

Study Committee D2

Information Systems and Telecommunication

Paper 11051_2022

ANALYSIS OF THE IMPACT OF CRYPTOGRAPHY IN THE GOOSE COMMUNICATIONS

Miguel Á. SÁNCHEZ

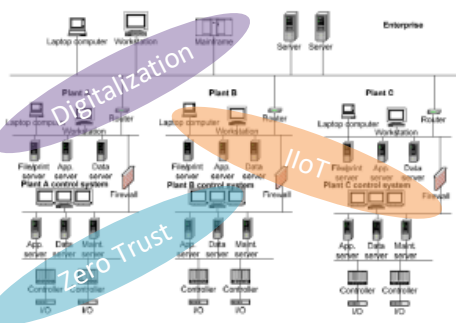
Arteche (Spain)

Gerard VIDAL

Enigmmedia (Spain)

Motivation

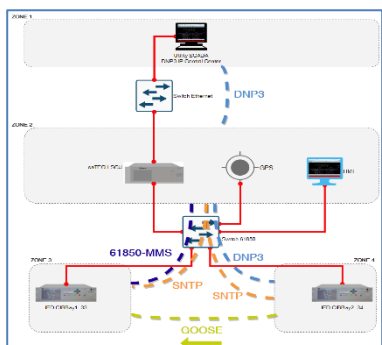
Along the years, cryptographic mechanisms have been proposed to protect different aspects of substation communications. But for various reasons, these mechanisms have not yet been standardized and deployed. One of these reasons is that there are restrictions on the limits on the speed at which certain processes have to be transmitted through the network. Another reason to take into account are facts as the long lifespan of industrial devices (from 30 to 60 years), and changes needed in OT culture and processes. Digitization and increased exposure of IEDs in power systems, along with strategies such as the defense in depth proposed in IEC 62443, and the growing and evolving risks, make it necessary to reconsider the use of cryptography in critical areas and conduits, especially if they are exposed.



Typical substation architecture

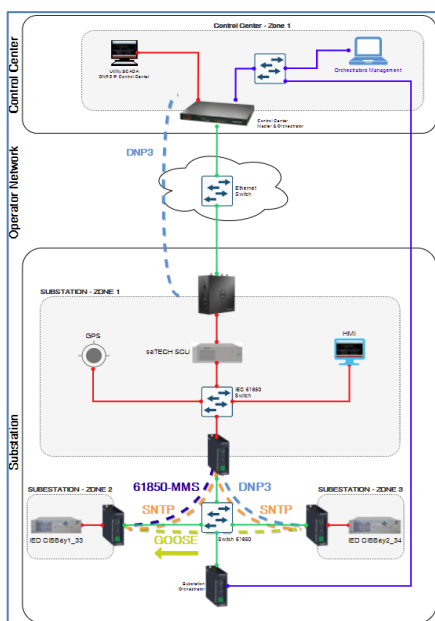
Method/Approach

For the experimental set-up, we have followed the enclave gateway model. We defined a basic substation architecture, covering levels 0 (field), 1 (bay) and 2 (substation). We defined zones one to four, and a conduit for each communication protocol, and we have introduced external hardware appliances, called ciphers, into the architecture to secure the traffic and measure their impact in the field devices. We did not need to modify any IED configuration. The latency was measured in GOOSE conduit, between zone 4 and zone 3. Network traffic was captured to verify that it were encrypted.



Basic substation, without security

Red lines represent unsecured communications
Green lines represent secured communications



Experimental set-up, with security

Study Committee D2
 Information Systems and Telecommunication
 Paper 11051_2022

**ANALYSIS OF THE IMPACT OF CRYPTOGRAPHY IN THE
 GOOSE COMMUNICATIONS**
 continued

Object of investigation

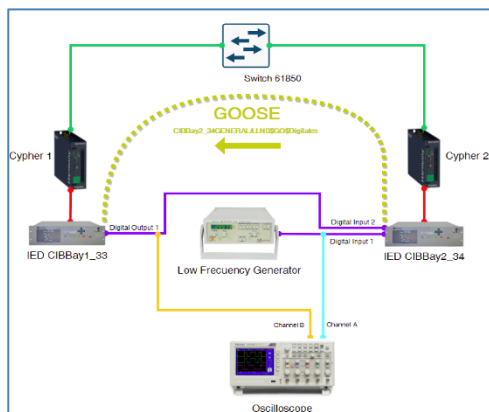
We have analyzed mechanisms that allows providing a basic classic substation architecture without communications cybersecurity requirements with means providing confidentiality, authentication, and integrity, in addition to allowing the establishment of logical segmentation by zones and conduits in accordance with the IEC62443 standard, asset control and reduction of the attack surface, among other benefits. This analysis focuses on the impact in Class TT6 GOOSE, with transfer times requirements less or equal to 3ms, for which algorithms specially designed for low delay (<1ms) will be used to evaluate its viability at the various levels of a substation architecture.

This approach allows a more widespread use of encryption techniques in environments where it is important to protect confidentiality and integrity, and the communication endpoints usually have low performance CPUs, and/or there are less demanding latency requirements than those of class TT6 of the IEC61850 standard.

Transfer Time Class	Transfer Time [ms]	Application examples
TT0	> 1000	Files, events, log
TT1	500 < t ≤ 1000	Events, alarms
TT2	100 < t ≤ 500	Operator commands
TT3	20 < t ≤ 100	Slow automatic interactions
TT4	10 < t ≤ 20	Fast automatic interactions
TT5	3 < t ≤ 10	Releases, status changes
TT6	≤ 3	Trips, blockings

Experimental setup

For latency measurement, the next set-up has been configured over the secured architecture:



- Digital Input 1 in IED CIBBay2_34 will send a GOOSE frame, `CIBBay2_34GENERAL/LLN0$G0$Digitales` GOOSE Control Block on any change in the signal value. It is included in the dataset `LLN0$DigitalesBCU2`.

- The IED CIBBay1_33 is subscribed to `CIBBay2_34GENERAL/LLN0$G0$Digitales`, and has a logic programmed to activate the Digital Output 1 when the `CIBBay2_34CIB_220_Bay2/GGIO2.Ind1.stVal[ST]` changes.

- The Digital Output 1 from CIBBay1_33 is wired back to Digital Input 2 from CIBBay2_34.

With this test environment running, the Low Frequency Generator generates 125 VDC pulses at a fixed rate, to activate and deactivate the Digital Input 1 of IED CIBBay2_34. This causes a GOOSE event to be sent to CIBBay1_33, which in turn triggers the logic that activates the digital output, activating digital input 2 back in CIBBay2_34. The complete process is registered in CIBBay2_34 events log, and it can be measured by subtracting DI2 timestamp minus DI1 timestamps for each event:

Orden	Id	Fecha	Descripción	Tipo	Estado / Orden	Calidad
1400	47825	2022-01-21 14:10:20.927	CIBBay2_34. FALLO COMUNICACION UCSCIB	ESTADO	NORMAL	Válida
1399	47824	2022-01-21 14:09:58.881	CIBBay2_34. ESTADO PUERTO ETHERNET LAN 1	ESTADO	NORMAL	Válida
1398	47823	2022-01-21 14:09:35.998	CIBBay2_34. BCU2 GGIO2 ENTRADA DIGITAL 01	ESTADO	VALOR1	Válida
1397	47822	2022-01-21 14:09:35.606	CIBBay2_34. BCU2 GGIO2 ENTRADA DIGITAL 01	ESTADO	VALOR1	Válida

Study Committee D2

Information Systems and Telecommunication

Paper 11051_2022

ANALYSIS OF THE IMPACT OF CRYPTOGRAPHY IN THE GOOSE COMMUNICATIONS continued

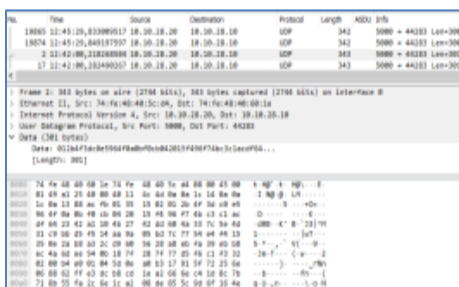
Test results

We evaluated latency in 3 tests:

- **Complete circuit with oscilloscope:** We generated 5000 events by connecting the IEDs directly to switch (without security), and then we repeat the same measure process by connecting the IEDs through the cyphers (with security). We calculated the average of whole processing time.
- **Only GOOSE latency:** Two instances of IED Scout were connected to the IEC 61850 Ethernet switch, one publishing the CIBBay_24 GOOSE (right window in figures) and another one subscribed to this GOOSE (left window in figures) to get network latencies with and without cryptography. Port mirror was configured to analyze the network traffic and verify it were encrypted.
- **ICMP traffic:** We tested non-GOOSE traffic too, by sending 1000 ICMP requests at 2 req/sec rate. The results were coherent with the former experiments.

Test method	Mean delay (ms.)
1 - Complete circuit with oscilloscope	1.159
2 – Only GOOSE latency	1.309
3 - ICMP traffic	1.029

Measured delays introduced by cryptography



Encrypted GOOSE's

Conclusion

In this paper we review the security of IEC-61850 and IEC-62351 and the reasons for the lack of cryptographic mechanisms on them. We also review the most common approaches to introduce compensatory measures and propose a new solution based on Zero-Trust-Architecture approach with low-latency encryption.

The experimental results show that a higher level of cybersecurity is achieved without impacting the performance or modifying the configuration of the devices within the network.

In table 3 we summarize which points of the IEC-62443-3-3 and IEC-62443-4-2 are resolved by means of encryption and basic cryptography mechanisms. These standards are of enormous importance in industrial cybersecurity and energy verticals. For the sake of simplicity, we provide a high-level overview of the system and functional requirements.

Requirement	Mentioned in	How encryption and enclave approach solve it
Control system shall protect the integrity of transmitted information	62443-3-3: SR 3.1 62443-4-2: SR 3.1	The appliance supports integrity mechanisms and provides
Control system shall protect the confidentiality of information at rest or in transit.	62443-3-3 and 62443-4-2: SR 4.1, 4.2 and 4.3	All traffic is encrypted among different appliances that support usernames and passwords for authorization
Network segmentation	62443-3-3 and 62443-4-2: SR 5.1	Different keys are used to keep the traffic within the boundaries defined logically and enforced physically by the appliance
The control system shall protect the integrity of sessions	62443-3-3 and 62443-4-2: SR 3.8	Unauthorized messages are discarded as they are not using a valid ID or key
The control system shall protect private keys using hardware mechanisms	62443-4-2: SR 3.11- 3.14	The appliance supports Secure Element or TPM and allows integration with 3rd party PKI
The control system shall support cryptographic mechanisms to recognize changes to information during communication	62443-3-3 and 62443-4-2: SR 4.1, 4.2 and 4.3	Enabled using secure protocols