Deterministic Ethernet Security

Edin Arnautovic, TTTech

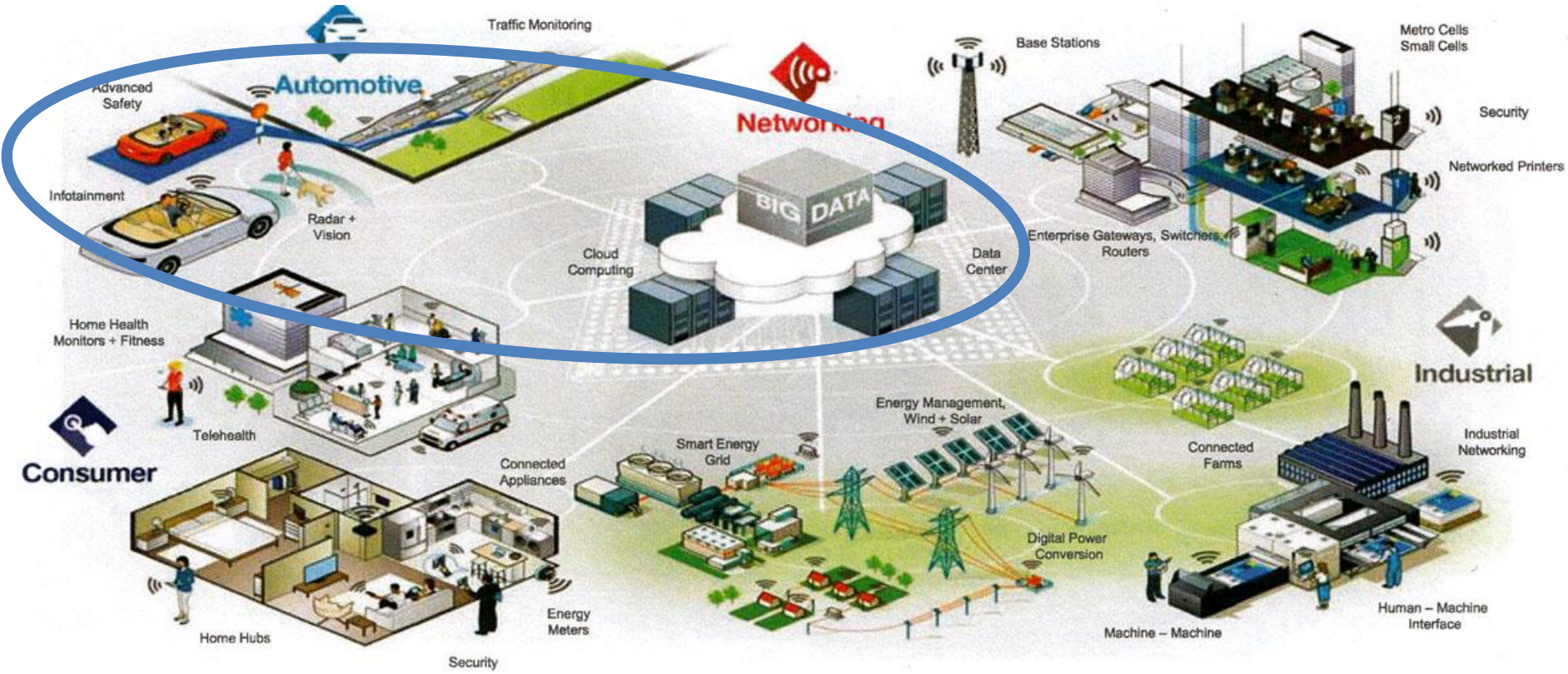
HiPEAC
SAFURE Workshop
22th January 2018
Manchester, UK

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

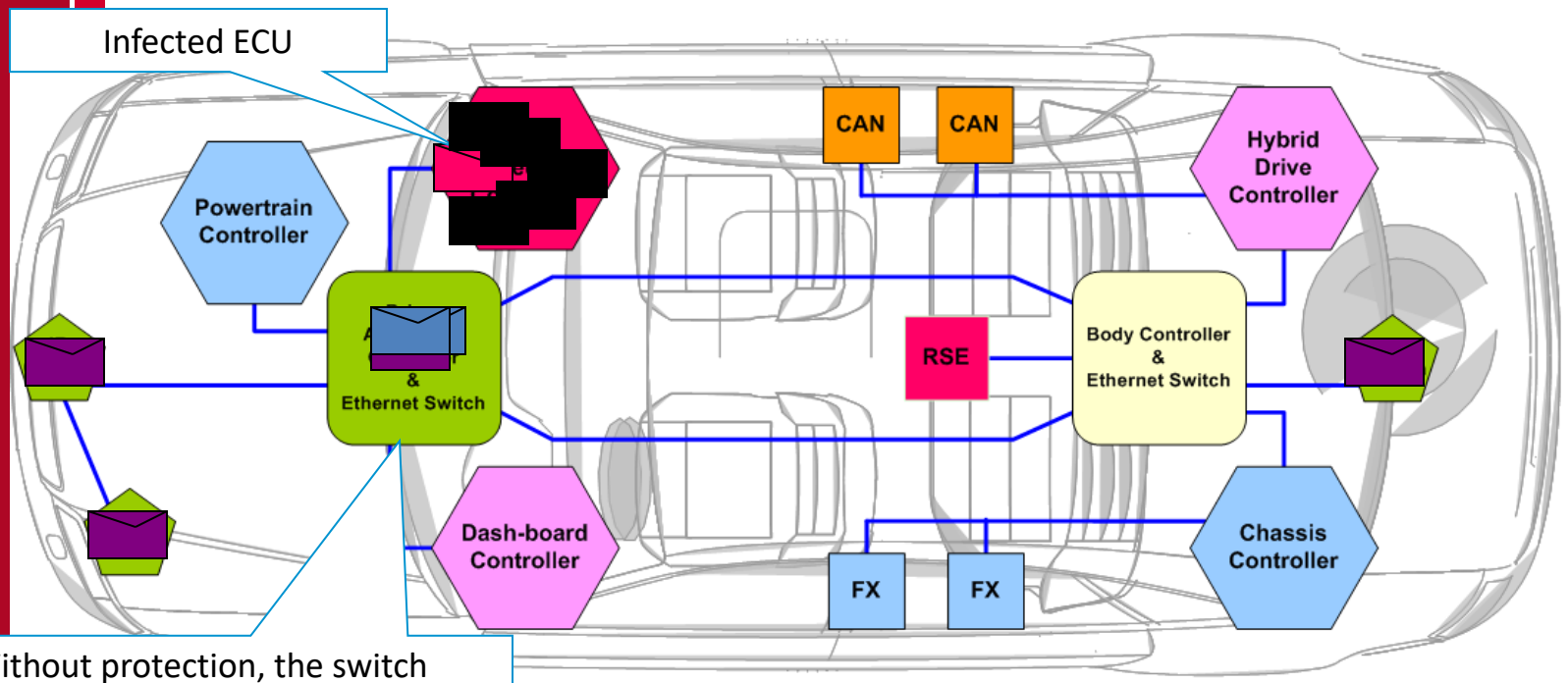
SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems

Motivation for Automotive Ethenet Security



SAFURE

Motivation for Automotive Ethernet Security II



Without protection, the switch forwards all frames from the attack.

At some magnitude of attack, the switch starts loosing frames from other, independent applications.

Overview

- MAC Level Encryption for Deterministic Ethernet
  - Overcomming potential issues with MACSec
  - Overhead of IEEE 802.1X
  - Nececery renewal of Secure Assiciation Key (SEK)
  - → New solution based on Vernam Principle
- Common Criteria for Automotive Ethernet
  - Common Language and Best Practices

SAFURE

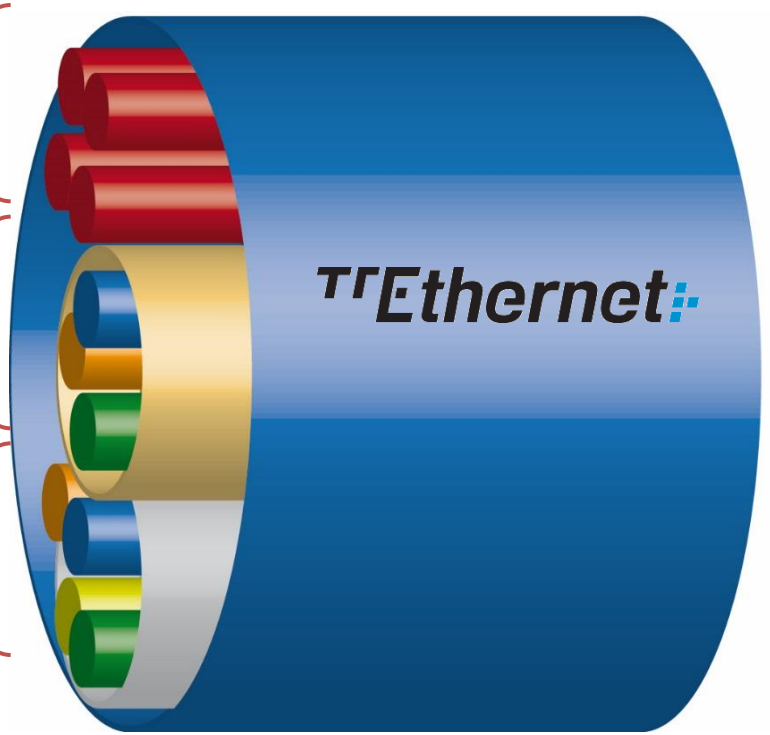
TTEthernet & Security

- Goal of Deterministic Ethernet: make Ethernet better suitable for real-time and fault-tolerant applications

Real-Time & Determinism
- SAE AS6802 clock synch (1588)
- Real-time control, ultra-low latency
- Safety systems

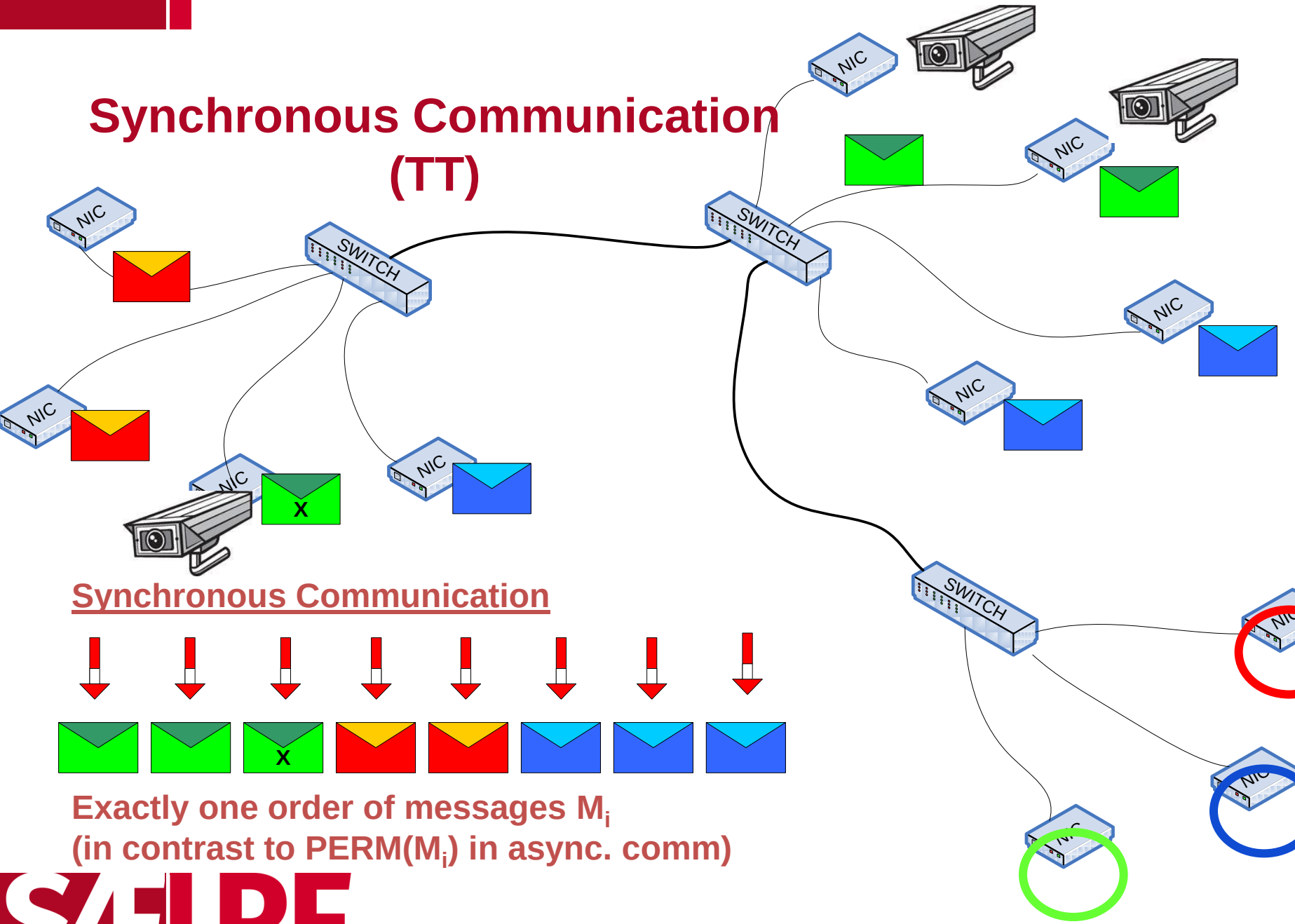
Streaming
- AVB / ARINC 664
- Audio/video
- Sensor fusion

Ethernet (IP)
- IEEE 802.3
- compatible with standard traffic



SAFURE

Synchronous Communication (TT)



Synchronous Communication

Exactly one order of messages M_i
(in contrast to PERM(M_i) in async. comm)

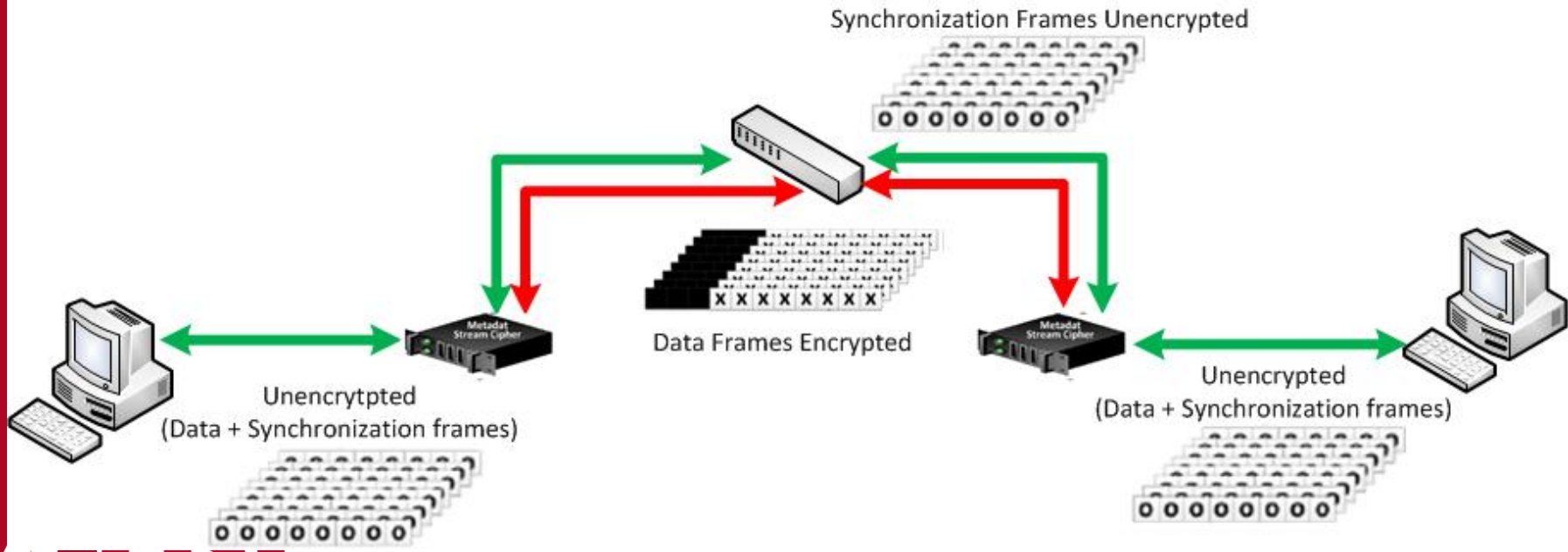
MAC Level Encryption - Goals

1. Secure end-to-end data flow
2. Maintain determinism, minimize impact on real-time properties
   - minimal latency increase
   - avoid additional jitter
   - Line-speed performance (100Mbps/1Gbps)
3. Metadat Scrambler (MDS) simplfies the design of stream ciphers
   1. Based on XOR-ing of incoming data by pseudorandom values
   2. Vernam Principle with one-time pad (per Ethernet frame)
   3. Use of Dynamic Feedback Shift Registers
   4. Advantage of stream cipher: speed of transformation→ algorithms are linear in time and constant in space

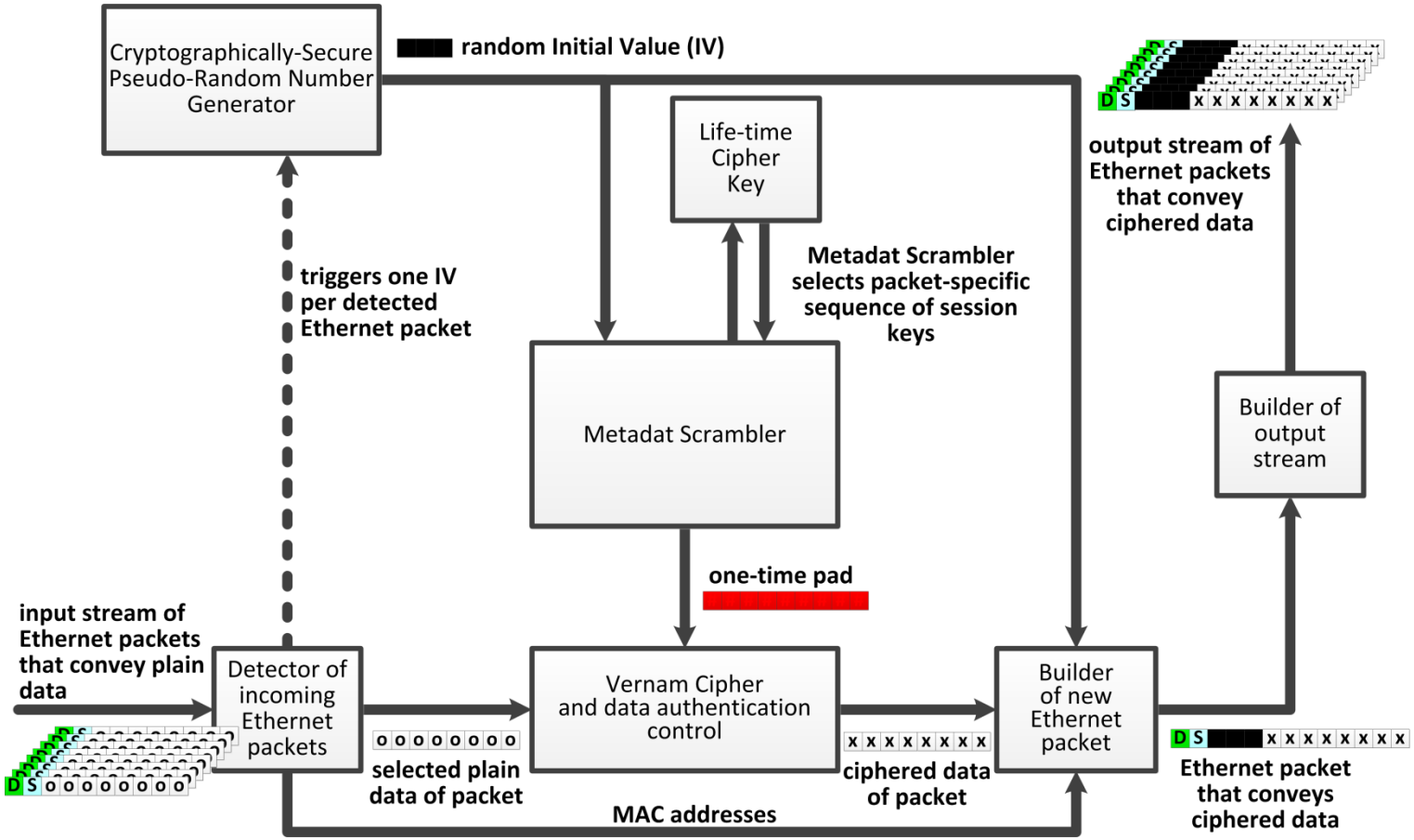
SAFURE

End-to-end encryption of dataflow

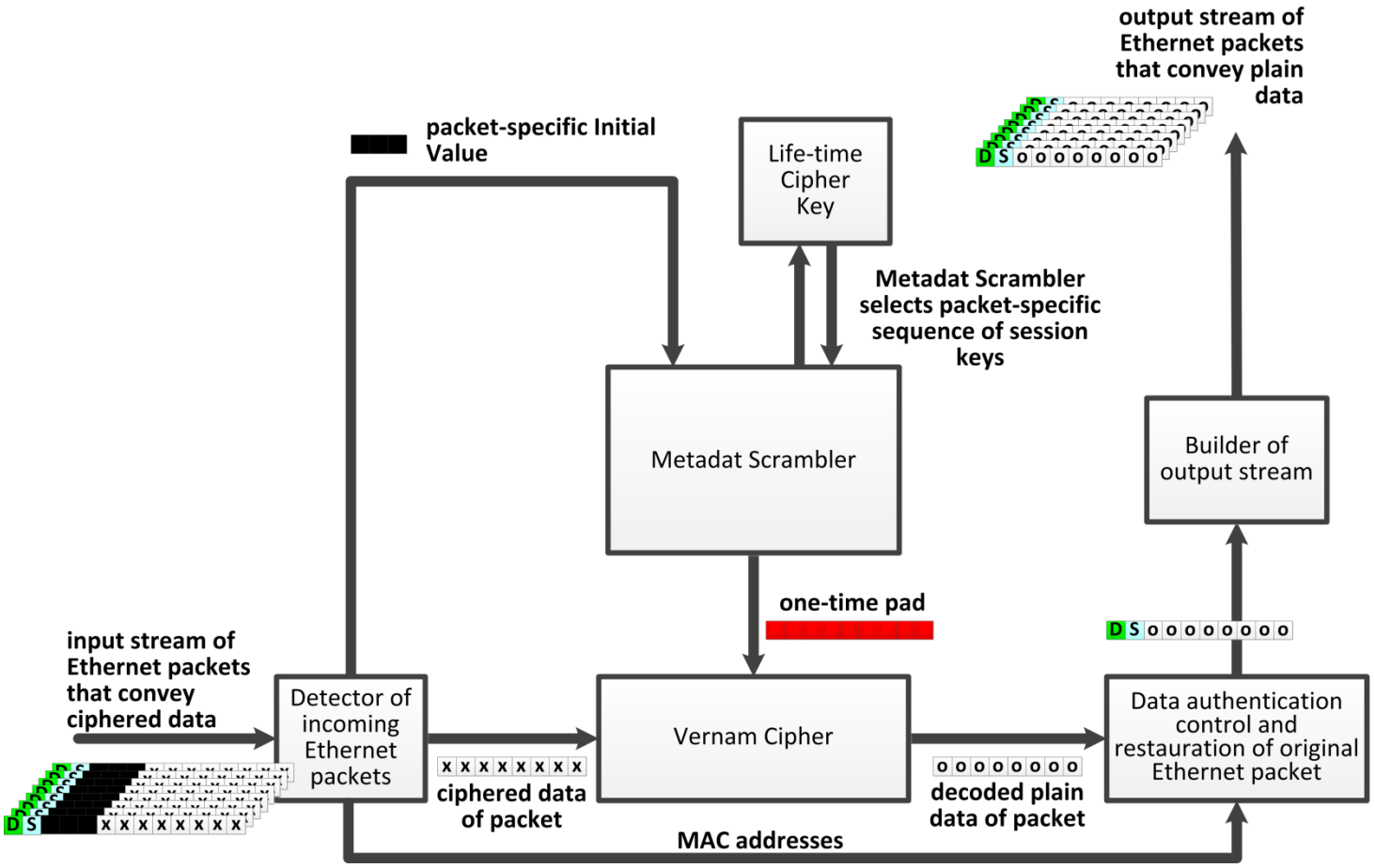
- Secure end-to-end communication: data stream will be secured.
- Requires implementation at each hop (cost), latency cost at each hop
- Completely transparent to network nodes



Encryption process @sender

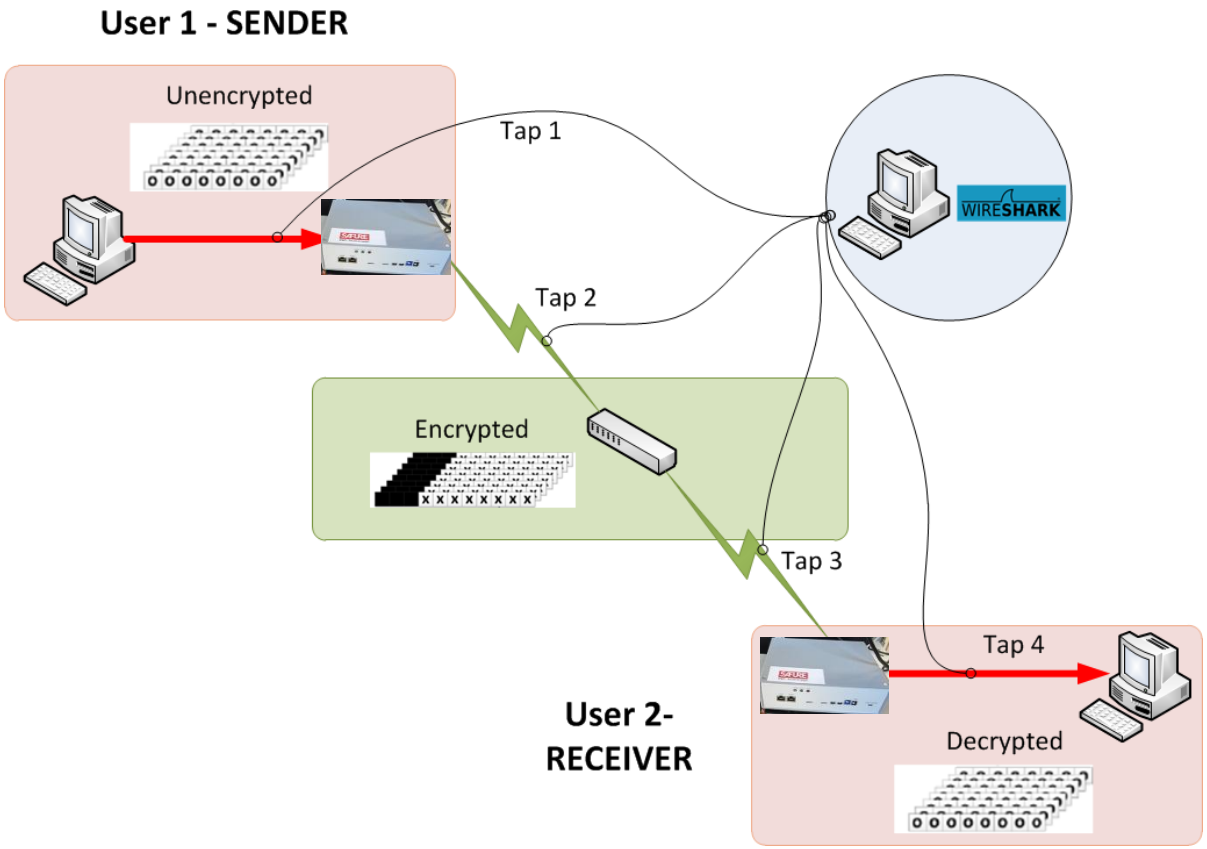


Decryption process @receiver



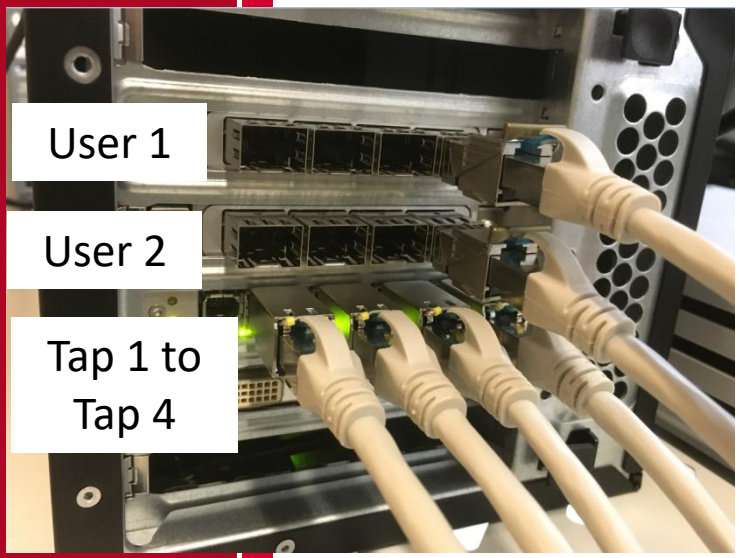
Performance Evaluation - Setup

- Evaluate latency, jitter, bit rate in various data flows



Switch

Tap



User 1

User 2

Tap 1 to Tap 4

MDSC devices

SAFURE

Performance Evaluation

Setup

- Best effort traffic, 100 Mbps, Frame interval: 10ms

Results

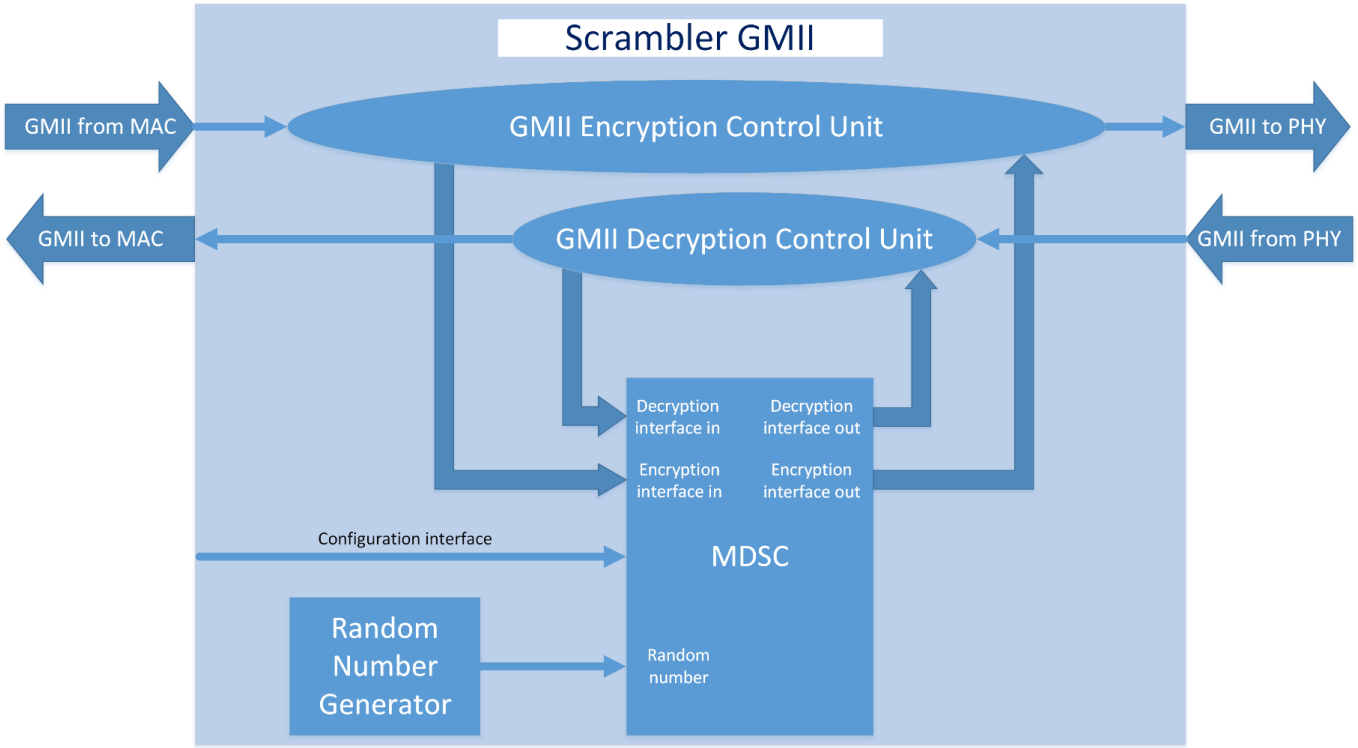
- Jitter is high for Time Triggered Ethernet
- Caused by Software, Network interface and the Scrambler in external device
- Jitter can be avoided by implementing the scrambler directly in the End Point Card.
- **Porting the FPGA Implementation**
- MDSC Extension for GMII

Process	Frame size [Bytes]	Min latency [µs]	Max Latency [µs]	Avg Latency [µs]	Jitter [µs]
Encryption	64	77	307	176	230
Encryption	1418	224	495	388	271
Decryption	64	72	151	106	79
Decryption	1418	253	488	378	235

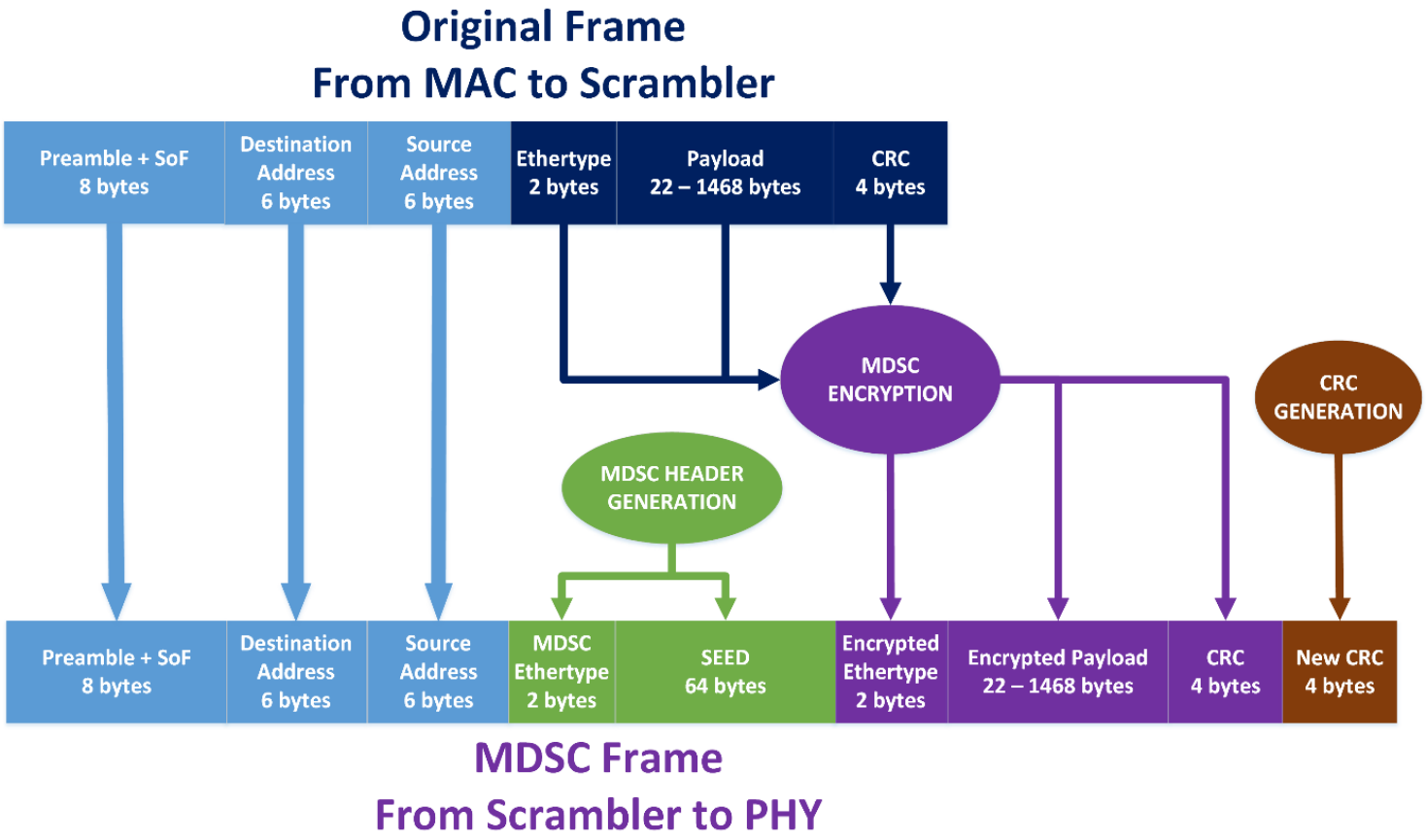
SAFURE

MDSC Extension for GMII

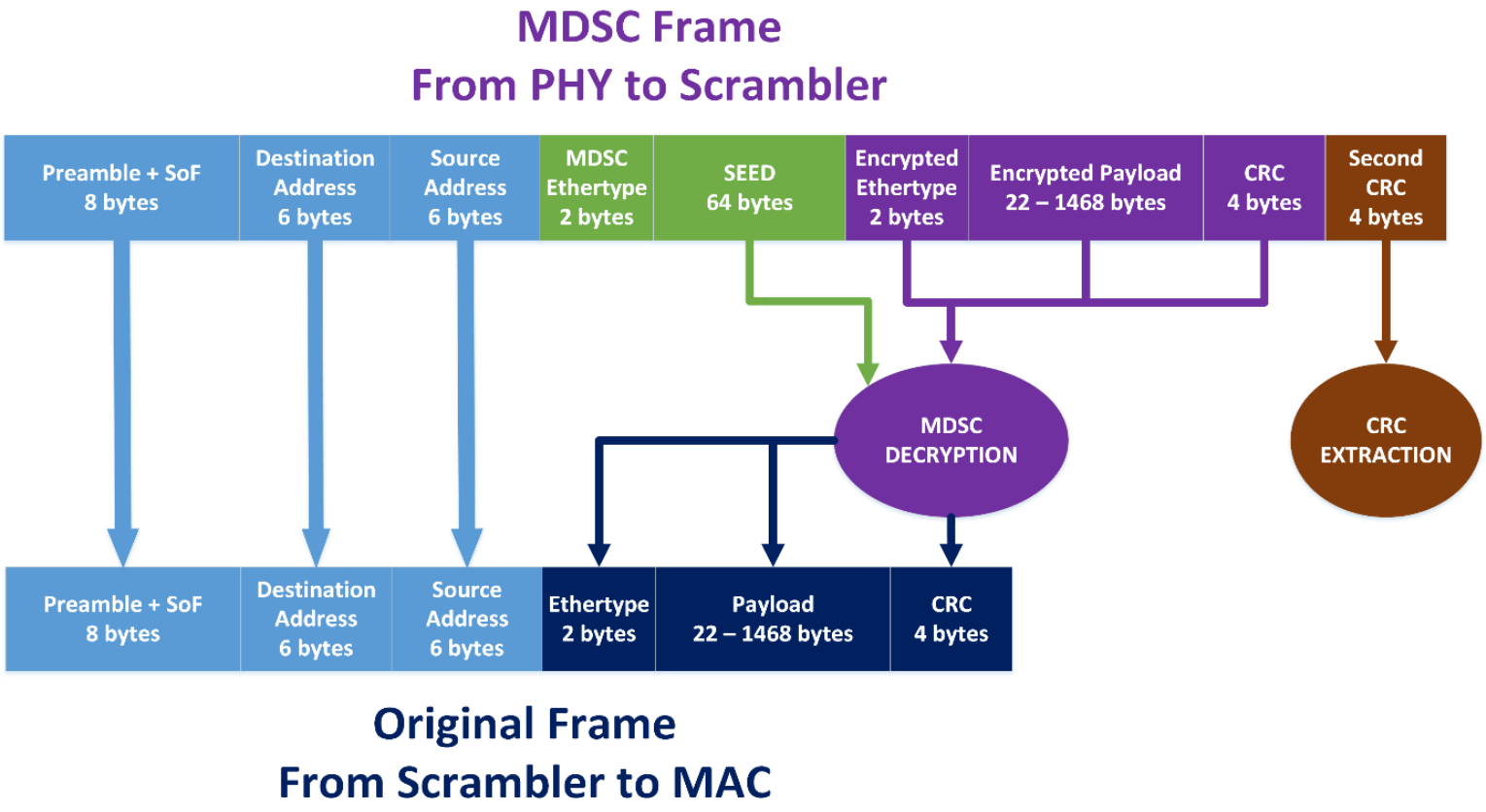
- GMII – standard 1 Gbit/s interface between MAC and PHY.



Frame Encryption (MAC → PHY)



Frame Decryption (PHY → MAC)



MDSC Internal Modifications

- Several internal modification was applied to the original MDSC Scrambler:
  - Xilinx models of memories and FIFOs were replaced by register-transfer level (RTL) models → can be used for simulations and other FPGA platforms
  - State machines responsible for encryption/decryption in Scrambler were improved by removing the need of information about the frame length before the encryption/decryption starts → no need to buffer the entire frame to get the frame length (resource cost and latency optimization)
  - The Lookup table used for configuration of linear feedback shift register LFSR were merged → the new Scrambler consumes only 50% of memory resources in comparison to the original version

SAFURE

Technical Parameters

- Scrambler GMII is designed for 1 Gbit/s Ethernet speed.
- Only one clock domain is used, Clock freq.: 125 MHz.
- Period of one clock cycle is 8 ns.
- For 1 Gbit/s Ethernet speed, one byte has to be processed per one clock cycle.
- Original *random number generator* was replaced by an implementation based on Cellular Automata
  - Reason: the original *random number generator has introduced latency* high (non-constant) latency for random number generation
  - The new RNG requires **only one clock** cycle to generate a new random value → encryption/decryption latency is reduced
  - The Cellular Automata consists of 512 cells that generate 512-bit pseudo-random vectors
  - 2^{512} possible values in total

SAFURE

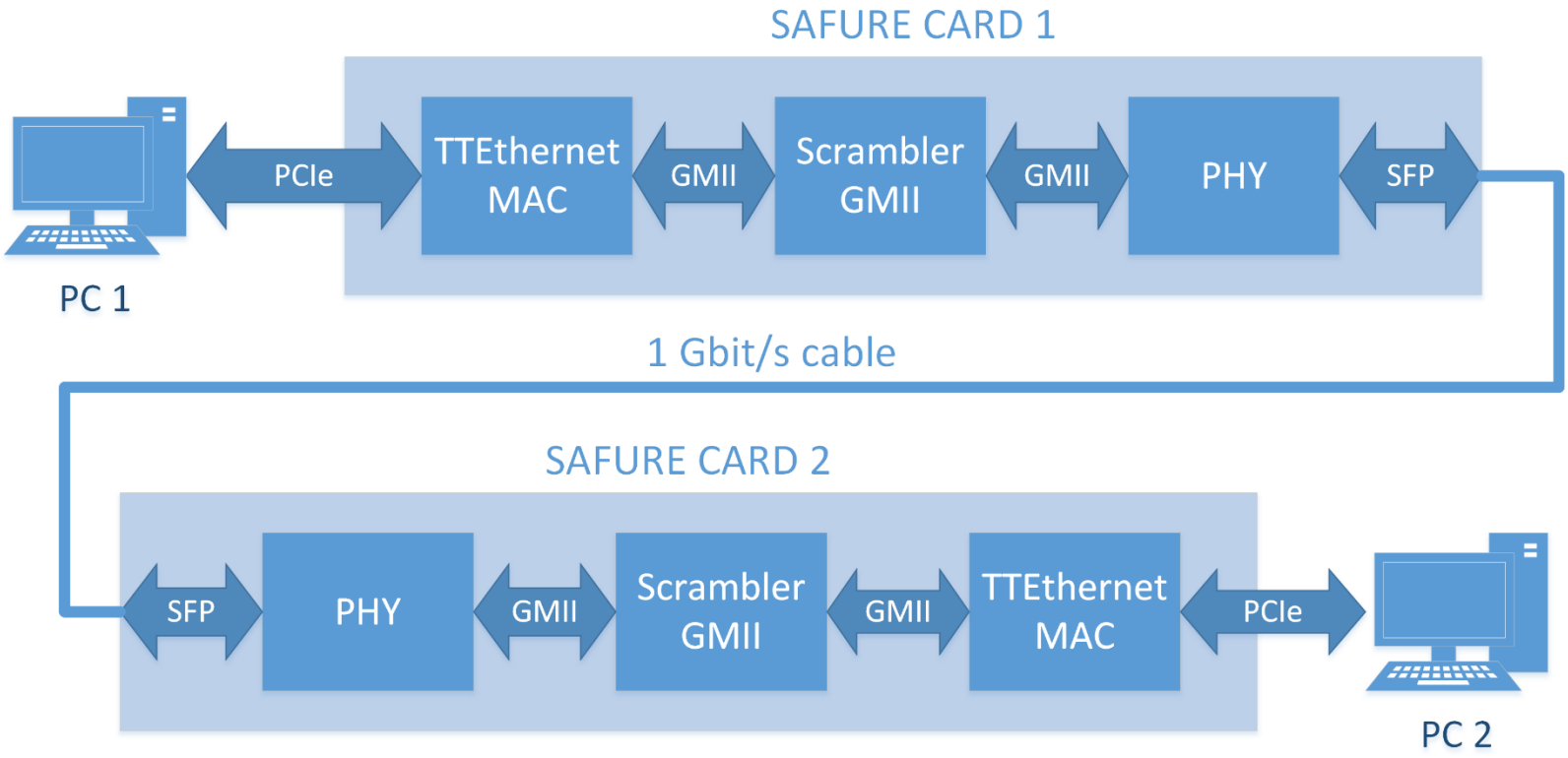
Simulation Results

- **Latency** for frame encryption and decryption remains **constant** regardless of frame size → **jitter is 0**
- **Frame extension** is caused by MDSC Ethertype (2 bytes) and Seed (64 bytes) = 66 bytes total → 66 clock cycles (528 ns)
- **Encryption processing latency:** 12 clock cycles (96 ns)
- **Encryption total latency:** processing + frame extension = 78 clock cycles (624 ns)
- **Decryption processing latency:** 41 clock cycles (328 ns)
- **Decryption total latency:** processing + frame extension = 107 clock cycles (856 ns)

SAFURE

Test Scenario

- Two PCIe cards containing Scrambler GMII between MAC and PHY
- End systems connected directly with 1 Gbit/s cable
- **Performance evaluation and comparison to MACSec ongoing**



Common Criteria for Automotive Ethernet

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems

Unified Approach to Automotive Security

Do we as an industry want to establish common best-practices in automotive security design?

- There is a broad agreement that, indeed, we do.

How can we do that?

- We need a common language.
- The common criteria is a candidate solution.

Some Abbreviations

- CC: Common Criteria
- TOE: Target of Evaluation
- TSF: TOE Security Functionality
- PP: Protection Profile
- ST: Security Target
- SFR: Security Functional Requirements
- SAR: Security Assurance Requirements
- EAL: Evaluation Assurance Level

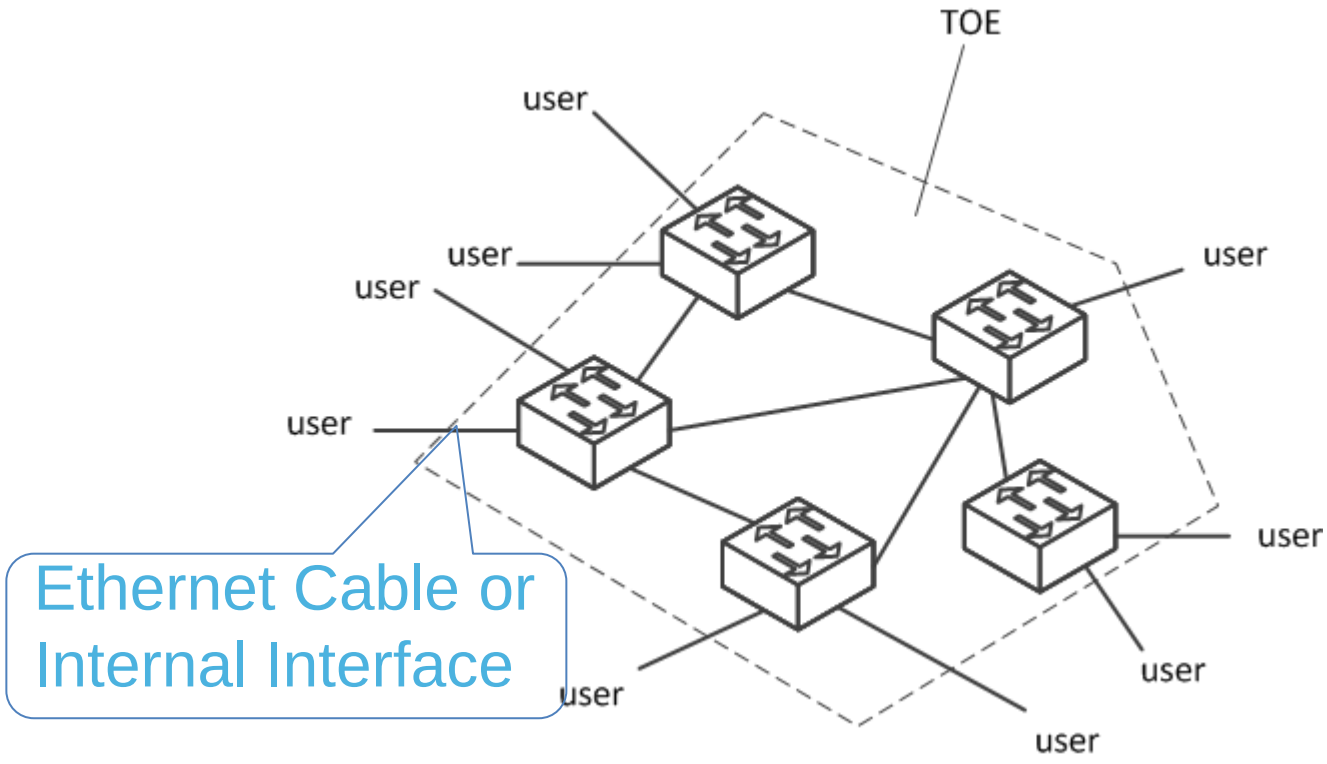
SAFURE

Draft Protection Profile for Automotive Ethernet

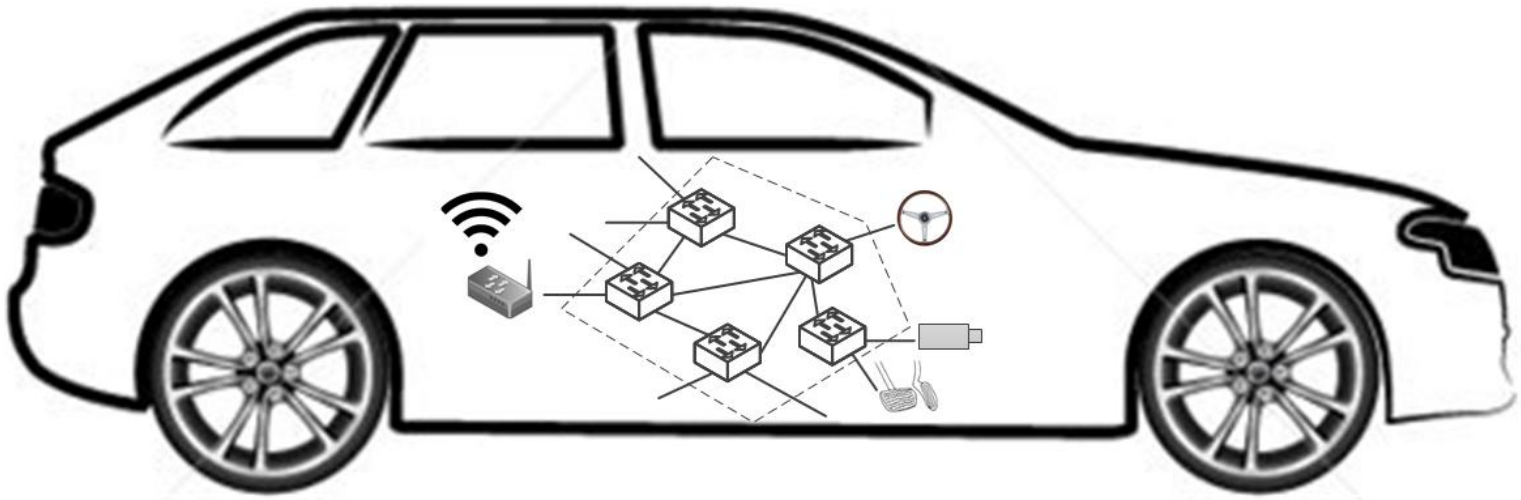
"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

SAFURE

Target Of Evaluation (TOE)



TOE Operational Environment

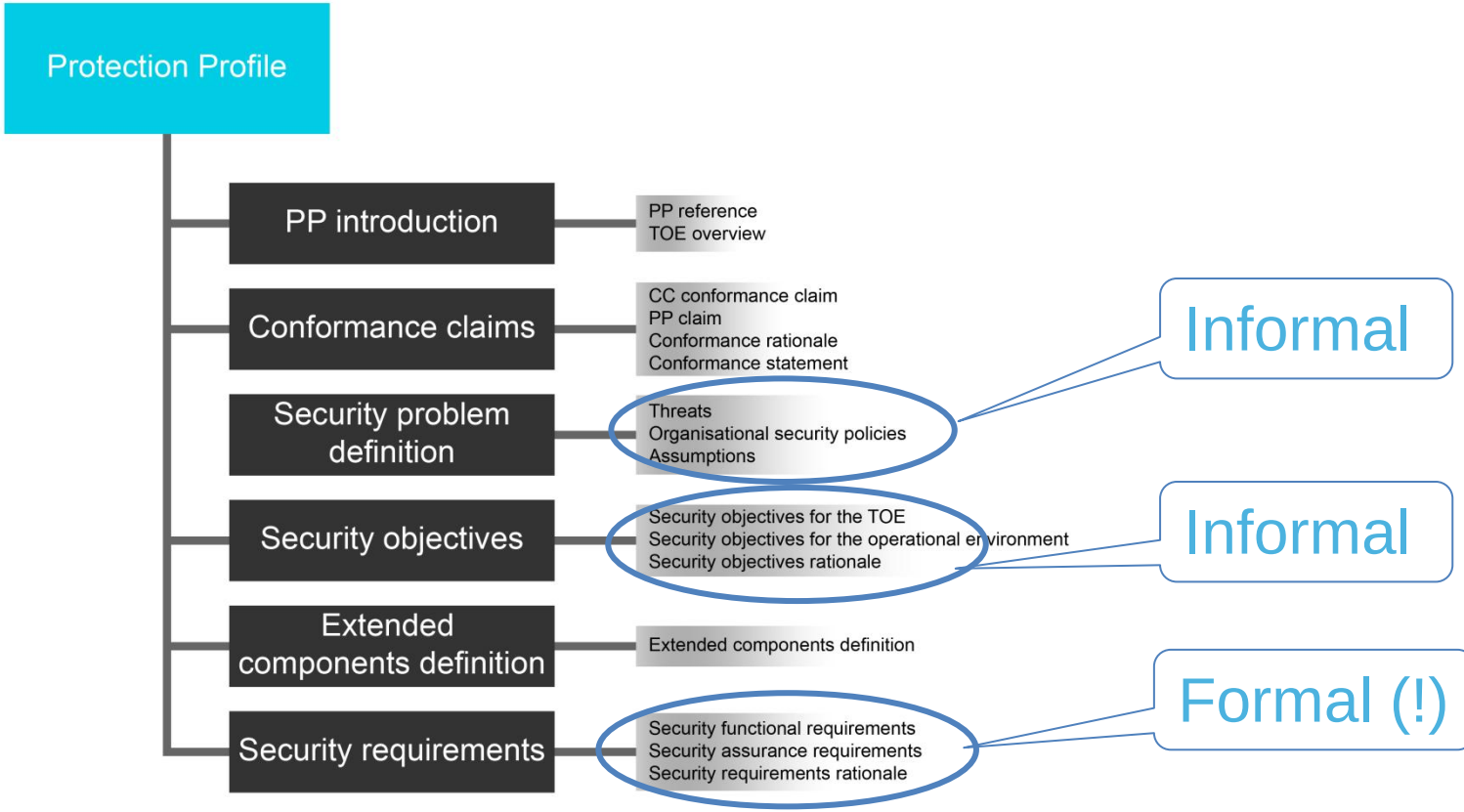


SAFURE

CC Workflow

- CC General Workflow:
  - An organization seeking to acquire a particular type of IT security product develops their security needs into a PP (protection profile), then has this evaluated and publishes it.
  - A developer takes this PP, writes an ST (security target), that claims conformance to the PP and has this ST evaluated.
  - The developer then builds a TOE (target of evaluation) (or uses an existing one) and has this evaluated against the ST.
- Suggested Automotive Workflow
  - **A group of automotive OEMs** seeking to acquire a particular type of **E/E security** product develops their security needs into a PP (protection profile), then has this evaluated and publishes it.
  - A **specific OEM or Tier takes this PP**, writes an ST (security target), that claims conformance to the PP and has this ST evaluated.
  - The **Tier** then builds a TOE (target of evaluation) (or uses an existing one) and has this evaluated against the ST.

Protection Profile Structure



Examples – Threats

- From the CC:
  - a worm seriously degrading the performance of a wide-area network;

- Automotive Ethernet Specific:
  - T_INSERT_DELAY: The threat agent sources messages into the Ethernet network thereby delaying real-time messages for more than the length of one maximum sized Ethernet frame.

SAFURE

Examples – Security Objectives

- From the CC:
  - The TOE shall keep confidential the content of all files transmitted between it and a Server;

- Automotive Ethernet Specific:
  - O_MSG_WHITELISTING: The TOE shall ensure that only whitelisted real-time messages are communicated in the Ethernet network.

Example – Security Funct. Requ.

- **FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:**
  - *the TOE switch memory*
  - *the communication bandwidth between any two switches in the TOE and between switches and users in the TOE*
  - *time slots in time-triggered communication*
  - **that** *individual user* **can use** *over a specified period of time***.**

Conclusion – Common Criteria for Automotive Security

- Industry-wide agreement on E/E security best-practice optimally reduces risk at and is cost-efficient.
- There is a need for a common language for these best-practices.
- The common criteria can be such a language.
- The CC have a track record in critical IT products.
- Application of the common criteria to Automotive Ethernet.

SAFURE

Summary

- Security for (Automotive) Deterministic Ethernet is critical
- Address it on technological and process level
  - MAC level encryption for secure end-to-end data flow
  - Common Criteria and Protection Profile

SAFURE

THANK YOU!

SAFURE

SAFURE Grant Agreement No. 644080

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

"This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government."

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@safure.eu