Nazionale Interuniversitario per i Trasporti e la Logistica IOSight