Dr. Alexander Apostolov

OMICRON electronics

Cyber security threats to IEC 61850 based transmission line protection schemes and what we can do to stop them

6 April 2023

Questions?

> What are we doing?

> Why are we doing it?

> How are we doing it?

What are we doing?

> Detecting abnormal behavior of the electric power system and its protection, automation and control systems

> Defining methods and tools to identify the reasons for the abnormal behavior

> Defining methods and tools to prevent or reduce the impact of abnormal behavior caused by humans

Why are we doing it?

To protect the electric power grid and its equipment from short term or long-term damage caused by:

> Natural weather or other random events

> Human errors during maintenance or system operation

> Intentional actions by disgruntled employees

> Random attacks by unsophisticated hackers

> Malicious attacks by highly skilled hackers

How are we doing it?

Based on:

> Understanding of the threats – operation of primary equipment, change of the configuration of an IED, publishing of IEC 61850 messages, etc.

> Understanding of the impact of specific threats

> Knowledge of the electric power system parameters and connectivity (digital twin)

How are we doing it?

- Knowledge of the electric power system real time topology
- Knowledge of the communications architecture
- Knowledge of the communications system configuration
- Knowledge of the capabilities of the components of the SPACS (digital twins)
- Knowledge of the configuration of the IEDs

How are we doing it?

> Knowledge of the IEC 61850 standard

> Knowledge of the level of implementation of IEC 61850 in the IEDs

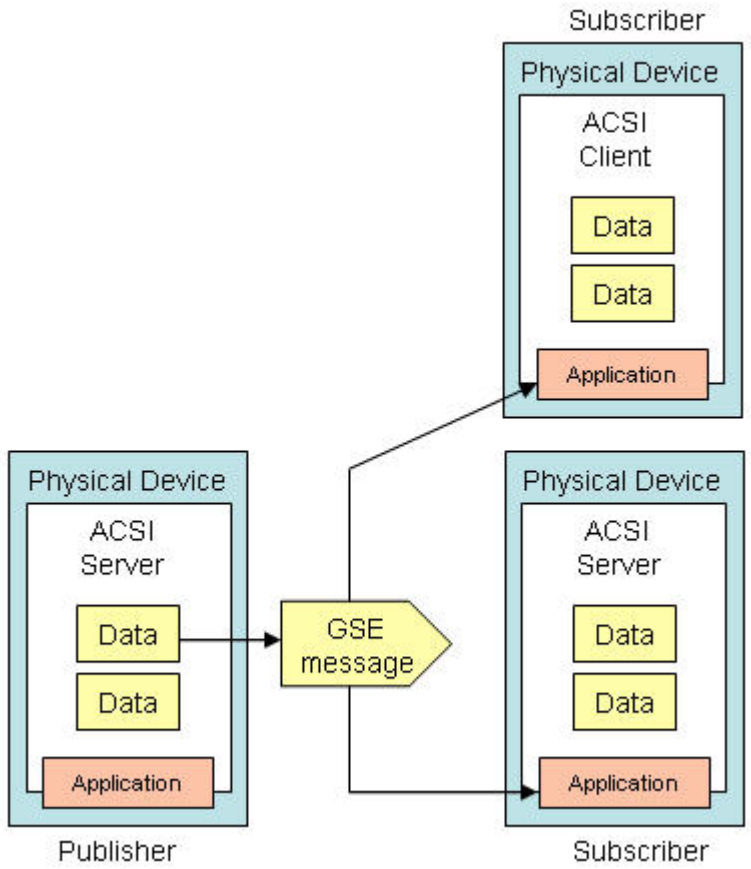
> Knowledge of the test system

> Continuous collection and analysis of data available from various sources – IEDs, MUs, PMUs, weather information, scheduled events information, etc

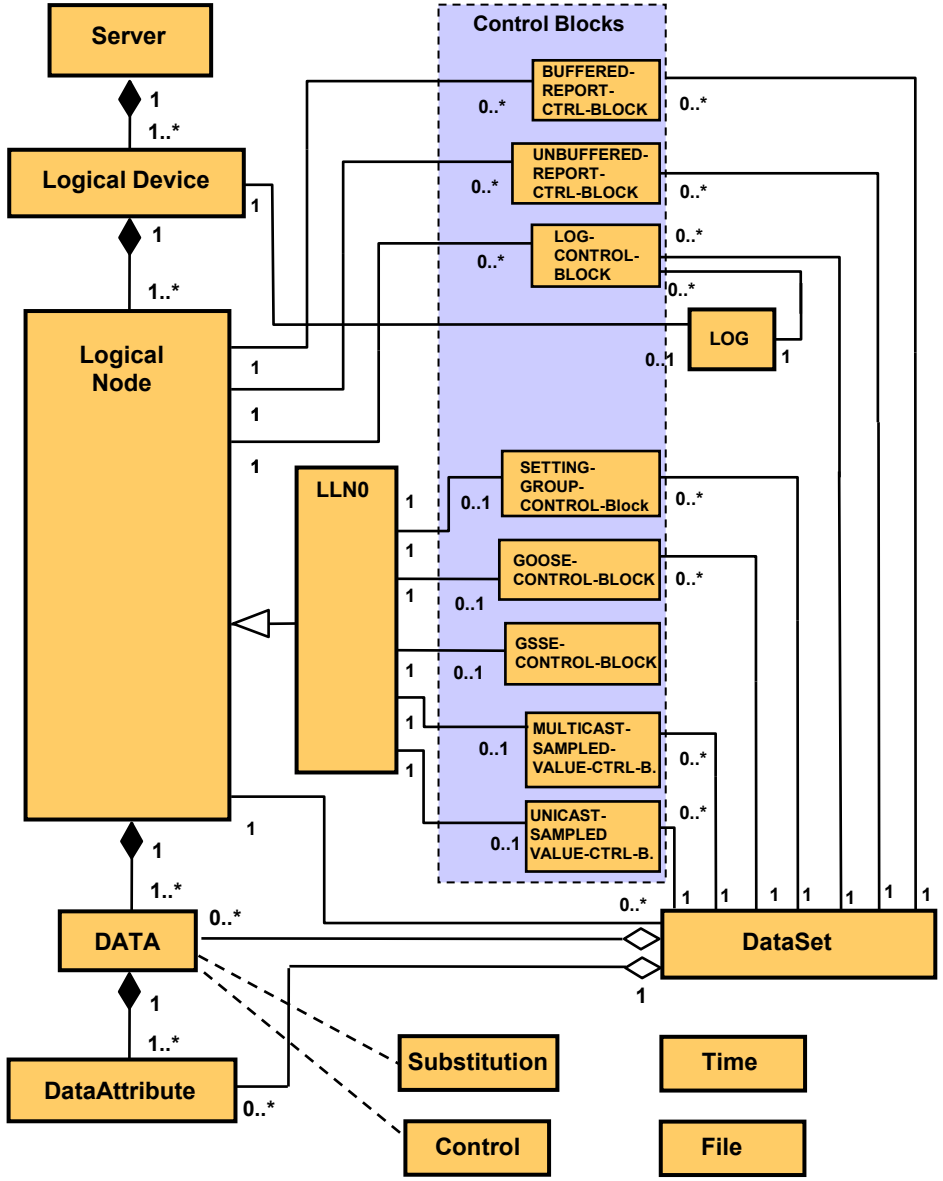
How are we doing it?

> Analysis of the data using different methods – expert systems, AI tools, comparison between predicted behavior and actual behavior, etc.

IEC 61850 Services



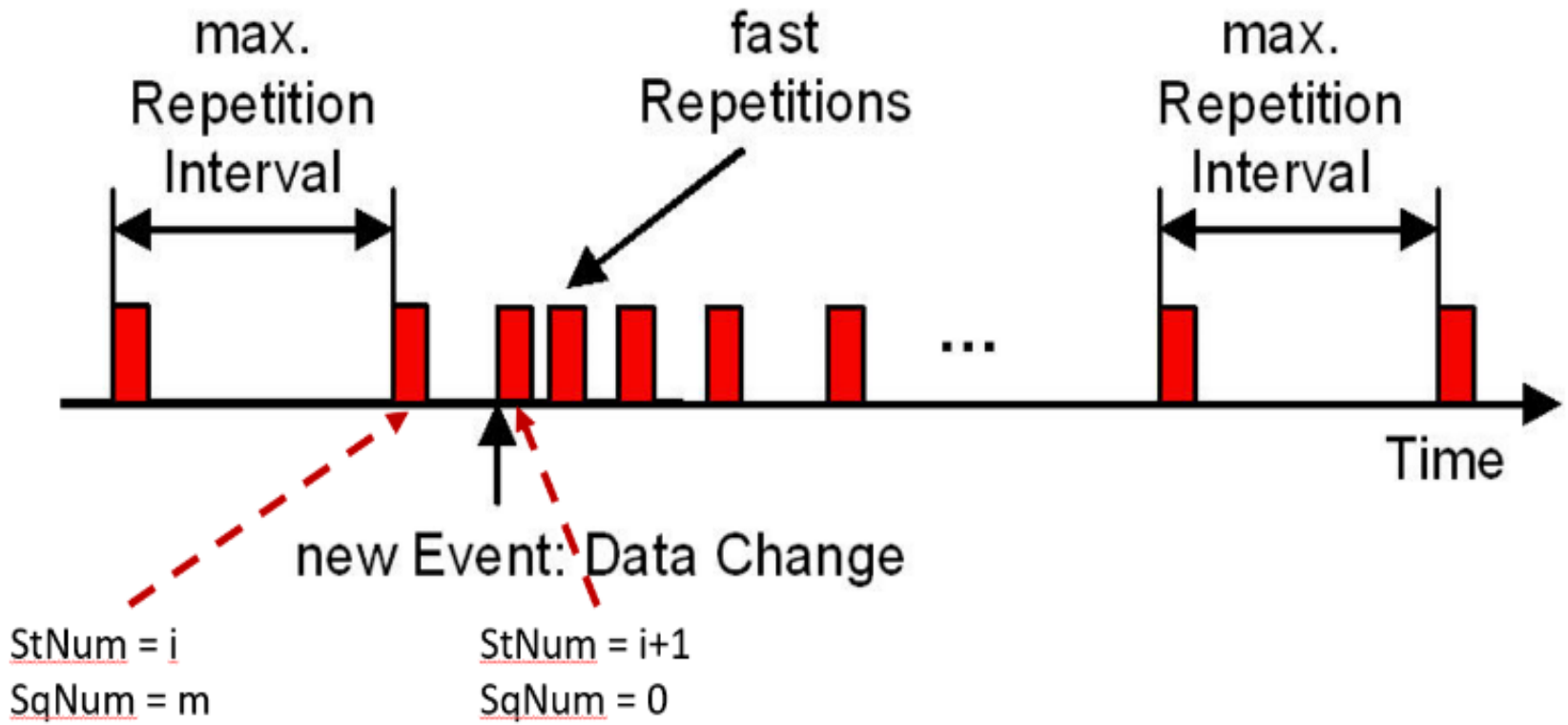
IEC 61850 Services



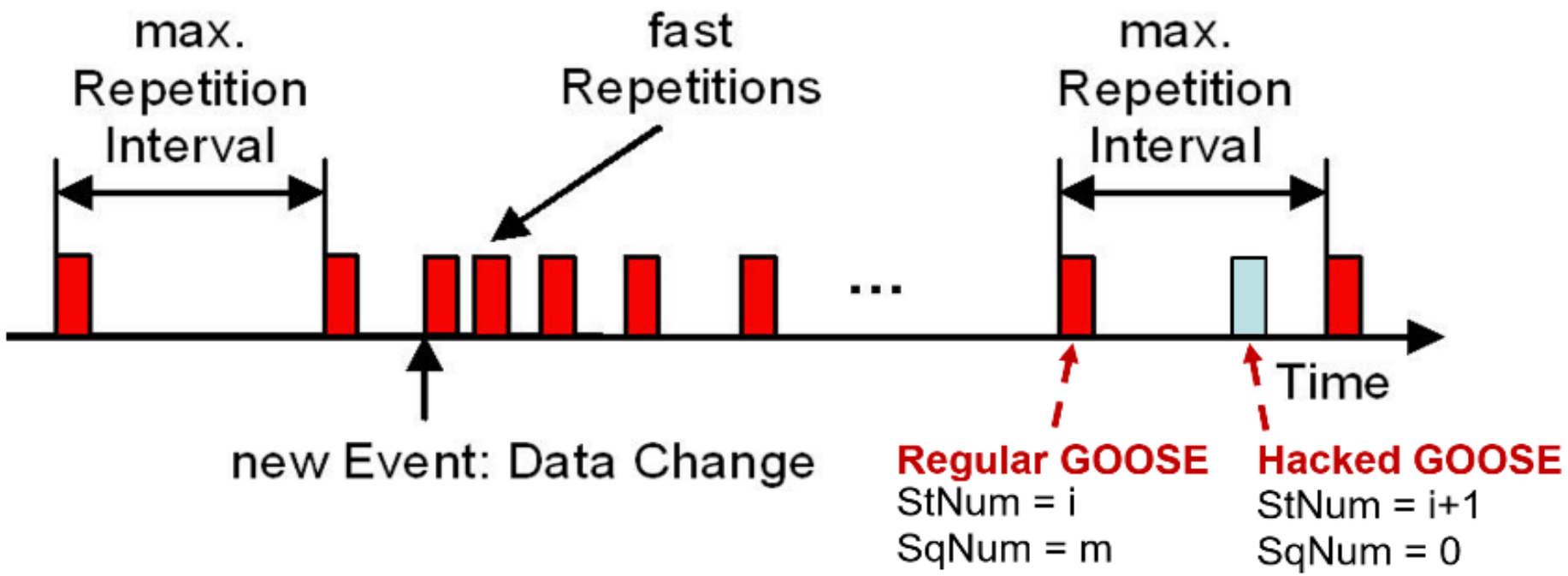
GOOSE message

GOOSE message		
Parameter name	**Parameter type**	**Value/value range/explanation**
DatSet	ObjectReference	Value from the instance of GoCB
GoID	VISIBLE STRING129	Value from the instance of GoCB
GoCBRef	ObjectReference	Value from the instance of GoCB
T	TimeStamp	
StNum	INT32U	
SqNum	INT32U	
Simulation	BOOLEAN	(TRUE) simulation | (FALSE) real values
ConfRev	INT32U	Value from the instance of GoCB
NdsCom	BOOLEAN	Value from the instance of GoCB
GOOSEData [1..n]		
Value	(*)	(*) type depends on the appropriate common data classes (CDC).

GOOSE Messages:



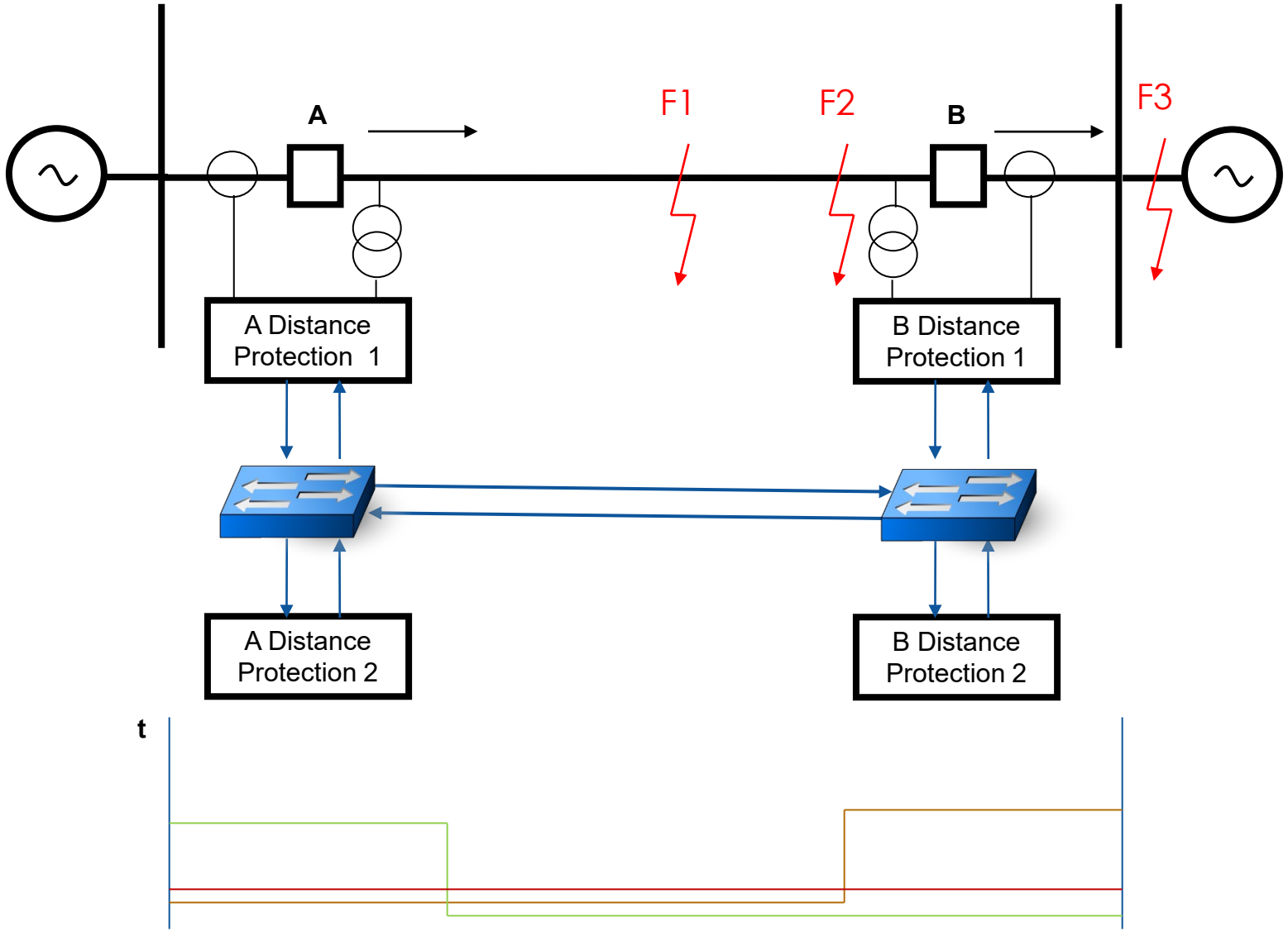
Hacked GOOSE Messages:



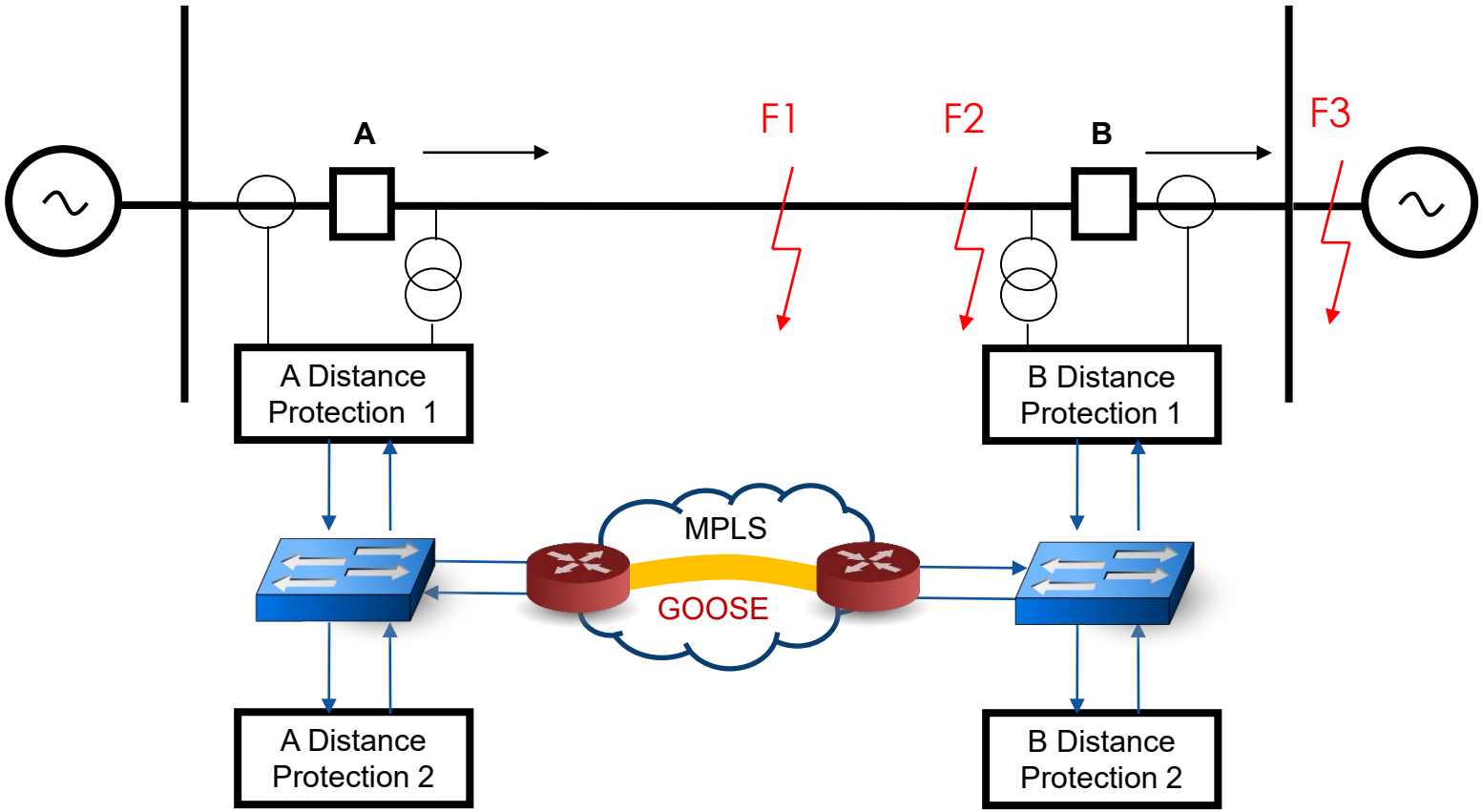
Sampled Values Communications

Hacked Sampled Values Communications

IEC 61850 Based Accelerated Line Protection



IEC 61850 Based Accelerated Line Protection



Security Issues

> Transition from local to some forms of distributed protection functionality

> Requirements for more efficient communications based protection schemes

> Need for local and remote user interface from different types of corporate clients

Security Issues

- Use of protection IEDs as the main data source for integrated data acquisition and control systems
- Use of multifunctional IEDs as distributed power system disturbance recording devices
- It is not an IEC 61850 problem

Threats Sources

> Natural disasters and equipment failure

> Well-intentioned employees who make inadvertent errors, use poor judgment, or are inadequately trained

> Employees with criminal intent to profit or to damage others by the misappropriation of utility resources

> Disgruntled employees or ex-employees who cause damage to satisfy a grudge

Threats Sources

> Hobbyist intruders who gain pleasure from unauthorized access to utility information systems

> Criminal activity by both individuals and organizations directed against the utility, its employees, customers, suppliers, or others

> Terrorists

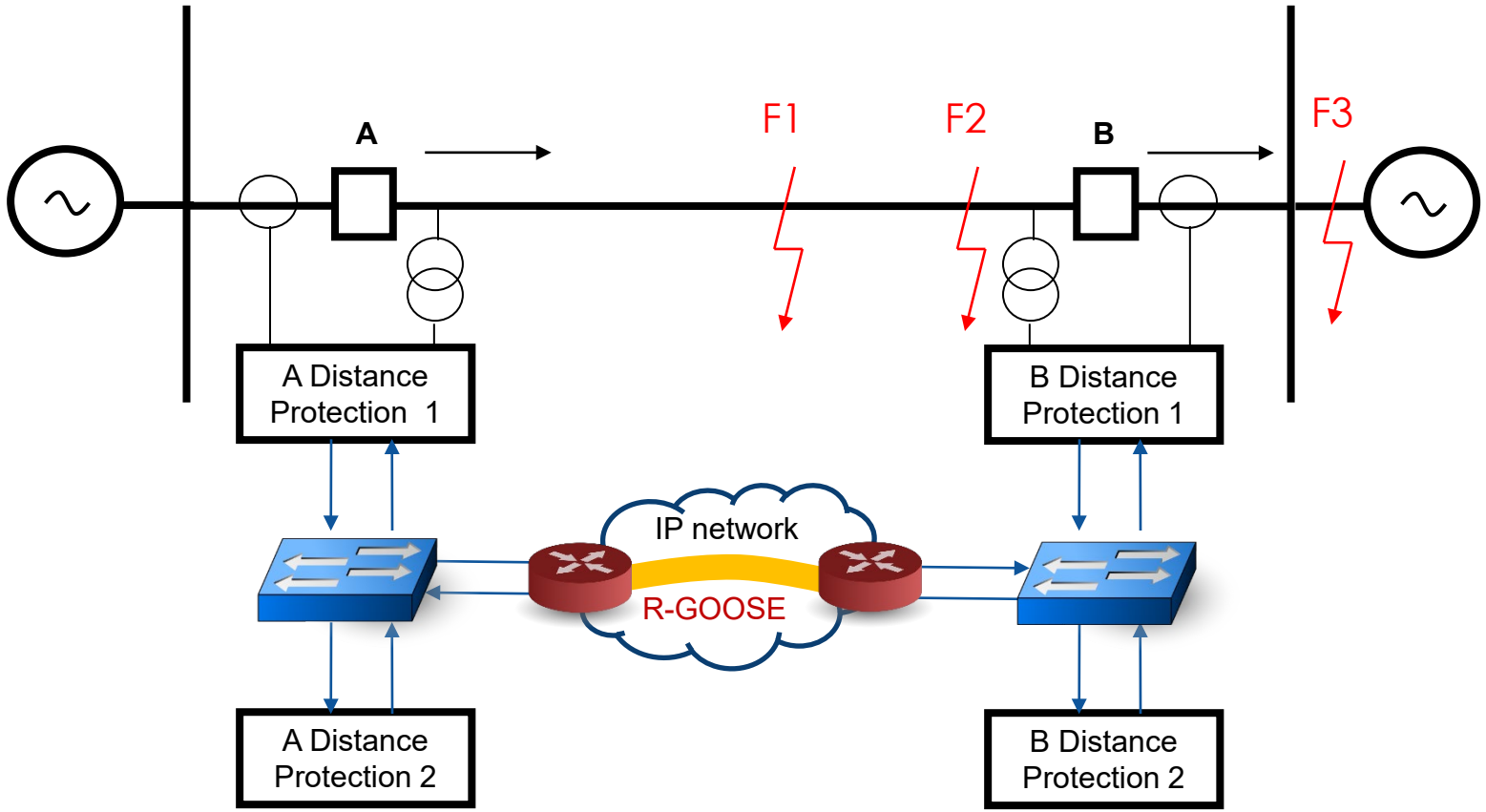
Threats Sources

> Competing organizations searching for proprietary information of the utility, its suppliers, or customers

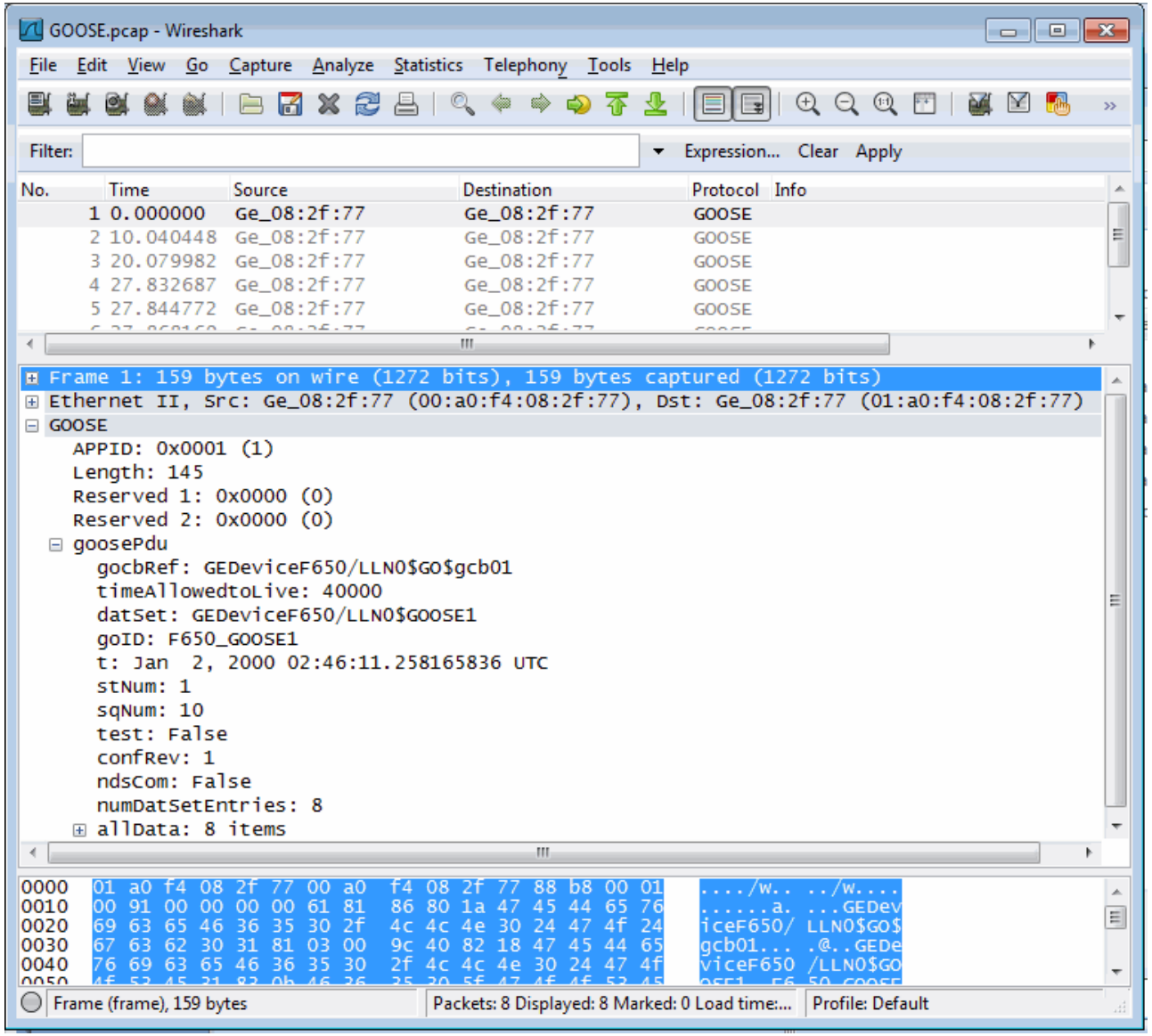
> Unscrupulous participants in the markets for electric power or derivatives

> Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes

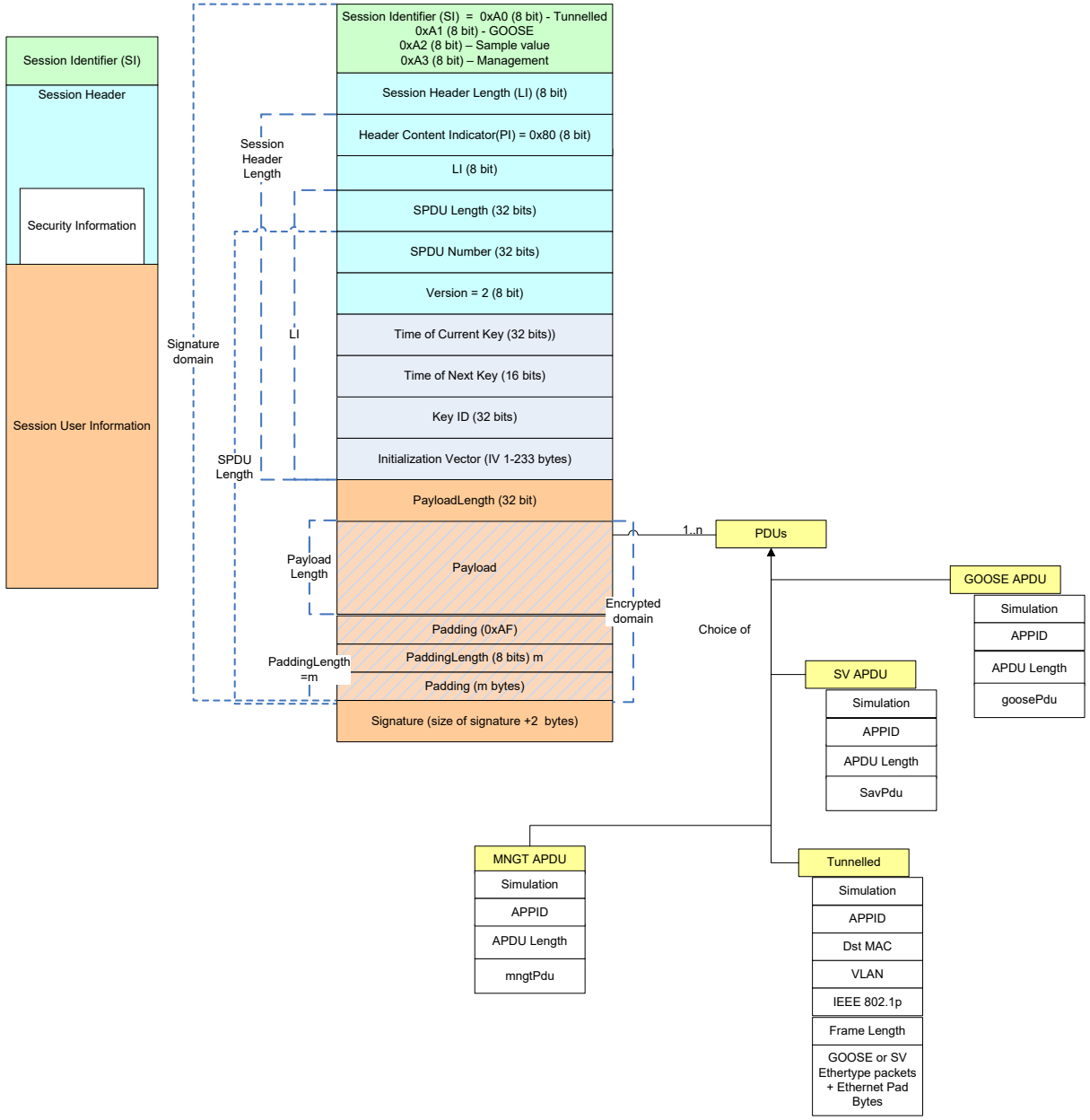
IEC 61850 Based Accelerated Line Protection



GOOSE in WireShark



IEC 61850 90-5 Session Protocol



Functional security

> Based on the protection scheme principle (POTT)

> Based on redundant data (DTT)

Conclusions

> The availability of specific features in the GOOSE publishing mechanisms allows for the development of intrusion detection methods that can be implemented in the subscribing IEDs.
> The intrusion detection is based on the monitoring of state and sequence numbers, as well as data attribute value changes.
> Additional end-to-end security is implemented in R- GOOSE based on IEC 62351-6.
> Using good understanding of the protection system of the transmission line and its operation during different fault conditions can be used to implement a mechanism of “functional security” that will prevent the undesired tripping of the transmission line even if an intruder has been able to successfully avoid the cyber security protection mechanisms.