Paris Session
2022

For power system expertise

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?

B5-PS3

Q3.06

Paulo Junior - Brazil

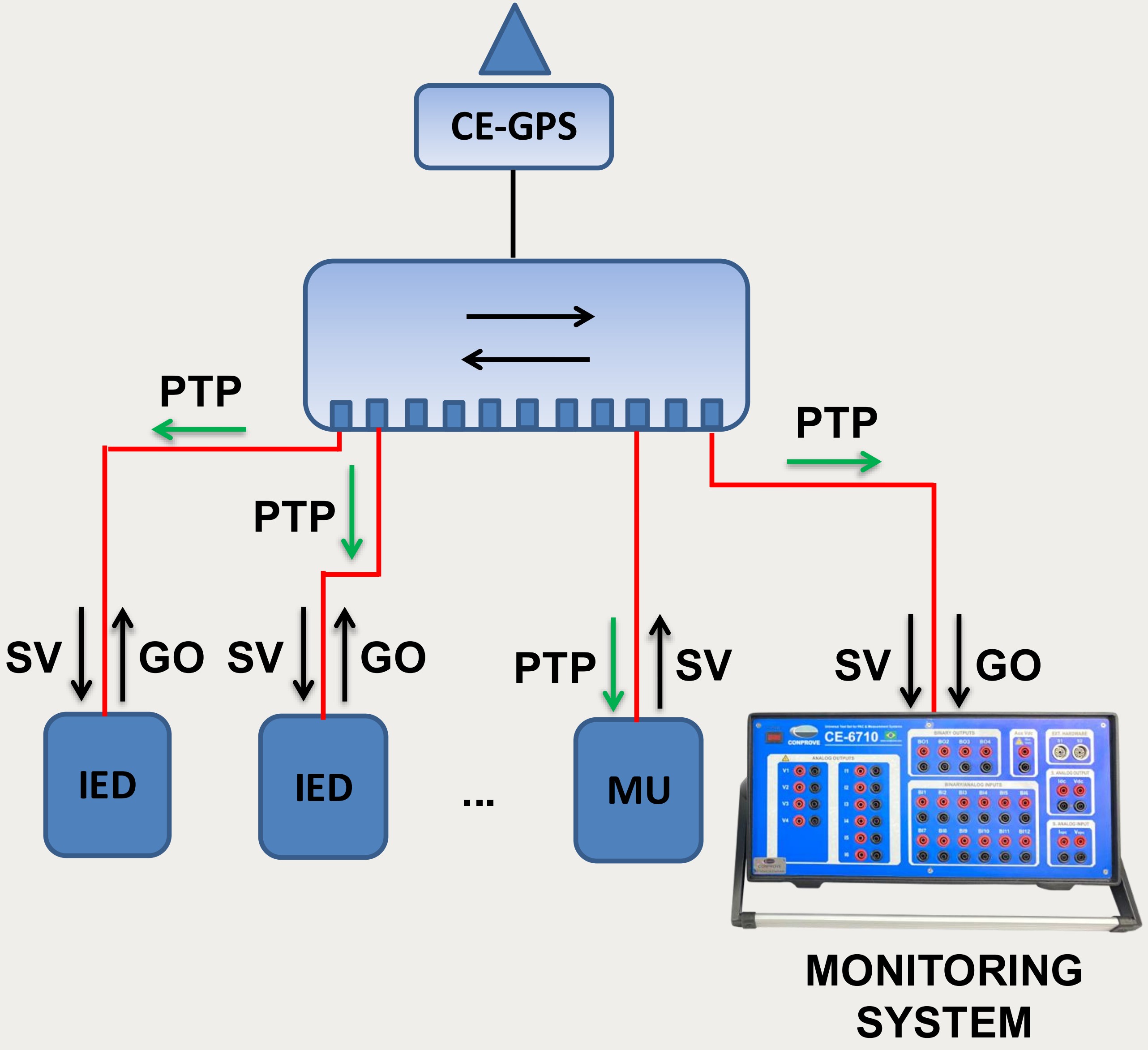
CONPROVE

Q3.06

- ***PACS network*** must incorporate ***monitoring functions*** able to:
  - Detect and point out ***anomalies*** or ***lacking*** of messages, like ***GOOSE*** or ***SV***, or yet ***unforeseen messages***;
  - Detect ***lacking of synchronism*** signal;
  - Verify and point out ***abnormal propagation time***, i.e. ***latency***, and asymmetry or excessive variation, i.e. ***jitter***;
  - Be implemented in a ***independent*** way of protection devices or local teleprotection devices;
  - Resources for ***storing event records*** of ***detected anomalies***.

Q3.06

- Sampled Values:
  - Propagation delay;
  - Processing time;
  - Time between frames;
  - Lost and errors;
  - Sync flag.
- GOOSE:
  - Is GOOSE there?
  - Retransmission time;
  - SqNum and StNum order;
  - Transfer Time.
- PTP:
  - Announce/Sync frames;
  - Errors and jitter.

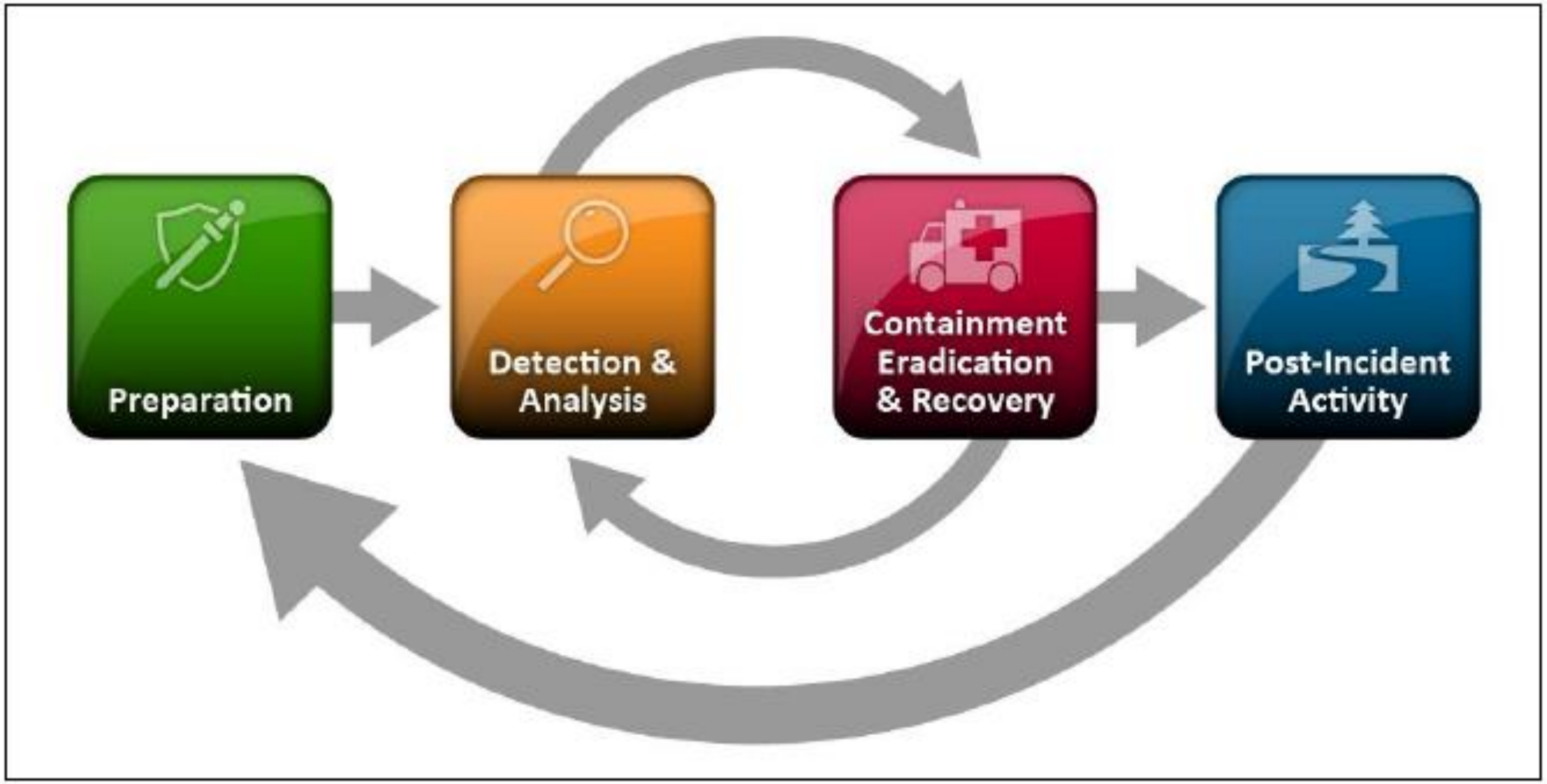


Q3.06

- 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***.

Q3.06

- ***NIST SP 800 Series***:
  - ***SP 800-61 Rev. 2 – Section 3***: Basic incident handling steps and provides advice for performing incident handling more effectively, particularly incident detection and analysis.



Group Disc