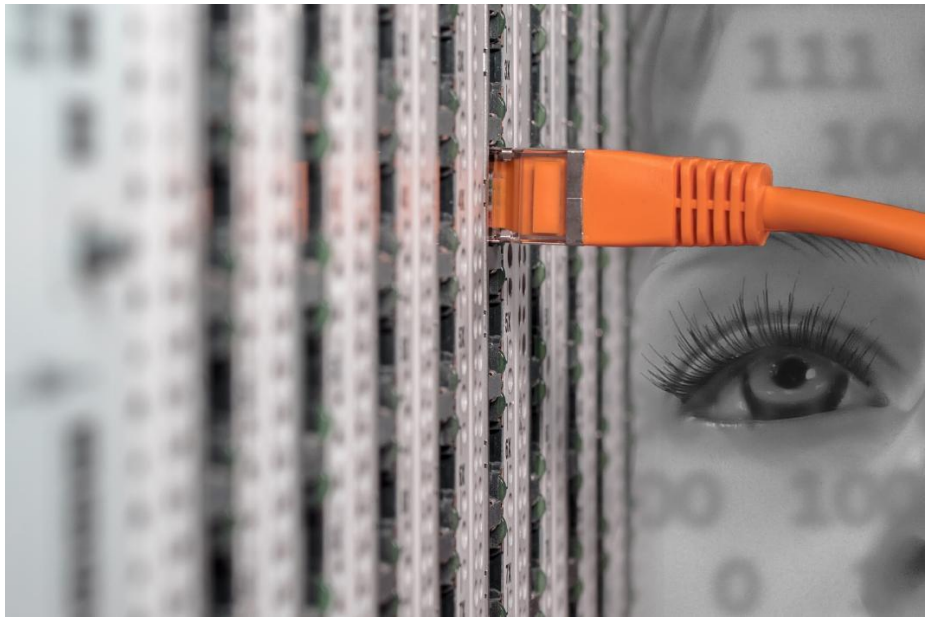
Protecting Time-Aware Real-Time Traffic in the Smart Grid

Author: Mikel Rodriguez

Index

- Communications in Smart Grid
- Security Mechanisms and Protocols
- Requirements
- Enabling Secure Communications in Smart Grid



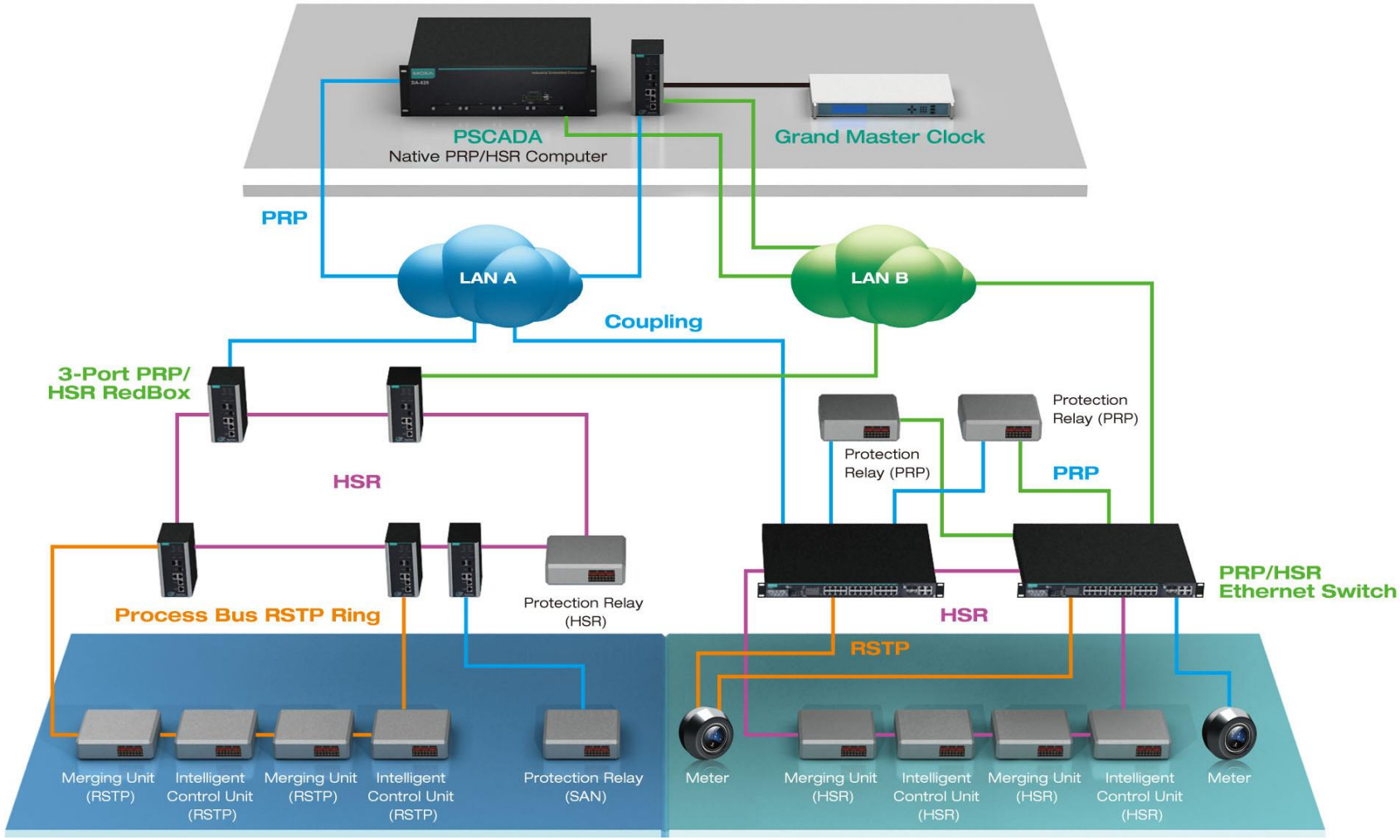
SoCe

SoCe

Communications in Smart Grid

SoCe

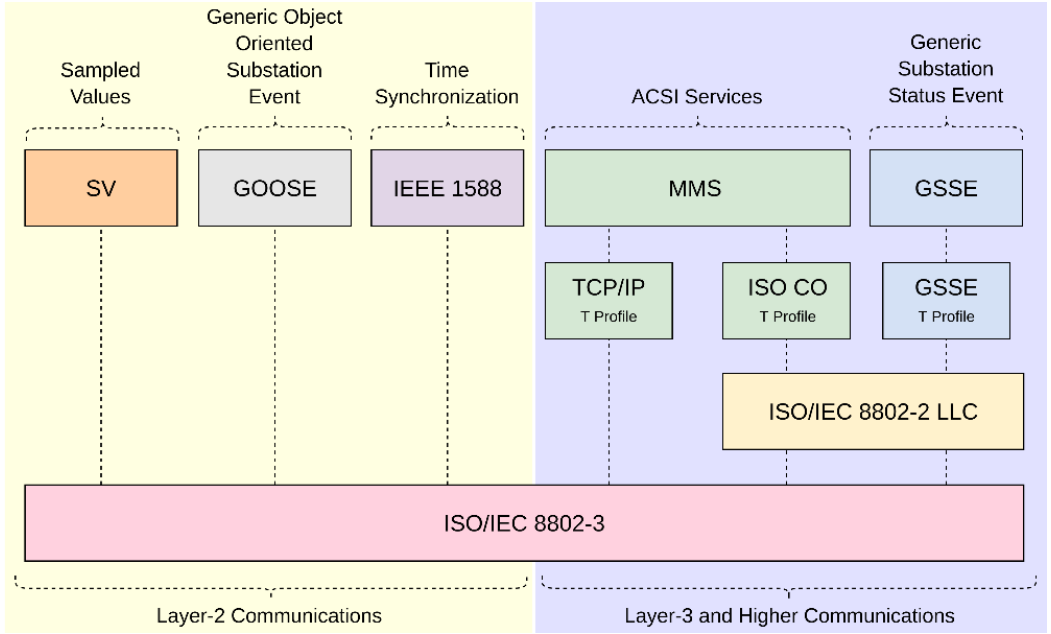
Complex Network Topology



SoCe

Standard Communication Protocol

- IEC 61850
  - » Provides interoperability among devices from different vendors
  - » Layer-2 communications → Hard real-time traffic (under 3 ms)
  - » Layer-3 communications



SoCe

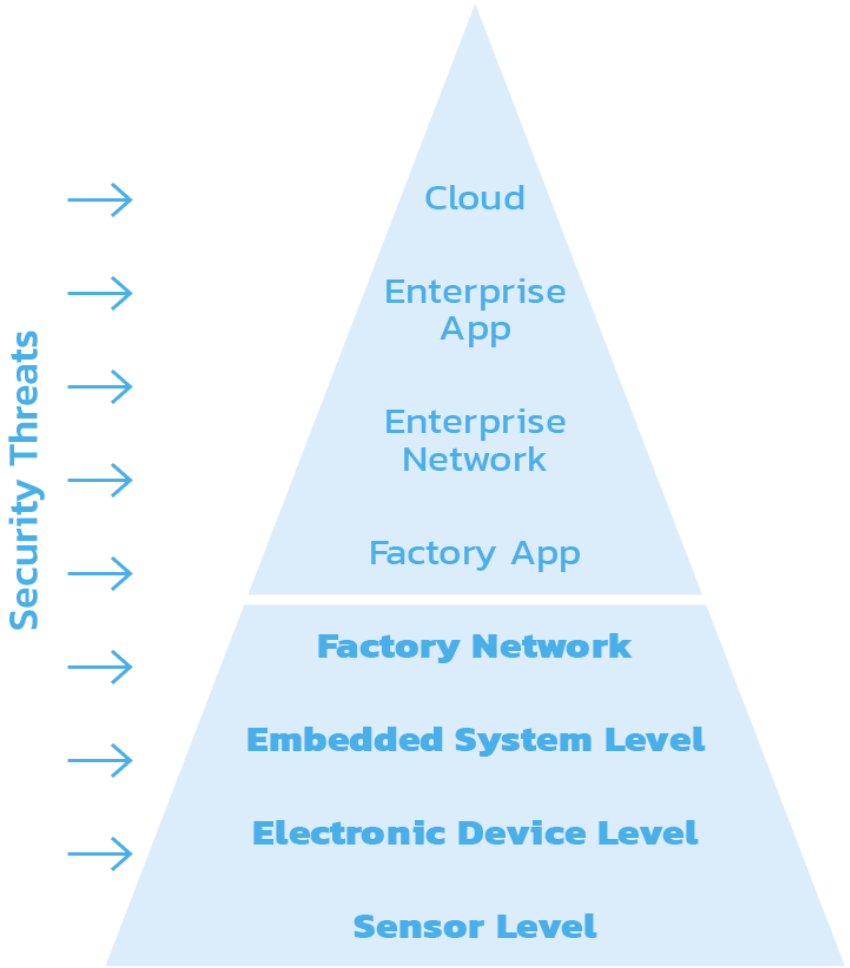
Security in Smart Grids

- Considered critical infrastructures
- IEC 61850
  - » Does not provide security features
  - » Difficult to protect layer 2 hard real-time traffic (GOOSE and SV)
- IEC 62351
  - » Security protocols for all the OSI layers

SoCe

Security Mechanisms and Protocols

Security for IEC 61850 – GOOSE and SV



IEC 62351-10 Security Architecture

IEC 62351-8 Security Role Based Systems

IEC 62351-3, -4, -5 Security IT world specific for the Sector

IEC 62351-7 Security Network and System Management

IEC 62351-9 Key Management System valid for OT (Groups)

IEC 62351-6 Security for Stringent Real-Time Traffic

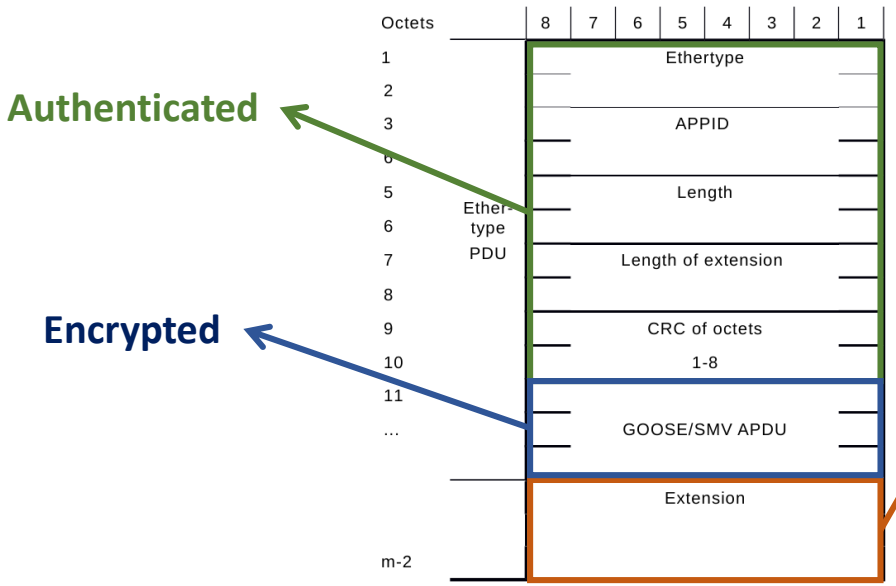
IEEE 1686, Standard for Substation Intelligent Electronic Devices (IED)

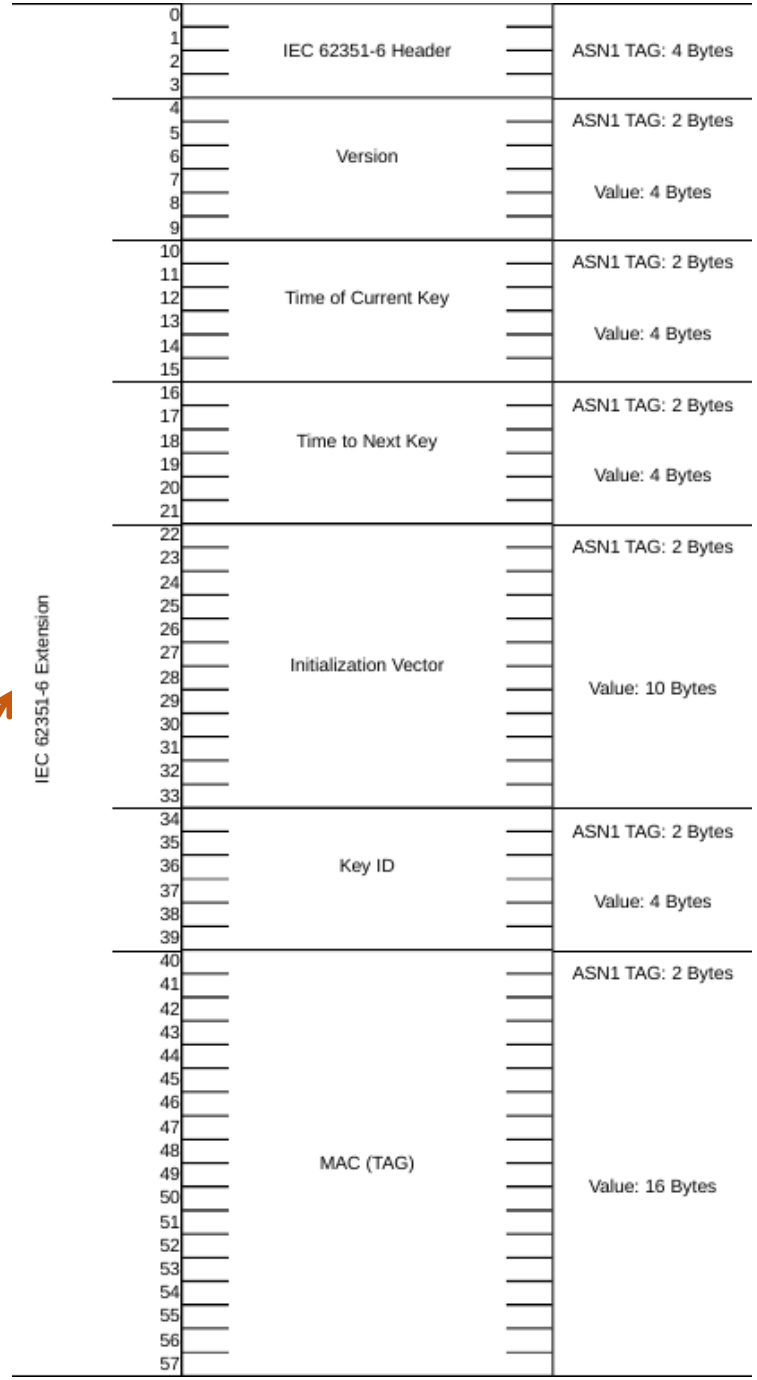
ISO/IEC 19790, Security Requirements for Cryptographic Modules

SoCe

Authentication and Encryption

- IEC 62351-6
  - » Security extension for IEC 61850
    - > Layer 2 GOOSE and SV
  - » Message authentication → Mandatory
  - » Message encryption → Desired (optional)

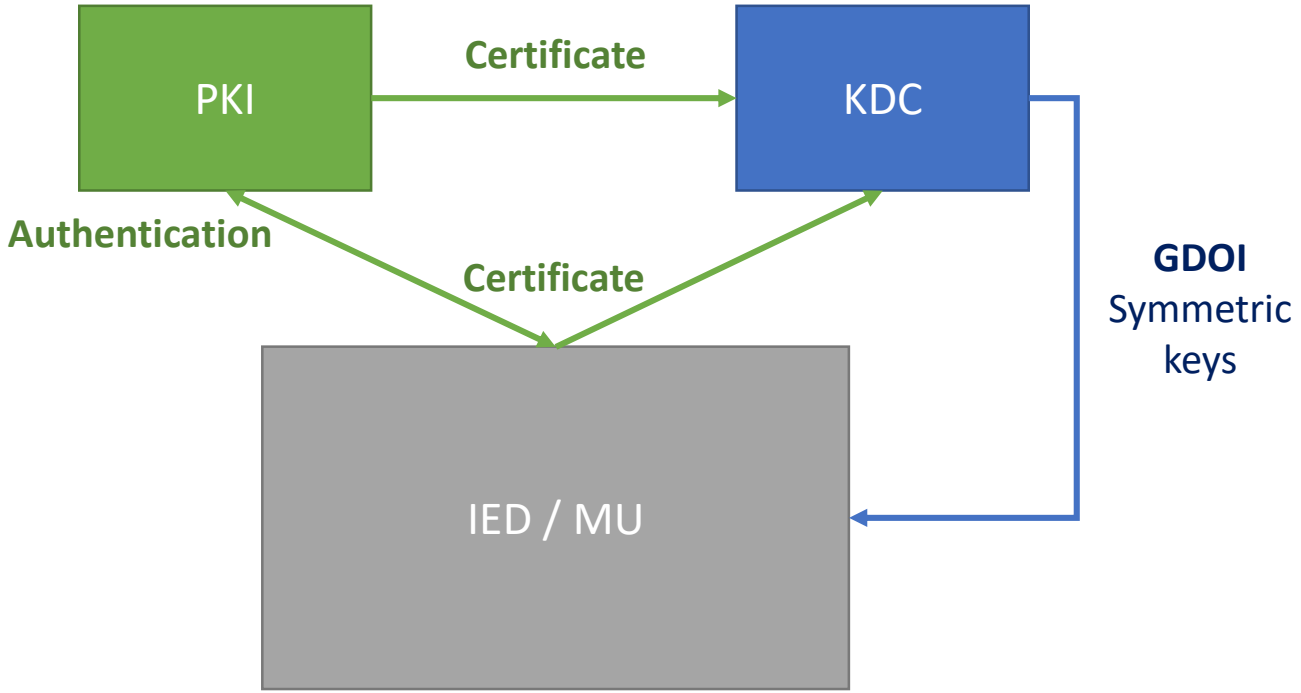




SoCe

Secure Key Exchange

- IEC 62351-9
  1. Each device must be authenticated by the PKI to get a valid certificate
  2. Certificate is used to get symmetric keys from KDC using GDOI



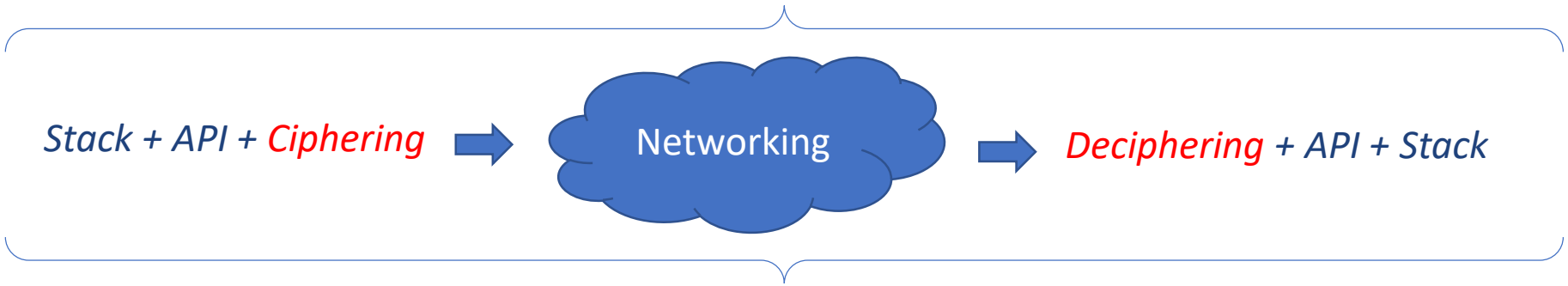
SoCe

SoCe

Requirements

Message Types – Performance Classes

Transfer Time Class	Transfer Time (ms)	Application: Transfer of
TT0	1000	Files, events, log contents
TT1	1000	Events, alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases, status changes
TT6	3	Trips, blockings



In less than 3 ms

SoCe

Limitations of Software Solutions

- First version of IEC 62351-6 based on RSA

Key Size	Pentium M @ 1.7 GHz (1 GB RAM)	Intel Core 2 Duo @ 2.2 GHz (2 GB RAM)
1024	6.8 ms	4 ms
512	3.9 ms	1.5 ms

Time use for RSA signature operations

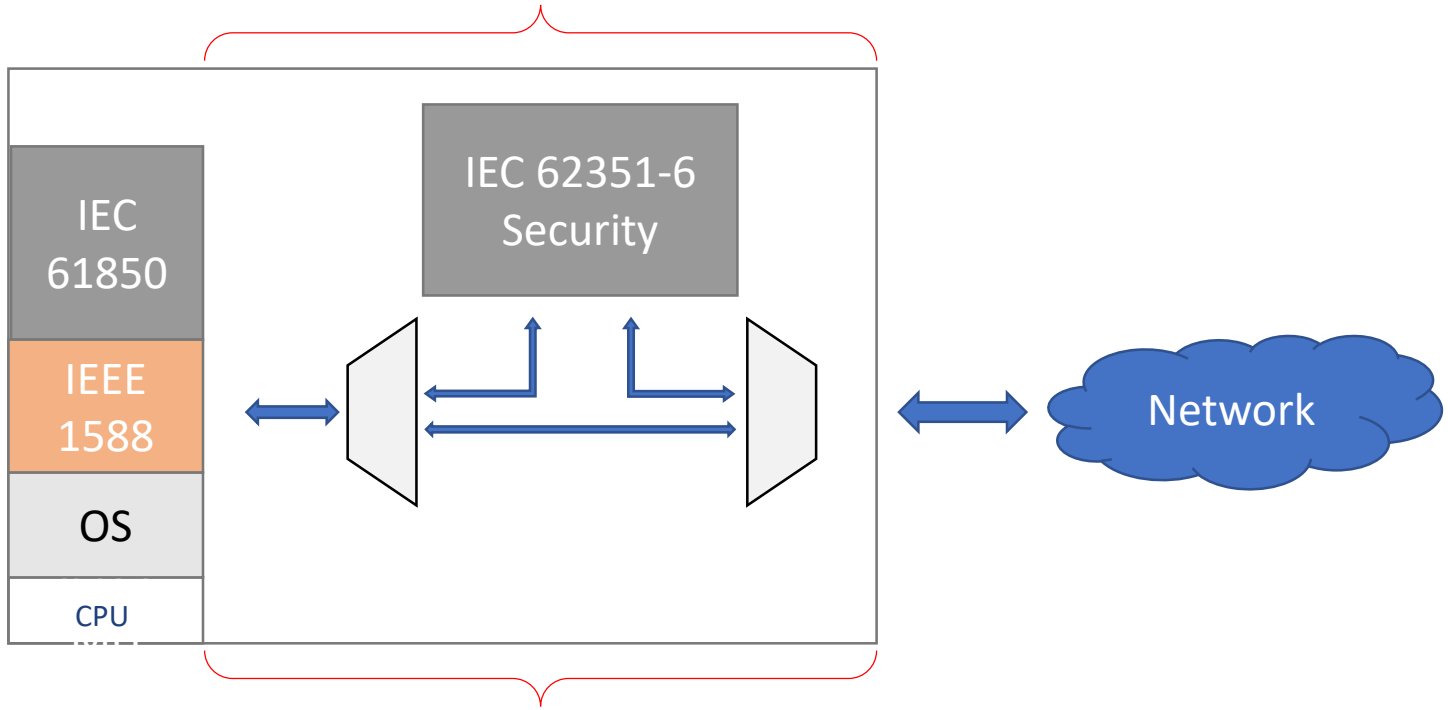
3 ms requirement not met
Changes in the standard required

- Revision of IEC 62351-6 based on block-cipher cryptographic suites (AES-GCM)

SoCe

Transparent to Other Protocols

- Higher layer protocols (MMS, GSSE…)
- Time Synchronization – IEEE 1588 (PTP)
  - » Transparent clock



SoCe

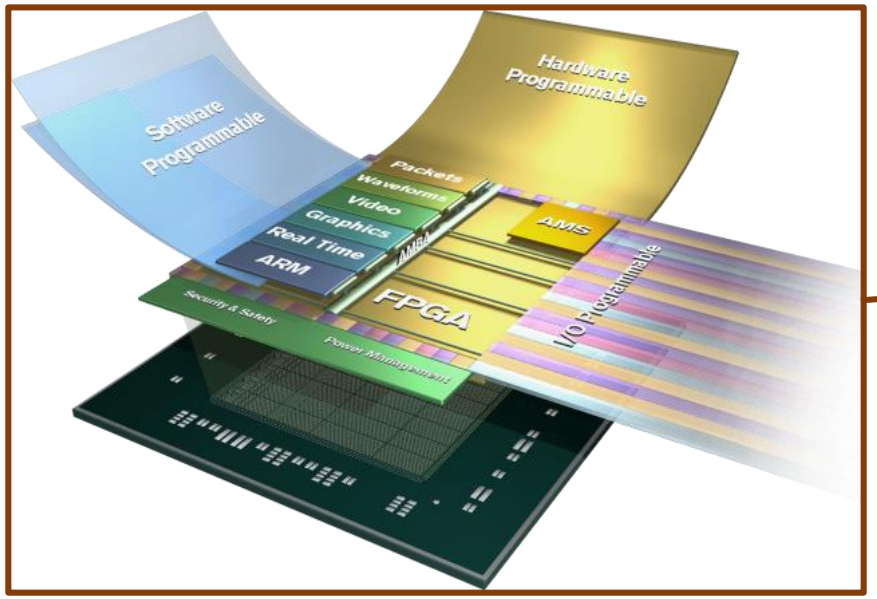
SoCe

Enabling Secure Communications in the Smart Grid

SoCe

Implementation: Reconfigurable Platforms

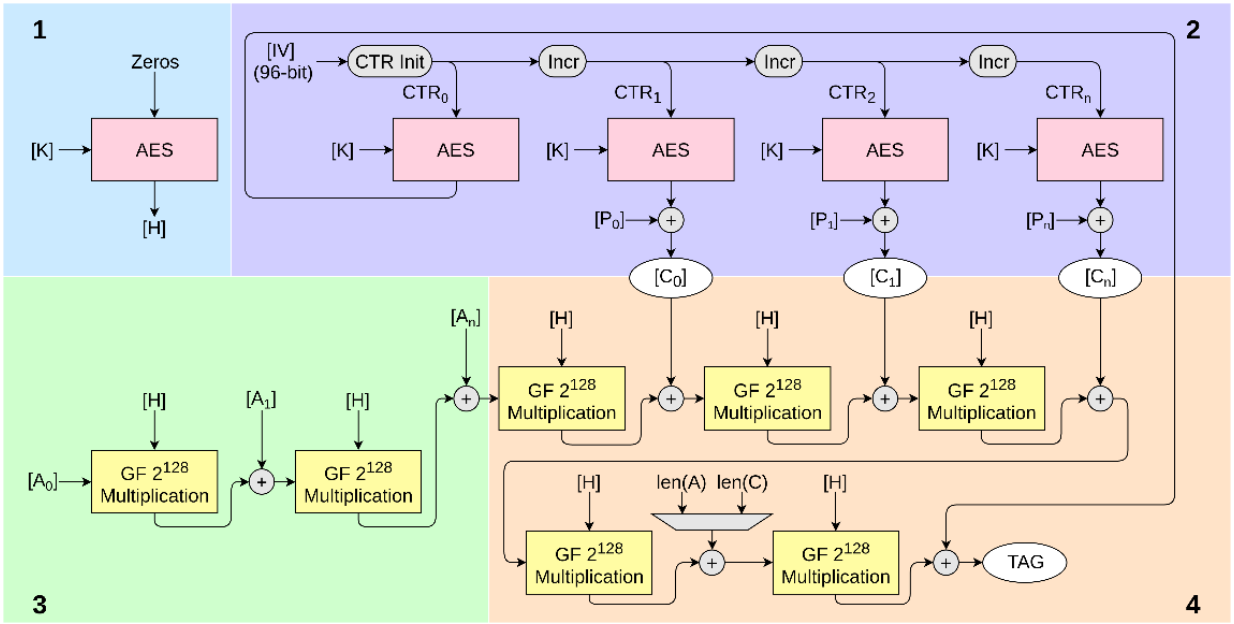
- Specialized IP Cores
  - »Wire-speed packet inspection
  - »Hardware cipher engine (AES-GCM)



Dedicated Data-Flow Hardware Processing

- AES-GCM hardware engine latency

Cryptographic Engine @ 16 Gbps (125 MHz)				
Word Size	Encryption Delay		Decryption Delay	
	Clock Cycles	Nanoseconds	Clock Cycles	Nanoseconds
128-bit	30	240	30	240



SoCe

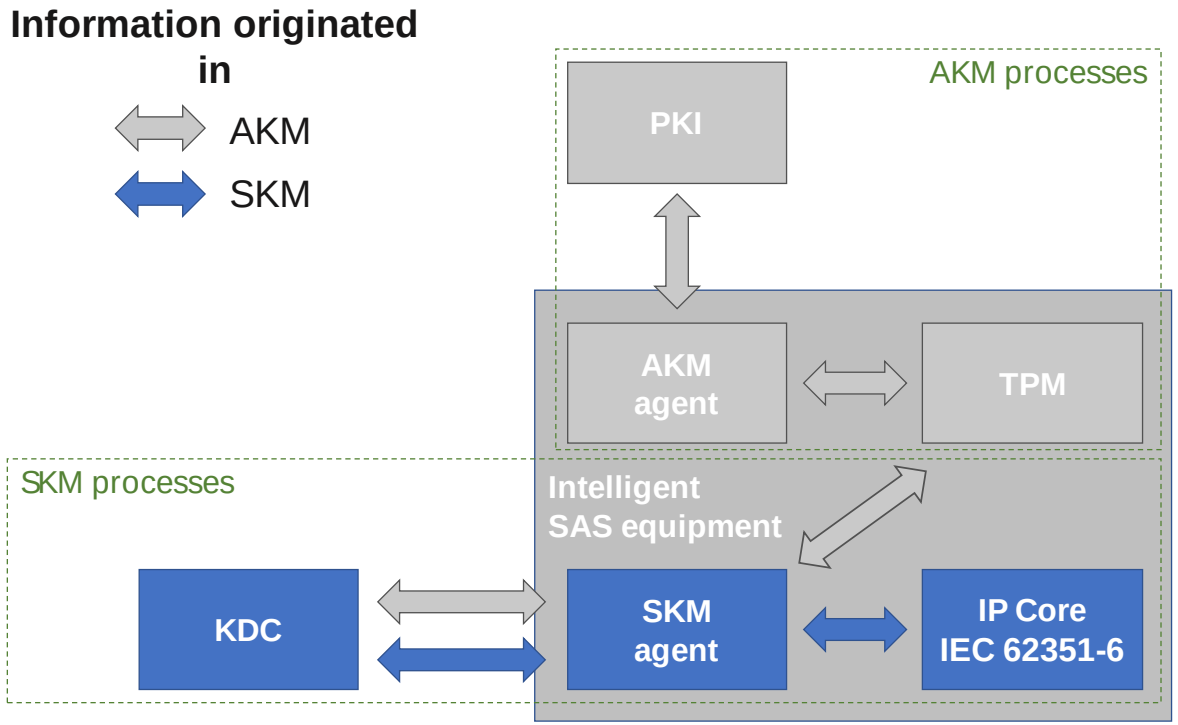
Dedicated Data-Flow Hardware Processing

- IEC 62351-6 IP Core Latency
  - » Deep packet inspection
  - » De/ciphering
  - » Frame regeneration

Cryptographic Engine @ 16 Gbps (125 MHz)				
Frame Length (bytes)	Encryption Delay		Decryption Delay	
	Clock Cycles	Nanoseconds	Clock Cycles	Nanoseconds
172	439	3512	565	4520
300	703	5624	829	6632
553	1225	9800	1351	10808
1057	2265	18120	2391	19128
1435	3044	24352	3170	25360

Security Key Exchange Mechanism

- IEC 62351-9
  - » Asymmetric key processes (AKM)
  - » Symmetric key processes (SKM)



SoCe

Conclusions

- IEC 62351 provides security to IEC 61850
- Requirements and challenges that must be met
  - Total delay < 3 ms
  - Transparent to other protocols
  - Correct delay of IEEE 1588 packets (PTP TC)
- Data-Flow hardware processing to provide low latency and low jitter

SoCe

About SoC-e

- Provides **IP Cores, modules and equipment** for
  - » Networking
    - > Deterministic Ethernet
      - MTSN, D-HSR
    - > High-availability Ethernet
      - HSR/PRP, MRP, S-HSR
    - > Time-aware ethernet
      - MES, UES, field-buses
  - » Synchronization
    - > IEEE 1588, IRIG-B
  - » Real-time Cybersecurity

SoCe

Thank you for your attention!

www.soc-e.com

T.+34 944 420 700
info@soc-e.com

Edificio Udondo, 6º planta
Avd. Ribera de Axpe, 50
48950 Erandio · Bizkaia | **SPAIN**