SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M0 - Course Introduction

Who I am

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

CWC Oulu CENTRE FOR WIRELESS COMMUNICATIONS University of Oulu

GE

ALSTOM Designing fluidity

CYBER CHALLENGE CyberChallenge.IT

MASTER DEGREE IN CYBERSECURITY UNIVERSITY OF PADUA

Publications

- Conference Papers
- Journal Papers
- Book Chapters

Patents

- 5 Patents (US/EP/WO/AU/ES,...)

Doctoral Studies

- Dr. Sc. (Tech)
- University of Oulu (FIN)

Industry

- Railway Signalling R&D
- Telecom Team Leader
- Program Manager
- System/Firmware Designer

Cyber-security

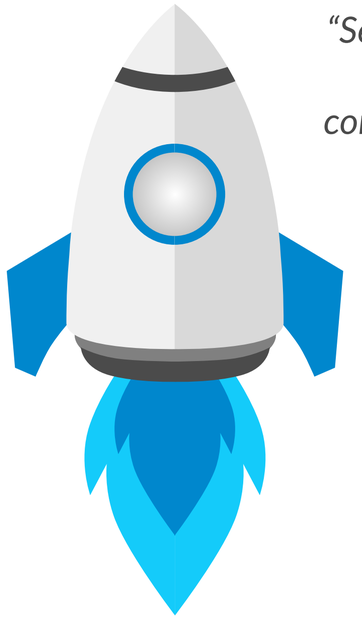
- Italy CyberSec Country Manager
- National Coordinator Cyberchallenge.IT
- Assistant Professor IMT
- Adjunct Professor UniPD

IEEE SENIOR MEMBER

Research Areas

Multilevel Security strategy

"Security engineering as a multidisciplinary field ranging from cryptography and computer science to hardware security and embedded systems".



Physical-layer Security (PLS)

PLS as a combination of **watermarking** and **jamming** receiver through RF, ultrasound and **VLC**

Network Security

L2- L3 network security for critical infrastructure.
Cyber-range as a tool for network security assessment and **education**

Covert Channels

Bit-rate modulation as a new **covert channel attack** against enterprise networks

Federated Learning systems turned into **covert channels** to implement a stealth communication infrastructure.

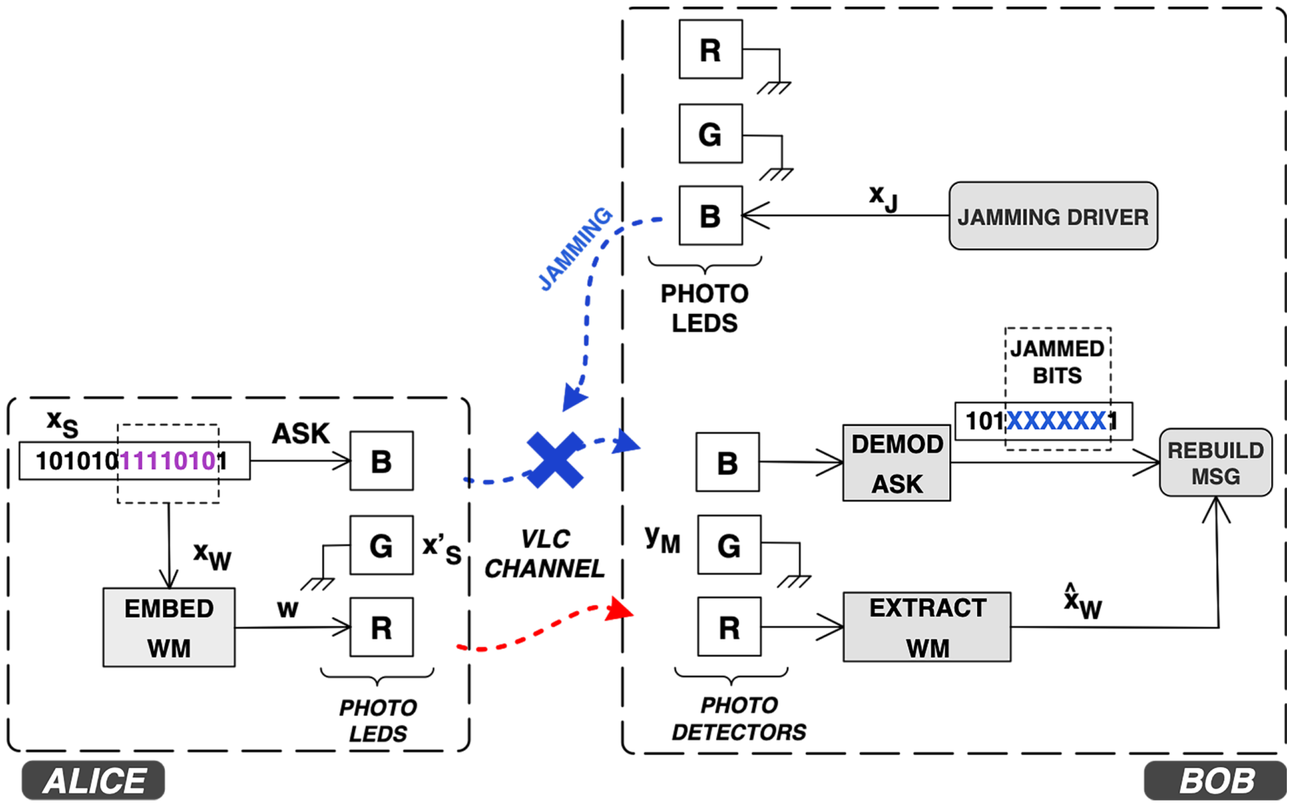
CAN bus Security

Wired WBPLSec to implement an **authenticated key distribution framework for devices communicating through the CAN bus network**

1st step

PLS for 6G Networks*

WATERMARKING AND JAMMING ALGORITHM APPLIED TO VLC



Since VLC is considered an enabling technology for 6G, specific mechanisms are needed to enforce data security.

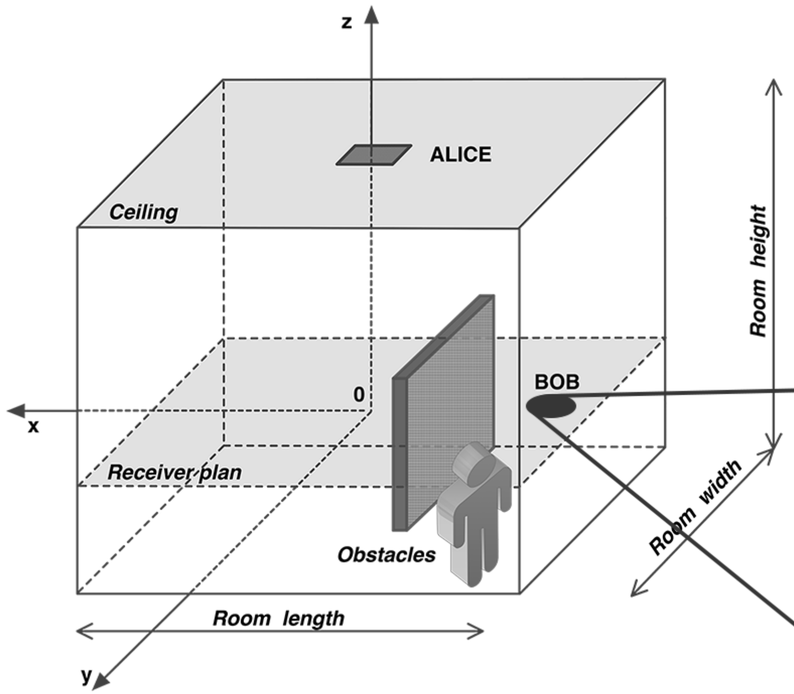
Proposed the approach that aims at obtaining VLC Physical Layer Security (PLS) by combining watermarking with RGB LEDS and jamming.

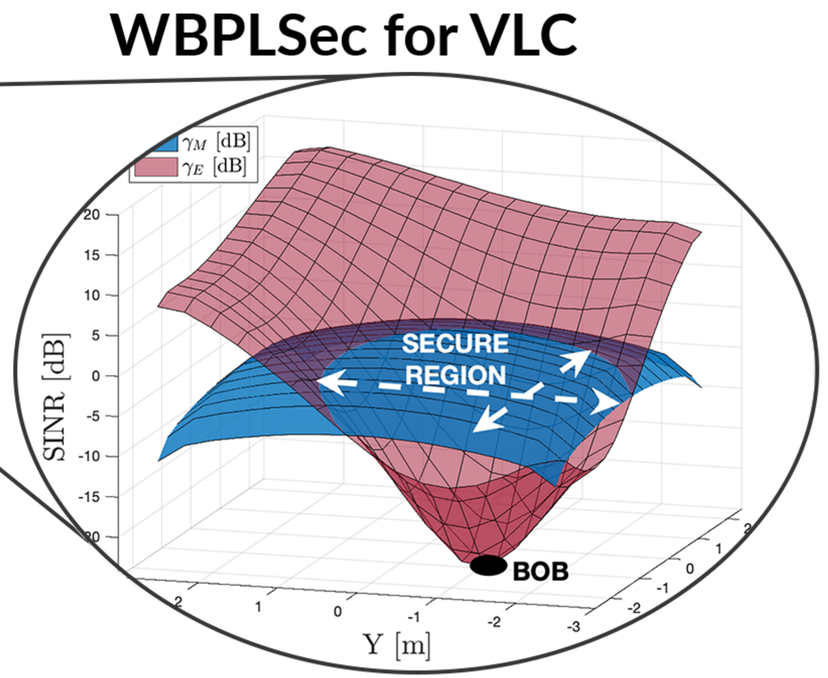
[*] Soderi, S., & De Nicola, R. (2021). 6G networks physical layer security using RGB visible light communications. IEEE Access, 10, 5482-5496.

1st step

PLS for 6G Networks

WATERMARKING AND JAMMING ALGORITHM APPLIED TO VLC





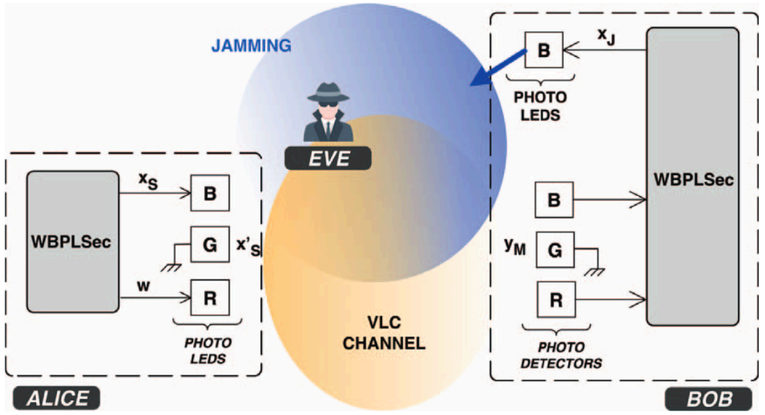
WBPLSec can be used to significantly improve confidentiality in the next generation of wireless communications (6G).

The results offer the possibility of **creating a secure region around the legitimate receiver by leveraging the jamming optical power**.

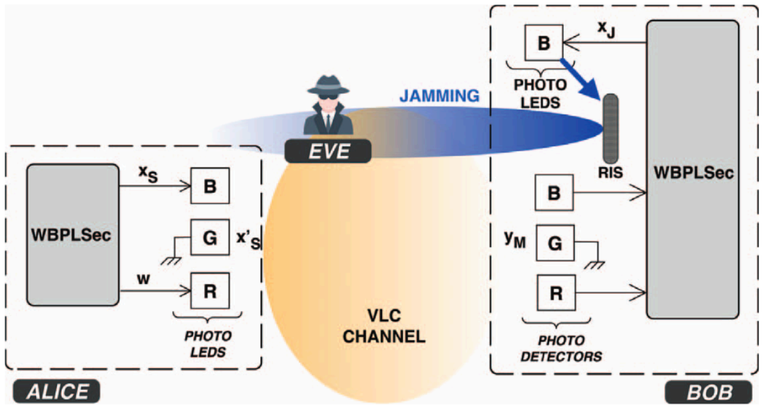
2nd step

PLS with RIS for 6G Networks*

WHAT DOES HAPPEN IF WE ADD A REFLECTIVE INTELLIGENT SURFACE (RIS)?



(a) System model without RIS.



(b) System model with RIS.

The introduction of RIS technology can improve the quality of the received beam.

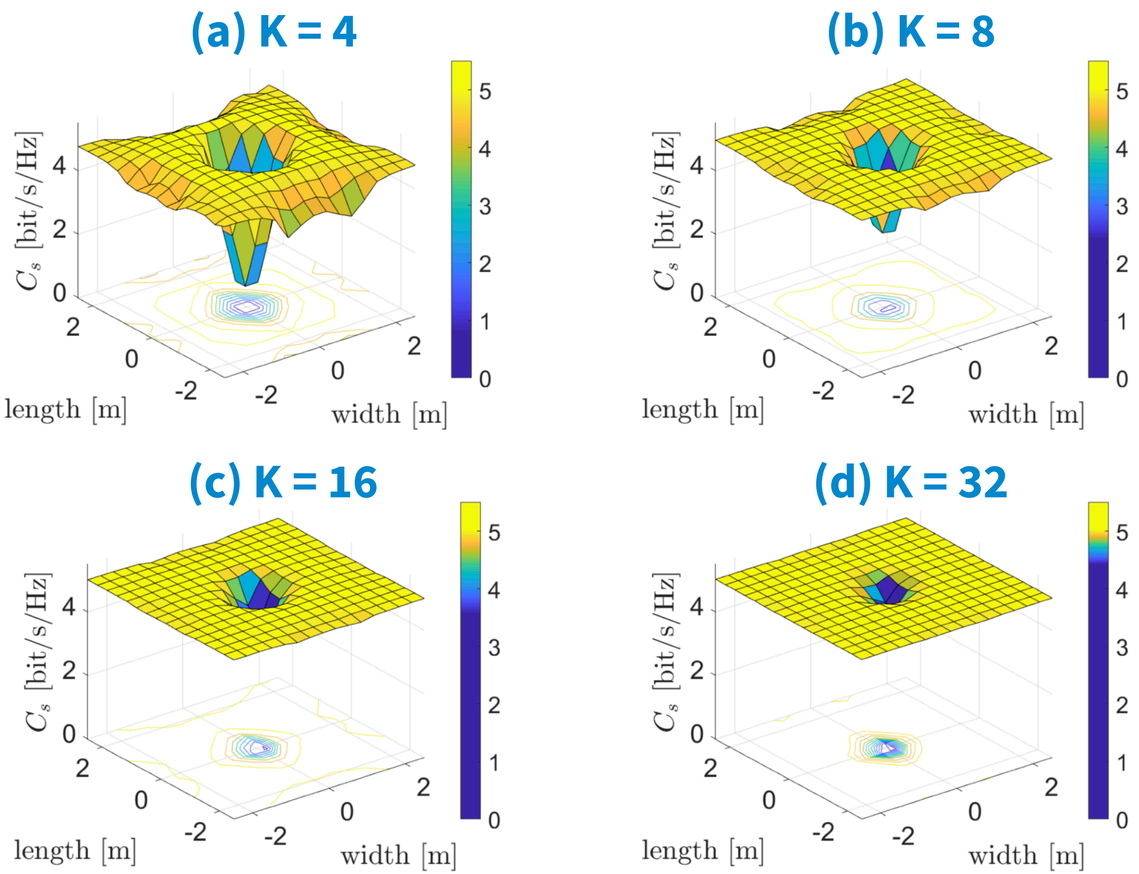
The introduction of RIS technology extends the area where secure communication occurs and that by increasing the number of RIS elements the outage probability decreases.

[*] Soderi, Simone, Alessandro Brighente, Federico Turrin, and Mauro Conti. "VLC Physical Layer Security through RIS-aided Jamming Receiver for 6G Wireless Networks." In 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 370-378. IEEE, 2022.

2nd step

PLS with RIS for 6G Networks

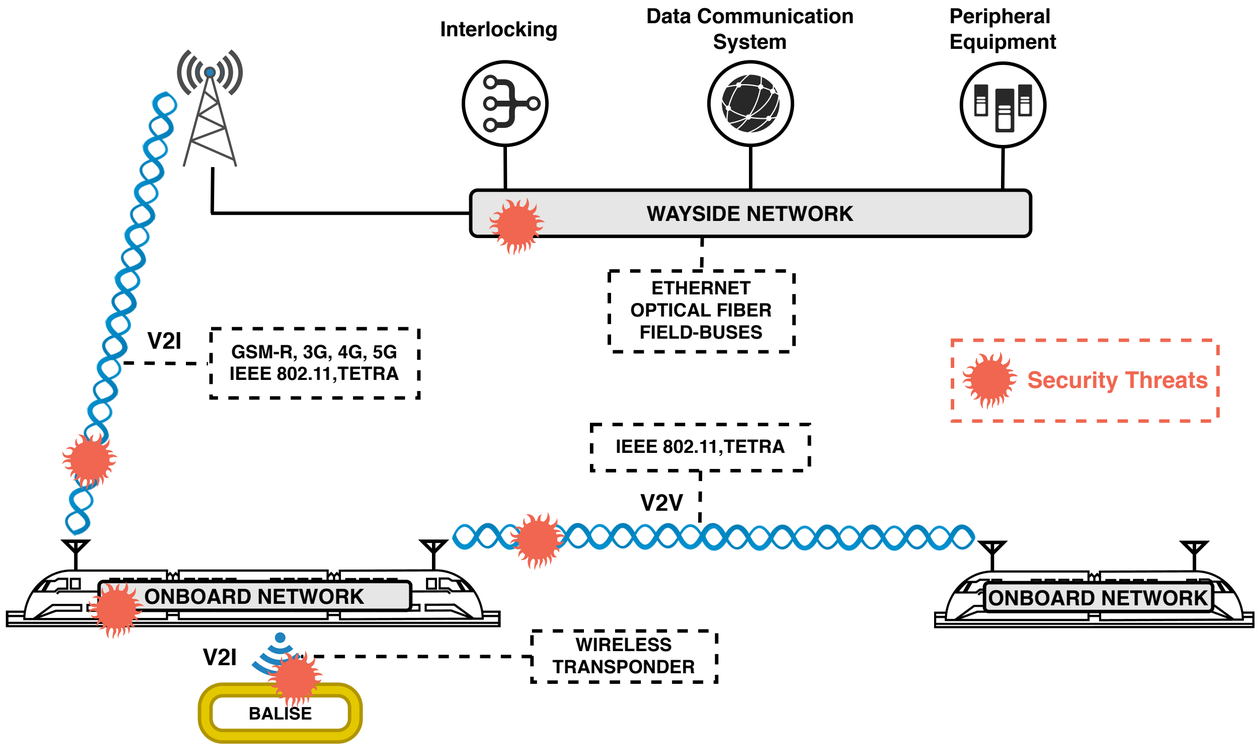
RESULTS WHEN WE KNOW EVE'S LOCATION



- **Secrecy rate** obtained for different Eve locations around the room **when increasing the number K** of RIS elements and considering known Eve locations.
- C_S **increases when we increase the number of RIS' elements.**
- [Weak spot around ALICE]
  This is a **characteristics or weakness of the WBPLSec** algorithm, that is, when EVE is close to the legitimate transmitter and thus away from the BOB jammer the secrecy capacity decreases.

Security Threats in Railway Signalling System

AFFECT THE DATA COMMUNICATION SYSTEM (DCS)



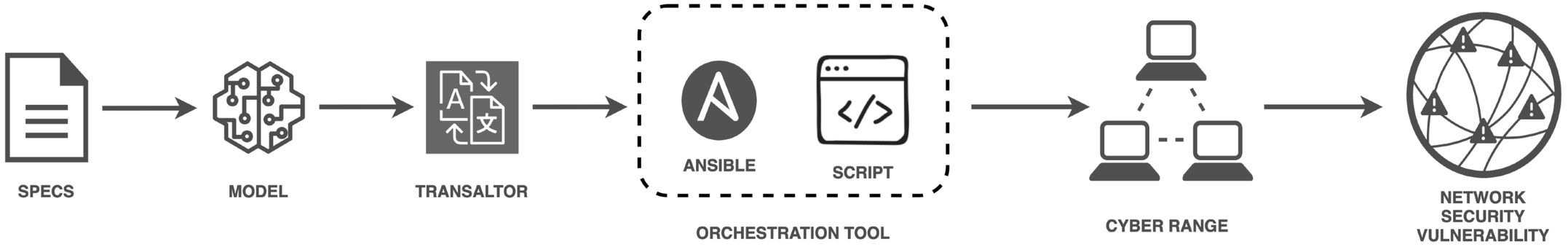
Wireless and wired communications offer new opportunities for development.

Unfortunately, these technologies expose railway signalling systems to **security threats**.

Thus emerges **the need to assess the cybersecurity posture of these complex systems even with new tools such as cyber-ranges.**

[*] Railway cyber-security in the era of interconnected systems: a survey. Soderi, S., Masti, D., & Lun, Y. Z. (2023). IEEE Transactions on Intelligent Transportation Systems.

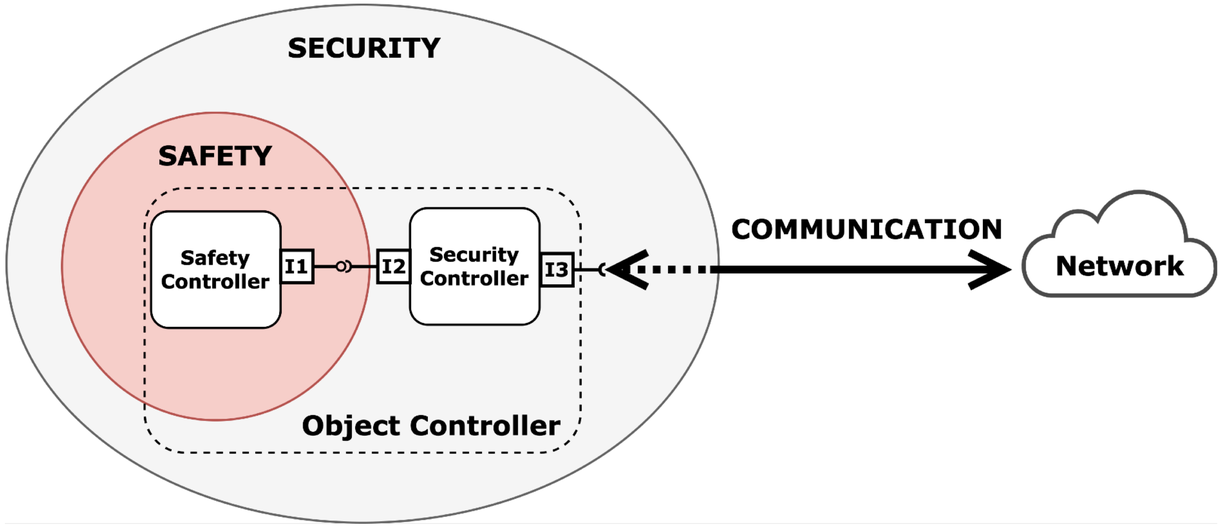
Cyber range: Network Security assessment



- We propose using dedicated cyber ranges as an **enabling technology to perform cybersecurity assessments**. In fact, with **cyber ranges**, we can emulate communication networks in a virtual perimeter and securely test various risk scenarios to verify security requirements and proper policy enforcement.

- Cyber ranges are also helpful for training personnel involved in railway signal installations to make them more aware of cybersecurity risks.

Security and Safety



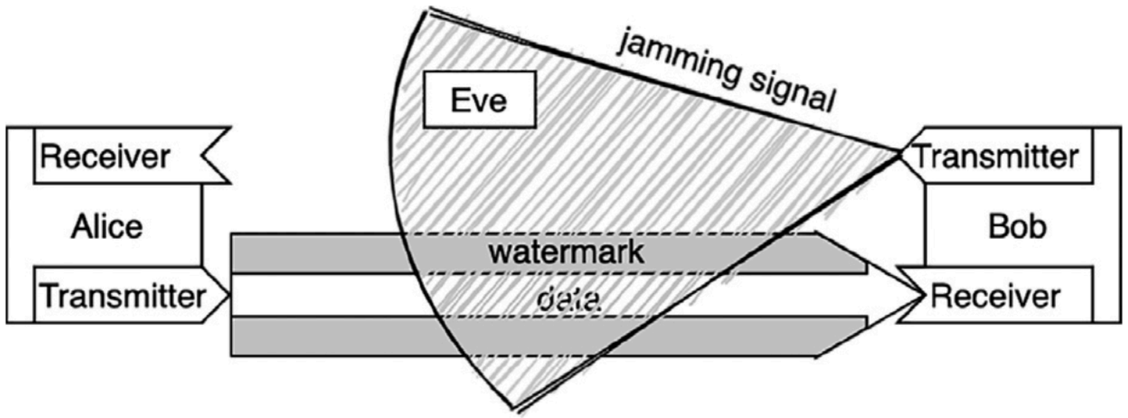
Example of a safety-critical object controller that integrates safety and security aspects. In this approach, the safety aspect functions as an external enclosure that protects the safety function.

- A technical specification (TS 50701) has recently been published that **aims to standardize the integration of cybersecurity into railway safety systems.**

- In railway signaling systems, it is therefore clear that **security requirements must be considered from the very beginning.**

Formal Verification of PLS*

System Model



Requirements characterization

Requirements for implementing WBPLSec.

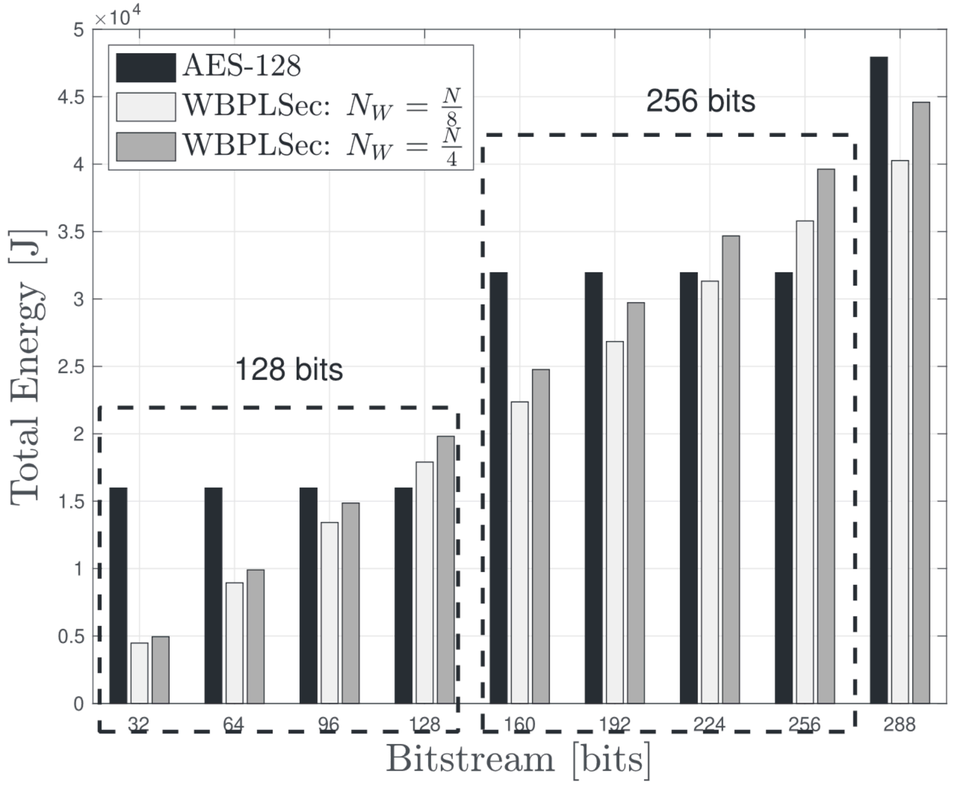
Requirement	Description
Transceivers	The network nodes should be equipped with at least one transmitter and one receiver that can be used in full-duplex.
Channel	The communication channel shall allow for intentional interference during data transmission.
Watermarking	1. The watermarking and the signal hosting it must be statistically independent. 2. The host signal should carry the watermark.
Jamming	1. The intensity of jamming shall be sufficient to destroy the received information. 2. When more jammers are present, their range should not overlap.

We formalized the two physical operators (watermarking and jamming) and we automatically prove that this proposal guarantees confidentiality of communications.

With this contribution we can now easily model protocols that use these PLS primitives on different communication media

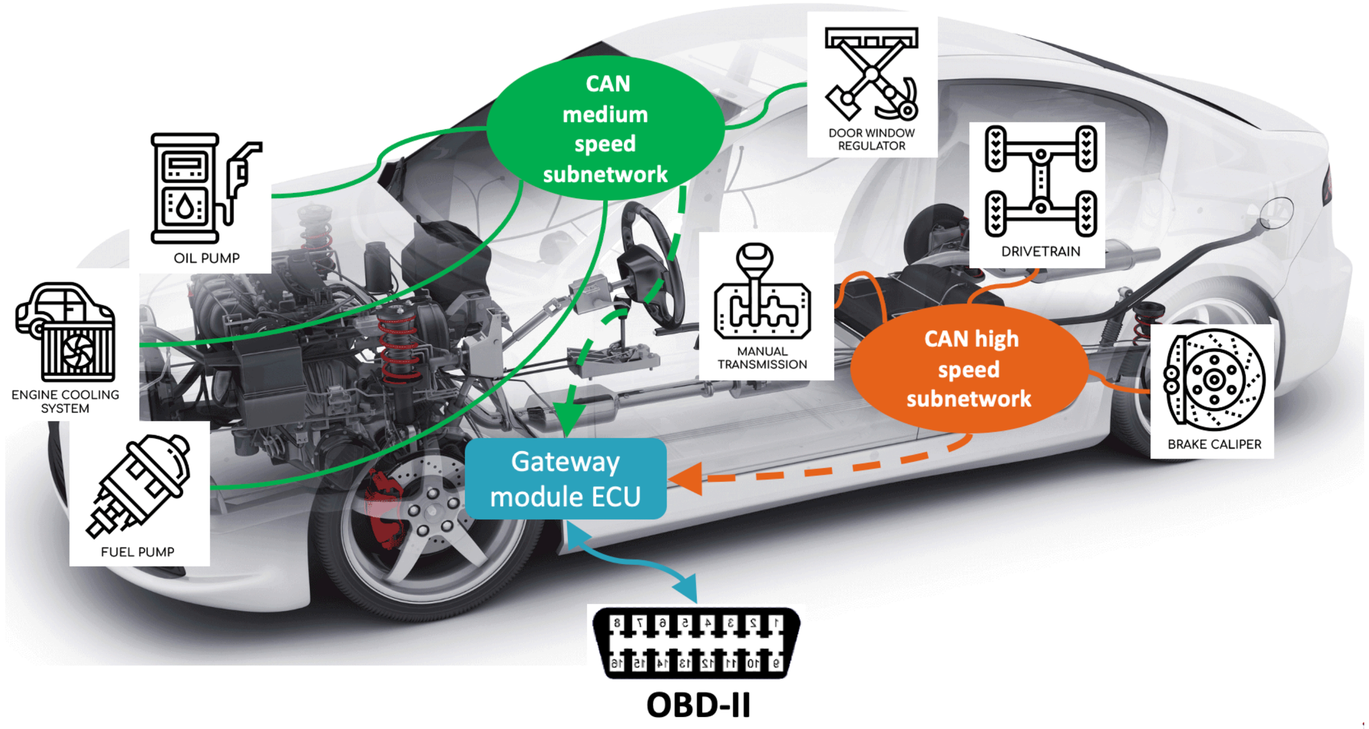
[*] Costa, G., Degano, P., Galletta, L., & Soderi, S. (2023). Formally verifying security protocols built on watermarking and jamming. Computers & Security, 103133.

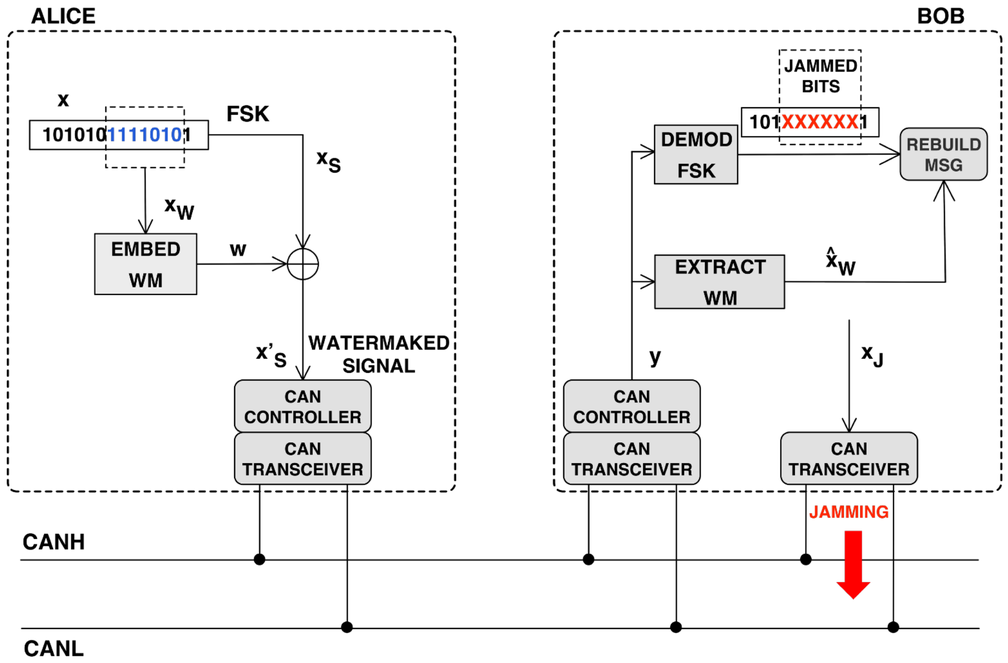
Formal Verification of PLS



We compared the energy consumption of WBLPSec with that consumed by of AES, and show that watermarking and jamming are often cheaper for the pair sender/receiver, and always less demanding for a battery powered sender.

PLS in a CAN bus scenario*

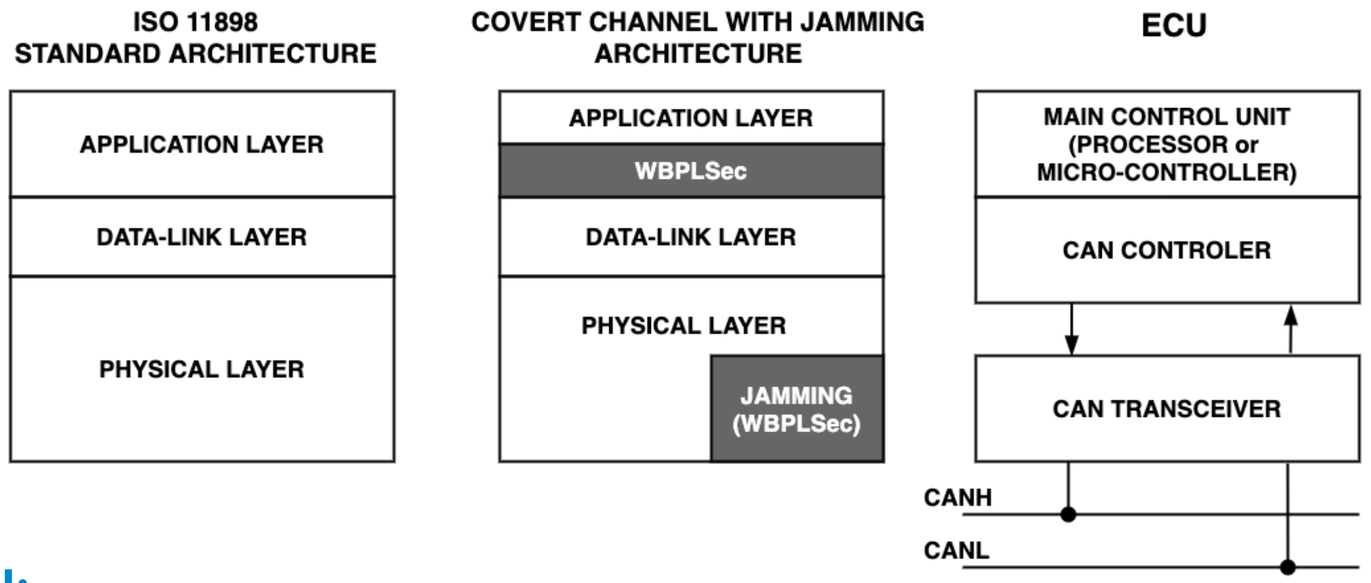




WBPLSec on CAN BUS

[*] Soderi, S., Colelli, R., Turrin, F., Pascucci, F., & Conti, M. (2022). SENECAN: Secure KEy DistributioN OvEr CAN Through Watermarking and Jamming. IEEE Transactions on Dependable and Secure Computing.

WBPLSec on CAN BUS

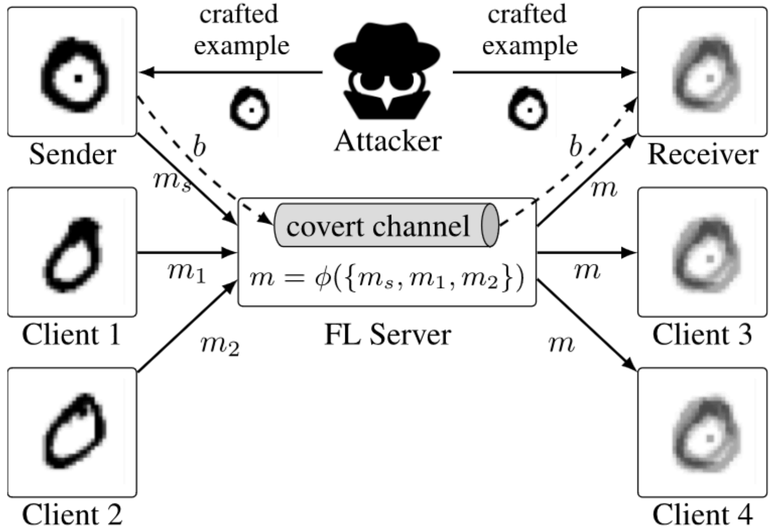


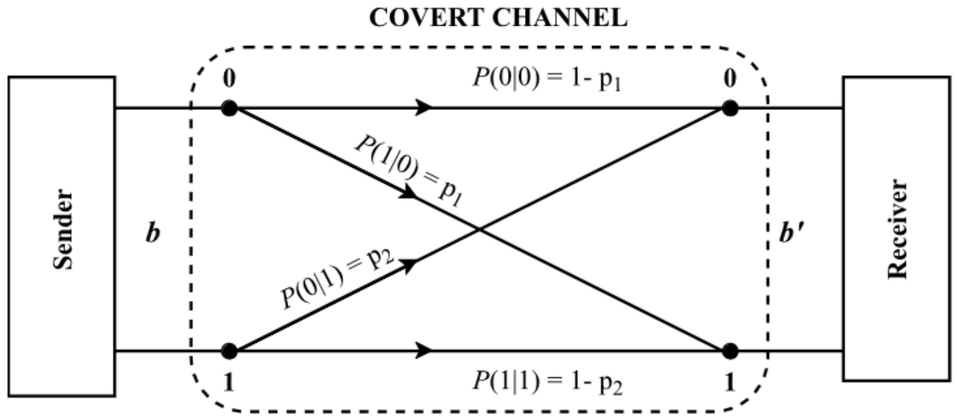
CAN BUS PLS Proposal:

Bump-In-The-Stack (BITS):

- WBPLSec intercepts the bitstream from the application layer as it is passed down to the protocol stack:
  - It watermarks the information (main security part of this protocol), and passes the watermarked bitstream to the data link layer.
- In the second part of the algorithm, the CAN transceiver of the legitimate receiver jams part of the information received
  - For the first time, we implemented the jamming on the wired bus!

Federated Learning System as Covert Channels*



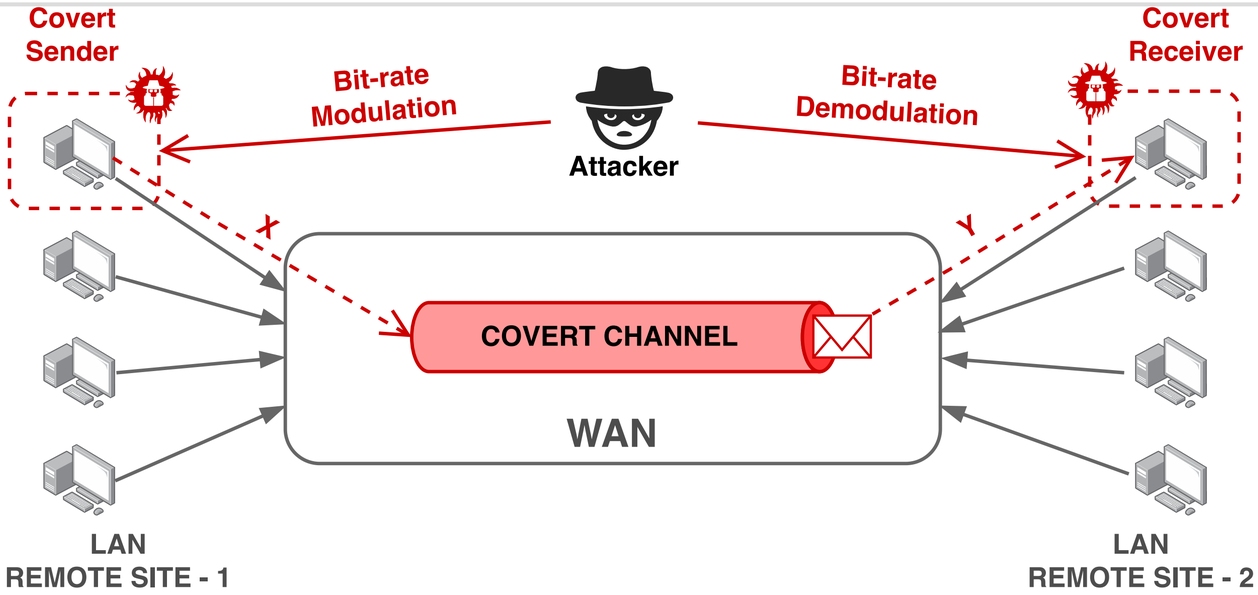


- In a federated learning system, **a malicious sender can poison the global model by sending ad hoc created examples.** Although the effect of poisoning the model is negligible for other participants and does not alter the overall performance of the model, it can be observed by a malicious receiver and used to transmit **an information**.
- We were then able to create, model, and evaluate the performance of this **covert channel, which in fact can be considered as a new attack model threatening FL infrastructures.**

[*] Costa, G., Pinelli, F., Soderi, S., & Tolomei, G. (2022). Turning Federated Learning Systems Into Covert Channels. IEEE Access, 10, 130642-130656.

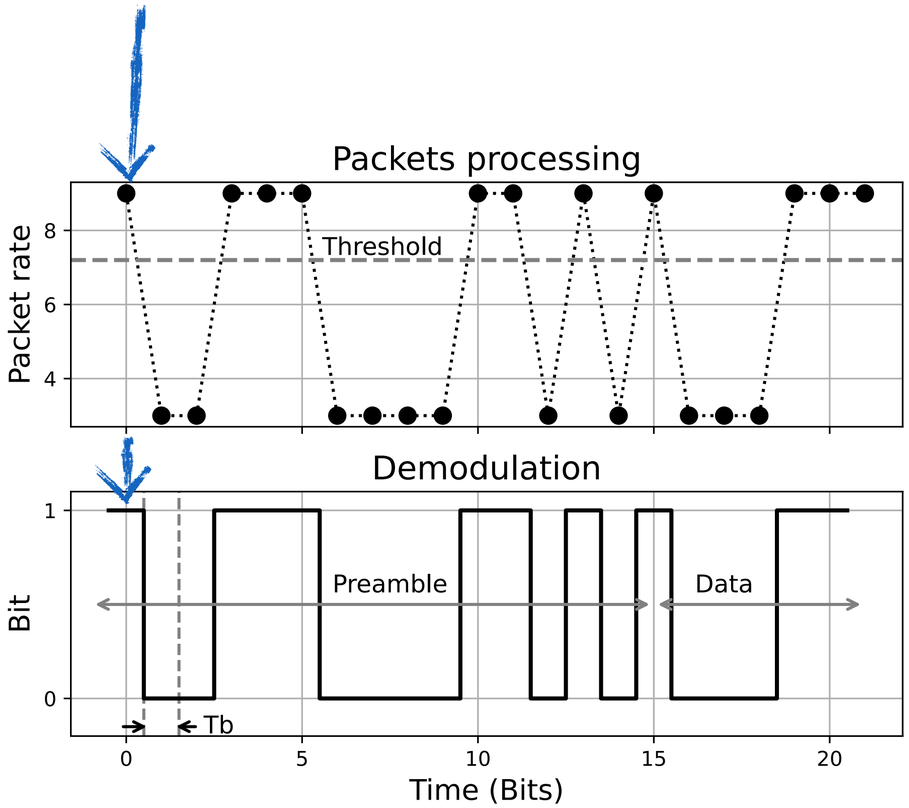
CONNECTION: COvert chaNnel NEtwork attaCk Through bIt-rate mOdulatioN

Attacker Model



- The **corruption** of the two entities can be achieved through **various methods:** supply chain attacks, the use of social engineering techniques, or the exploitation of hardware with pre-installed software/firmware.
- The attacker **does not require special permissions** to carry out this attack once the machines have been infected.
- The covert-sender initiates **covert communication attempts with each IP address within the target network's address space.** Upon successfully detecting this covert communication, the (infected) receiver responds to the sender by modulating its bit-rate.
- The covert-receiver using a **traffic dump can demodulate the encoded information.** By observing the traffic **envelope**, the covert-receiver can recognise, an **amplitude modulation** such as a Pulse Amplitude Modulation (PAM) or an On-Off Keying (OOK).

CONNECTION: COvert chaNnel NEtwork attaCk Through bIt-rate mOdulatioN*



5 bps
Transmission rate

0.9239 bps/Hz
Channel Capacity

[*] CONNECTION: COvert chaNnel NEtwork attaCk Through bIt-rate mOdulatioN. Soderi, S., & De Nicola, R. (2023, December). In International Symposium on Emerging Information Security and Applications (pp. 164-183). Singapore: Springer Nature Singapore.

Selected Publications

- CONNECTION: COvert chaNnel NEtwork attaCk Through bIt-rate mOdulatioN. Soderi, S., & De Nicola, R. (2023, December). In International Symposium on Emerging Information Security and Applications (pp. 164-183). Singapore: Springer Nature Singapore.
- Railway cyber-security in the era of interconnected systems: a survey. Soderi, S., Masti, D., & Lun, Y. Z. (2023). IEEE Transactions on Intelligent Transportation Systems.
- Formally verifying security protocols built on watermarking and jamming. Costa, G., Degano, P., Galletta, L., & Soderi, S. (2023). Computers & Security, 103133.
- VLC Physical Layer Security through RIS-aided Jamming Receiver for 6G Wireless Networks. Soderi, Simone, Alessandro Brighente, Federico Turrin, and Mauro Conti. In 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 370-378. IEEE, 2022.
- SENECAN: Secure KEy DistributioN OvEr CAN Through Watermarking and Jamming. Soderi, S., Colelli R., Turrin F., Pascucci F. and Conti M. in in IEEE Transactions on Dependable and Secure Computing, June 2022
- 6G Networks Physical Layer Security Using RGB Visible Light Communications. Soderi, S.; De Nicola, R. in IEEE Access vol. 10, pp. 5482-5496. January 2022
- Enhancing Security in 6G Visible Light Communications. Soderi, S. 2020 2nd 6G Wireless Summit (6G SUMMIT). March 2020
- Acoustic-Based Security: A Key Enabling Technology for Wireless Sensor Network. Soderi, S. International Journal of Wireless Information Networks, 27(1): 45–59. nov 2019
- Cybersecurity Assessment of the Polar Bluetooth Low Energy Heart-Rate Sensor. Soderi, S. 14th EAI International Conference on Body Area Networks. October 2019
- Physical layer security based on spread-spectrum watermarking and jamming receiver. Soderi, S.; Mucchi, L.; Hämäläinen, M.; Piva, A.; and Iinatti, J. Transactions on Emerging Telecommunications Technologies, 28(7). 2017
- Performance and security evaluation of intra-vehicular communication architecture. Liyanage, M.; Kumar, P.; Soderi, S.; Ylianttila, M.; and Gurtov, A. 2016 IEEE International Conference on Communications Workshops, ICC 2016,302-308. 2016
- Near-field measurements for safety related systems and jamming attack. Soderi, S.; Papini, M.; Iinatti, J.; and Hämäläinen, M. Progress In Electromagnetics Research B, 62(1): 289-302. 2015
- Signal fingerprinting in cognitive wireless networks. Soderi, S.; Dainelli, G.; Iinatti, J.; and Hämäläinen, M. Proceedings of the 2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CROWNCOM 2014,266-270. 2014
- An experimental evaluation of WiFi-based vehicle-to-vehicle (V2V) communication in a tunnel. Viittala, H.; Soderi, S.; Saloranta, J.; Hämäläinen, M.; and Iinatti, J. IEEE Vehicular Technology Conference. 2013
- Emulation of secure Wi-Fi communication: A performance gap analysis against a virtual test-bed. Soderi, S.; Viittala, H.; Saloranta, J.; Mancini, A.; Hämäläinen, M.; and Iinatti, J. 2013 13th International Conference on ITS Telecommunications, ITST 2013,226-231. 2013

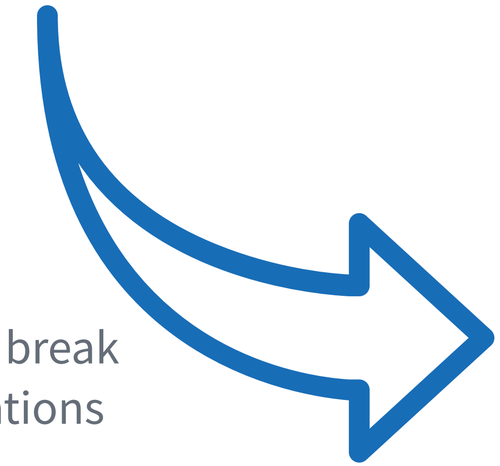
https://scholar.google.it/citations?hl=it&user=rlwSaycAAAAJ&view_op=list_works&sortby=pubdate

Course program

1. **Basic Concepts;**
2. **Planning for Cybersecurity;**
3. **Cybersecurity Operations and Management;**
4. **Security Assessment and use cases;**
5. **Certification and Frameworks for Organizations and management systems;**
6. **Certification of products and technologies;**
7. **Frameworks that describe the competencies;**
8. **Certification of people;**
9. **Most common Certifications available on the market;**
10. **Audit techniques and approach examples.**

Course program

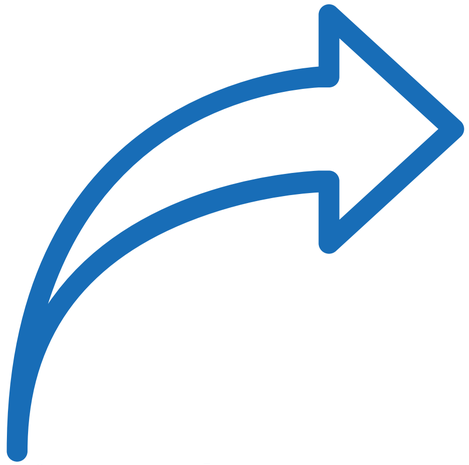
1. **Basic Concepts;**
2. **Planning for Cybersecurity;**
3. **Cybersecurity Operations and Management;**
4. **Security Assessment and use cases;**



until about the break
for Easter vacations

Simone Soderi
[24 h = 3CFU]

Course program



Antonio Belli
[24 h = 3CFU]

5. **Certification and Frameworks for Organizations and management systems;**
6. **Certification of products and technologies;**
7. **Frameworks that describe the competencies;**
8. **Certification of people;**
9. **Most common Certifications available on the market;**
10. **Audit techniques and approach examples.**

Useful Info

1. **Course Calendar:**
   - Start: 26/02/2024
   - End: 14/06/2024

2. **Course Schedule:**
   - Monday 10:30 - 12:30
   - Friday 10:30 - 12:30

3. **Course delivery method: *ONLY IN PRESENCE***
   - Classrooms:
     - ➡ DM 2AB/40 [Torre Archimede]

4. **Academic calendar and major deadlines 2023-2024**
   - Calendar of this course 2023/2024
   - Didactic activities are suspended from 29.03.2024 to 02.04.2024

Goal

1. **The course deals with**
   - the **assessment** of cyber risks that can damage a corporate information system;
   - the **methodologies** to mitigate these risks;
   - the necessary **countermeasures** to be applied with the aim of making the company or public institution secure from an IT point of view.

2. **Students will be introduced to**
   - principles **concepts**, and **practices** for governing, managing, and auditing cybersecurity in accordance with international standards;
   - generally accepted professional **best practices**, **certifications** and **reference frameworks**.

3. **Students will develop**
   - the skills to **plan** and **manage** the security of information systems and know the different alternatives while identifying security risks;
   - the **knowledge on the work context** related to information security, particularly on certifications concerning organisations, technologies, skills, and people, with an overview of the main reference frameworks.

Study materials

1. **Course slides**
   - Available on Moodle
2. **Book**
   - Effective Cybersecurity: A Guide to Using Best Practices and Standards, 2019, Stallings, W.
3. **Optional supplementary readings**
   - CyBok v.1.1 - The Cyber Security Body of Knowledge, 2021
     - https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Exam

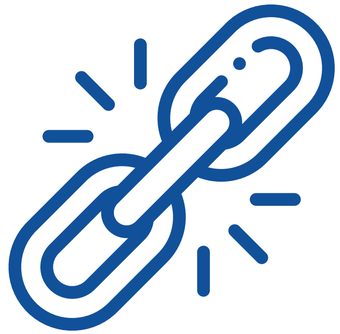
1. **What**
   - Students will take an exam at the end of the course. The final exam covers all material for the semester.
   - The examination format will be explained during the course

2. **When**
   - Examination dates will be announced during the course.

Links

1. **Course 2023/24**
   - Syllabus:
     - https://didattica.unipd.it/off/2023/LM/SC/SC2542/000ZZ/SCQ0089517/N0
   - Moodle:
     - https://stem.elearning.unipd.it/course/view.php?id=8423#section-0

2. **Contacts**
   - Simone Soderi simone.soderi@unipd.it



Questions?

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M0 - Course Introduction

Thanks for your attention!