NAME : Paulo Sergio Pereira Junior	GROUP REF. : B5
COUNTRY : Brazil	PREF. SUBJECT : PS3
REGISTRATION NUMBER : DLG5073	QUESTION N° : 3.06

Question nº 3.06: **What are your experiences to monitoring of IEC 61850 based PACS and how you secure the operation of critical infrastructure and respond to the incidents?**

PACS network must incorporate monitoring functions, considering cybersecurity aspects, able to:

1) Detect and point out anomalies or lacking of messages, like GOOSE or SV, or yet unforeseen messages;
2) Detect lacking of synchronism signal;
3) Verify and point out abnormal propagation time, i.e. latency, and asymmetry or excessive variation, i.e. jitter, of messages propagation times;
4) Be implemented in a independent way of protection devices or local teleprotection devices;
5) Have resources for storing event records of detected anomalies.

Figure 1 exemplifies a monitoring system setup:

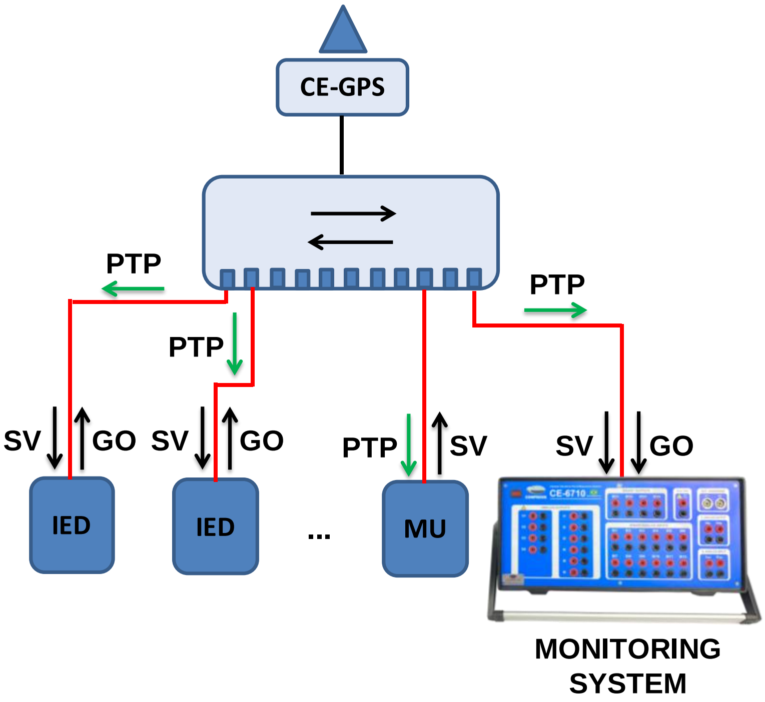


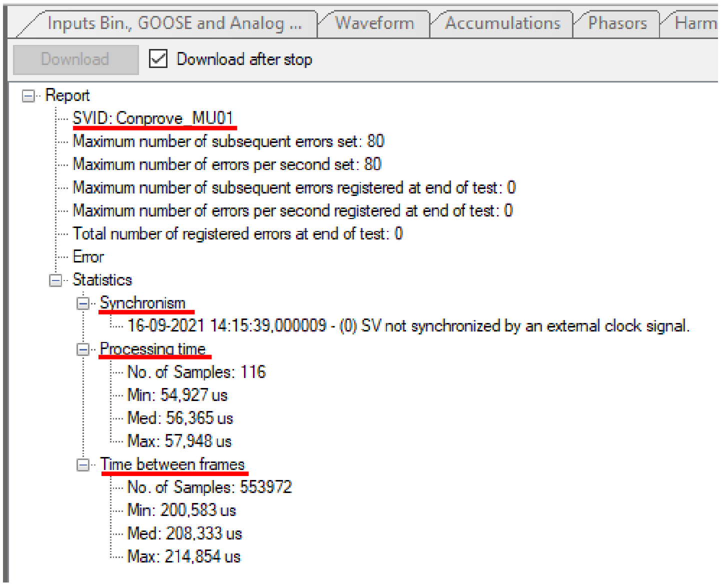
Figure 1 - Monitoring Sytem Setup

Considering Sampled Values, the goal is to verify propagation delay, processing time and time between frames. The first one is the time that a message takes to leave one device´s Ethernet port and enter another device´s Ethernet port, i.e. the network latency time. It is important for the monitoring system to verify the propagation delay and to analyze if there is a network overload.

The processing time is the time a MU/SAMU takes to sample the signals that are coming from instrument transformers, to encapsulate them into the standard frame and to publish them, plus the network latency time. Thus, the users can analyze if it is going out of the ordinary time of processing. Also, the number of SV frames errors in the network and the synchronism flag can be verified.

The time between frames indicates if the MU/SAMU is sampling properly according to what was set. This functionality can be implemented by the monitoring system just marking the frame’s incoming time on the network board and getting the difference between them.

Figure 2 exemplifies these statistical analysis of SV frames.



```
⊟ Report
   SVID: Conprove_MU01
   Maximum number of subsequent errors set: 80
   Maximum number of errors per second set: 80
   Maximum number of subsequent errors registered at end of test: 0
   Maximum number of errors per second registered at end of test: 0
   Total number of registered errors at end of test: 0
   Error
   ⊟ Statistics
      ⊟ Synchronism
            16-09-2021 14:15:39,000009 - (0) SV not synchronized by an external clock signal.
      ⊟ Processing time
            No. of Samples: 116
            Min: 54,927 us
            Med: 56,365 us
            Max: 57,948 us
      ⊟ Time between frames
            No. of Samples: 553972
            Min: 200,583 us
            Med: 208,333 us
            Max: 214,854 us
```

Figure 2 - Example of Statistical Analysis of SV Frames

In the case of GOOSE, the goal is to calculate the transfer time and to verify if it was under the limits defined by the IEC 61850-5 according to the performance classes defined in IEC 61850-8-1.

Based on item 11.1.1.4 of IEC 61850-5 Ed.2, the transfer time is defined as the complete frame´s transmission time including the processing of publisher and subscriber. In details, it is the sum of three times: t_a, t_b and t_c, where:

- t_a is the time counted from the moment the publisher puts the frame on top of its transmission stack (coding) to the moment it is sent to the network;
- t_b is the network latency time;
- t_c is the time counted from the frame´s incoming moment at the subscriber to the frame is extracted from the receiving stack.

Figure 3 illustrates the transfer time´s concept and Figure 4 gives an example of Transfer Time statistics.

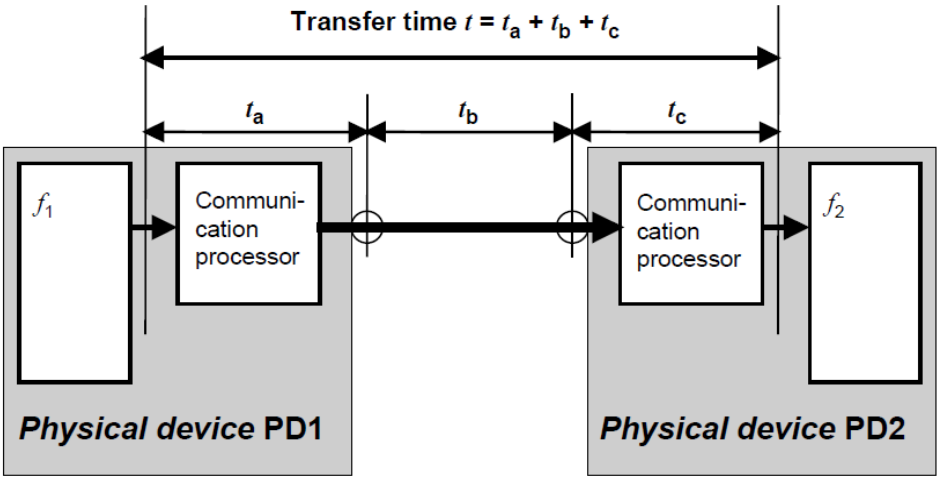
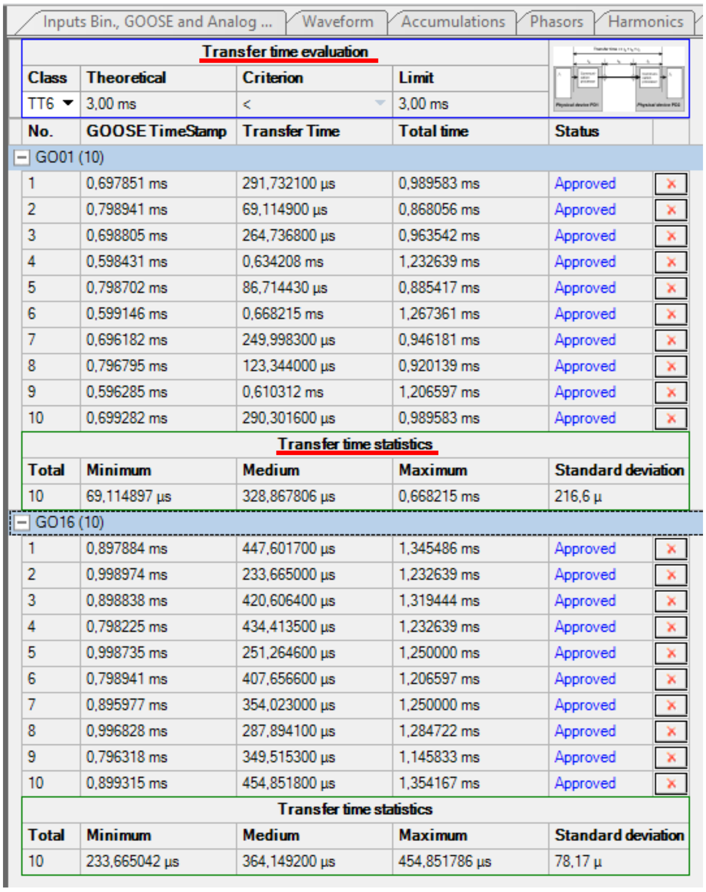


Figure 3 - The Concept of Transfer Time



Transfer time evaluation

Class	Theoretical	Criterion	Limit
TT6	3,00 ms	<	3,00 ms

No.	GOOSE TimeStamp	Transfer Time	Total time	Status	
GO01 (10)					
1	0,697851 ms	291,732100 µs	0,989583 ms	Approved	✕
2	0,798941 ms	69,114900 µs	0,868056 ms	Approved	✕
3	0,698805 ms	264,736800 µs	0,963542 ms	Approved	✕
4	0,598431 ms	0,634208 ms	1,232639 ms	Approved	✕
5	0,798702 ms	86,714430 µs	0,885417 ms	Approved	✕
6	0,599146 ms	0,668215 ms	1,267361 ms	Approved	✕
7	0,696182 ms	249,998300 µs	0,946181 ms	Approved	✕
8	0,796795 ms	123,344000 µs	0,920139 ms	Approved	✕
9	0,596285 ms	0,610312 ms	1,206597 ms	Approved	✕
10	0,699282 ms	290,301600 µs	0,989583 ms	Approved	✕

Transfer time statistics

Total	Minimum	Medium	Maximum	Standard deviation
10	69,114897 µs	328,867806 µs	0,668215 ms	216,6 µ

No.	GOOSE TimeStamp	Transfer Time	Total time	Status	
GO16 (10)					
1	0,897884 ms	447,601700 µs	1,345486 ms	Approved	✕
2	0,998974 ms	233,665000 µs	1,232639 ms	Approved	✕
3	0,898838 ms	420,606400 µs	1,319444 ms	Approved	✕
4	0,798225 ms	434,413500 µs	1,232639 ms	Approved	✕
5	0,998735 ms	251,264600 µs	1,250000 ms	Approved	✕
6	0,798941 ms	407,656600 µs	1,206597 ms	Approved	✕
7	0,895977 ms	354,023000 µs	1,250000 ms	Approved	✕
8	0,996828 ms	287,894100 µs	1,284722 ms	Approved	✕
9	0,796318 ms	349,515300 µs	1,145833 ms	Approved	✕
10	0,899315 ms	454,851800 µs	1,354167 ms	Approved	✕

Transfer time statistics

Total	Minimum	Medium	Maximum	Standard deviation
10	233,665042 µs	364,149200 µs	454,851786 µs	78,17 µ

Figure 4 - Example of Transfer Time Statistics

Besides GOOSE Transfer Time, the monitoring system must verify if all the frames are running on the network according to SCL file, if the retransmission time is correct and if the frames are not out of order through State Number and Sequence Number analysis.

Considering PTP synchronism, it is important to verify if the Grand Master frames are running on the network through Announce and Sync frames analysis. Also, the monitoring system must be a PTP slave in order to verify if the slave clock jitter is increasing in relation to master clock.

It is imperative that PACS network incorporates mechanisms that offer cybersecurity to prevent incidents and to ensure the following topics:

1) Confidentiality: to limit data access to authorized users only;
2) Integrity: to ensure that are no unauthorized modifications of messages data or information steals;
3) Availability: to ensure authorized access to data or services;
4) Authenticity: to ensure that the data comes from a legitimate source.

So, a cybernetic incident in PACS can be defined as an event that compromises really or potentially the availability, integrity, confidentiality or authenticity of the PACS network.

This way, cybersecurity devices must be configured to set an alarm in case of threat:

- Alarm configurations rules must be periodically reviewed;
- All the alarms must be logged and sent immediately to the cybersecurity staff;
- All the alarms must be analyzed and treated in the correct deadline defined by the security policy.

The NIST (National Institute of Standards and Technology) SP (Special Publication) 800 – series comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities.

NIST SP 800 – 61 rev. 2 provides guidelines for detecting, analyzing, prioritizing and handling incidents to respond to them effectively and efficiently. Item 3 - "Handling an Incident" - describes the main phases of the incident response process: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

In the Preparation phase, the incident response team must be established and trained; the necessary tools and resources must be acquired; the organization must select and implement a set of controls based on the results of risk assessment. This way, the company must try to limit the number of incidents that will occur.

In the Detection and Analysis step, the organization must be alerted about detection of security breaches whenever an incident occurs. Regarding this, there are some manners to implement security incident alert and timely inform the operator and the maintainer, through: publishing of GOOSE frames, MMS reports, binary outputs, emails, panel LEDs and etc. This way, each network monitoring and cybersecurity vendor can choose one or more manner to implement this solution. So, after analyse the threat´s gravity, the company can mitigate the impact of the incident by containing it and ultimately recovering from it. This phase, consisting of these two steps, is cyclical until the threat is eradicated.

Finally, in the Post-Incident Activity phase, the organization must issue a report that details the cause and cost of the incident and the steps the company must take to prevent future incidents, returning, this way, to the first phase.

Figure 5 exemplifies the phases of the incident response process.

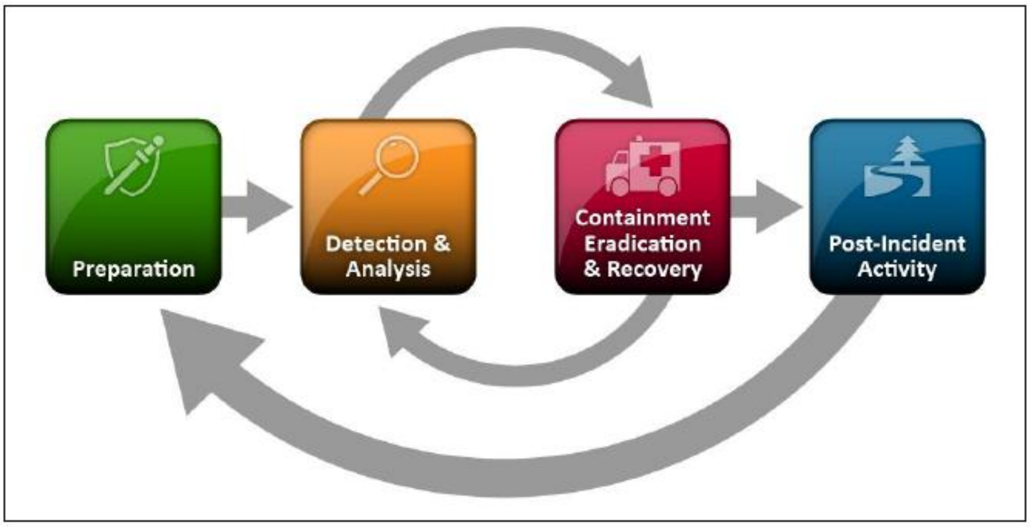


Figure 5 - Incident Response Process