NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PMUs & Critical Infrastructure Protection

Ryan D. Quint
NERC

Ken Martin
EPG

Sarma Nuthalapati
TAMU

NASPI Work Group Meeting
October 2016

RELIABILITY | ACCOUNTABILITY




Disclaimer

- *The material presented here is not intended as compliance guidance. Its sole purpose is to describe the technical aspects of the material being discussed.*
- *For questions related to compliance, please contact NERC Compliance Department directly.*

- *When we are discussing considerations related to the Bulk Electric System (BES). Statements regarding treatment of assets, ensuring reliability, control, decision making, etc., are related to BES Elements under NERC jurisdiction.*

Fundamentals

- Maintain physical and cyber security
  - **High priority**
  - Sufficient and **robust** levels of security
  - **Every** entity associated with reliable operation of the BPS
  - **Every** Element of the bulk power system (BPS)
- Protect your cyber and physical assets
- Continued PMU deployment – technology advancement
- Coexisting with protection, measurement, and other systems
- PMU data closer to real-time applications and decision making
  - Data being used as another measurement source for existing apps
  - New advanced apps providing improved situational awareness
- Cyber security practices and standards continuing to evolve

The 50,000 Foot Answer

If the PMU data is used to make **real-time decisions about the BES**

Within a **15 minute time horizon**

Or is **part of an autonomous control scheme on the BES**

Then the PMUs and associated infrastructure
are **BES Cyber Assets** and part of the **CIP** program.

BES Cyber Systems & Cyber Assets

- BES Cyber System is a grouping methodology
  - Provides flexibility for application of CIP standards
- BES Cyber System comprised of one or more BES Cyber Assets
  - Individual components – protective relay, PMU, RTU, etc.
- Core building block is the BES Cyber Asset
  - Can be grouped at entity's discretion to form BES Cyber Systems

PMUs in Digital Relays

- CIP standards are “device centric”

- If the relay is in scope because of its protection function, the entire relay device is in scope
  - PMU function is just one more data source

IF…

- The relay is considered “CIP” because of its protection function

THEN…

- The device is “CIP” – PMU data is just another functionality

PMUs in Digital Relays

IF…

- The relay is NOT considered “CIP” for some reason

BUT…

- The PMU data is used for operational decision making within the 15 minute time horizon

THEN…

- The device is “CIP” – PMU data will then make it “CIP”

Control Center Displays

IF…

- The PMU data is serving situational awareness purposes ONLY

AND…

- The displays are not used for making operational decisions (no dispatcher instructions tied directly to them)

  OR

- The operational decisions have been determined to be outside a 15-minute time horizon (*auditors would likely verify with operator interview*)

THEN…

- The PMUs and associated infrastructure **probably not** "CIP"

Control Center Displays

IF…

- The PMU data is serving control center applications used by operators

AND…

- The operational decisions are within a 15-minute time horizon

THEN…

- The PMUs and associated infrastructure **likely** “CIP”

PMU-Based Advanced Applications

IF…

- The PMU data is feeding an autonomous real-time application

AND…

- An operational decision could be made based on information from the application within a 15-minute time horizon

THEN…

- The PMUs and associated infrastructure **definitely** “CIP”

Alarming

IF…

- The PMU data is used for alarming in the control center
  - Voltage magnitudes
  - Phase angle limits
  - Underfrequency alarm
  - Oscillation damping alarms

AND…

- The operational decisions are within a 15-minute time horizon

THEN …

- PMUs and associated infrastructure **likely** “CIP”

Dispatcher Standing Orders

- Dependent on operator action timeframe

- **COULD** the operator action be within 15 minute time horizon?
  - If so, then they **will** meet the "CIP" definition.
  - If not, can you ensure it is outside the 15 minute time horizon?

- If the operator is going to take action on the data/information from the data AND that action could be within 15 minutes, then they meet the definition.

Operator vs. Engineer

"My dispatcher order is to get an Ops engineer…"

- Definition does not distinguish between who makes the decision, just that a decision is made within 15 minutes
- If order is to "leave a note" for Ops engineer to look at later, then it **is not** a 15 minute time horizon
- If the Ops engineer could make a decision within 15 minutes time horizon, then it **is** "CIP"

- Operator vs. engineer does not matter here

Overall Considerations

- Does the operator look to other data for further action?
- Does the operator ultimately use this data to make the decision within a 15 minute time horizon?
- What would happen if the PMU-based app failed to operate correctly?
- What would happen if the PMU-based app misoperated?
- What would happen if the data supplied by the PMU was modified or corrupted (more than unavailable)?
- What other data sources would then be reacted to?
- What are the dispatcher standing orders in response to the data?
  - Increased monitoring vs. taking immediate action

Integration with EMS & Advanced Applications

- Integration to EMS system and data historian does not necessarily mean PMU architecture is “CIP”

BUT…

- If the PMUs are added to EMS systems that use the data for operational decision making within 15 minute time horizon, they are **definitely** “CIP”
  - State estimation, economic dispatch, operational alarming

- The data is being used autonomously be real-time applications, and the output **is** used within the 15 minute time horizon

Another Data Source

"My PMUs are just another meter providing data to downstream applications"

- Great, so they're treated like the other types of meters for cyber security
  - RTUs
  - Tie-line meters
  - Breaker position indicators protective relays
  - Frequency, bus voltage, current meters
  - Etc.
- They're treated like CIP Cyber Assets because they're used by the myriad applications operators depend on
- Classify the primary data source as BES Cyber Assets, apply appropriate protection to prevent misuse of data

Communications Systems

If PMU data and associated architecture are “CIP”, then does that make the entire communications system “CIP”?

- Current exemptions for communications systems “between discrete ESPs”
  - Wide area component of communications infrastructure
  - No current plans to remove this exemption
- Unless and until this changes for traditional SCADA data, likely will not affect PMU data communications infrastructure
  - Often the same anyways
- There are no CIP requirements for encryption of real-time data
- Current SDT addressing FERC directive for comms between control centers, but not looking at field communications

Local Network Architecture

Example:

- At stations with “medium impact BES Cyber Assets/Systems” with routable protocol (Internet Protocol – IP – network)
  - Electronic Security Perimeter (ESP) must be drawn to include BES Cyber Assets (CA)
  - If PMU on that network, PMU is included in program as “Protected Cyber Asset (PCA)” – even if PMU is research-only
  - Rationale is PMU can interact with the BES Cyber Assets, adversely impact those devices, so needs to be protected just like a BES CA
  - For it to not be considered, it would need a firewall device between it and the BES CA network (moving it outside the ESP)

Timing Infrastructure

- Inside the station, the equipment will be included as part of the internal “local-area network”
  - GPS receiver
  - Clock or timing equipment
  - Distribution of this timing
- Anything wide-area receives the same exemption as communications systems
  - GPS radio signal
  - GPS constellation of satellites

TO / TOP / ISO / RC

- Entity function or registration does not matter
- Whether data from PMU could be used to make operational decisions within 15 minute time horizon **does** matter
- Bi-direction consideration of “CIP”

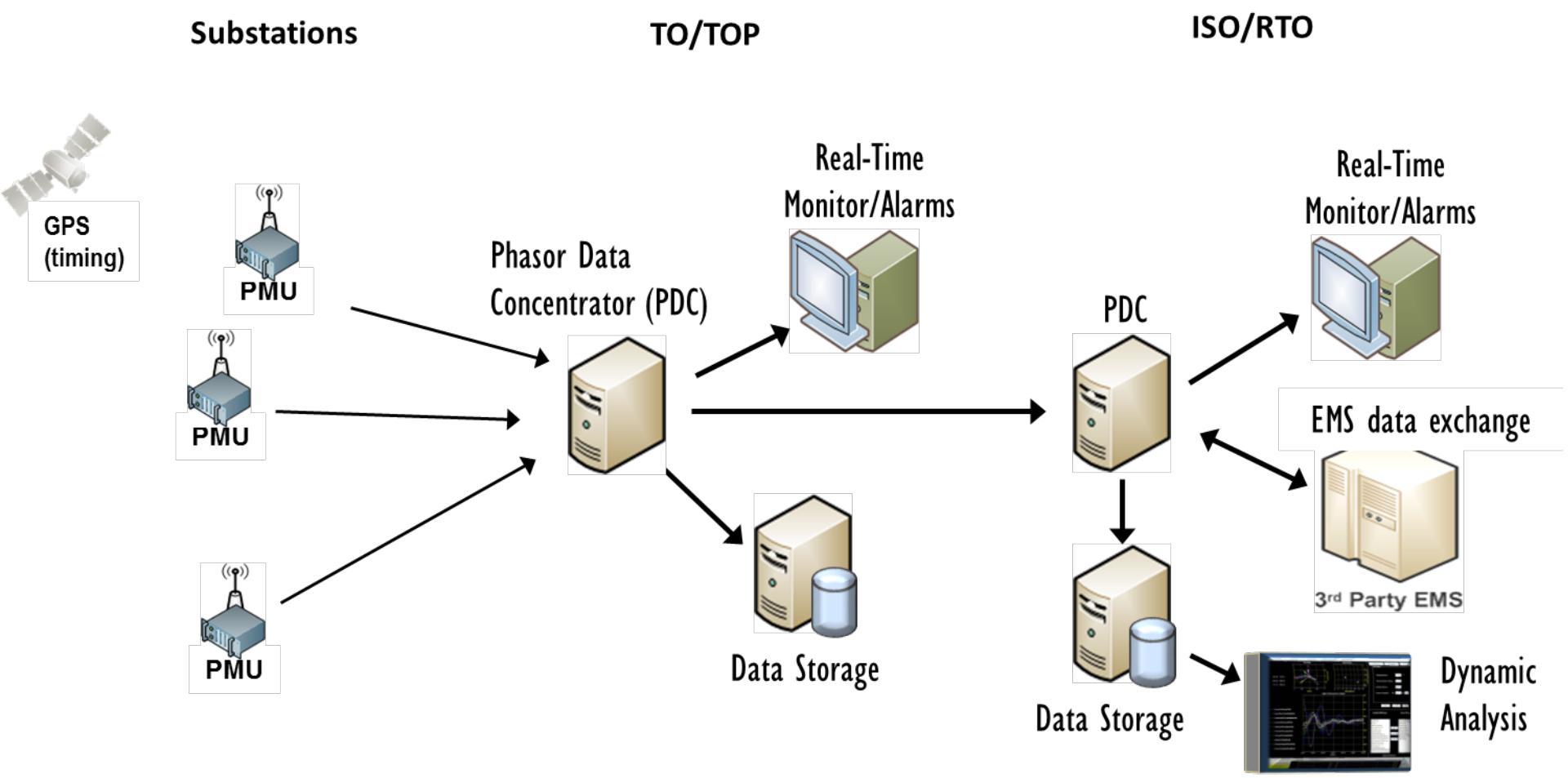
IF…

- ISO/RC uses the PMU data for advanced apps or operational decision making…

THEN…

- The equipment at substation and at control center **is** “CIP”

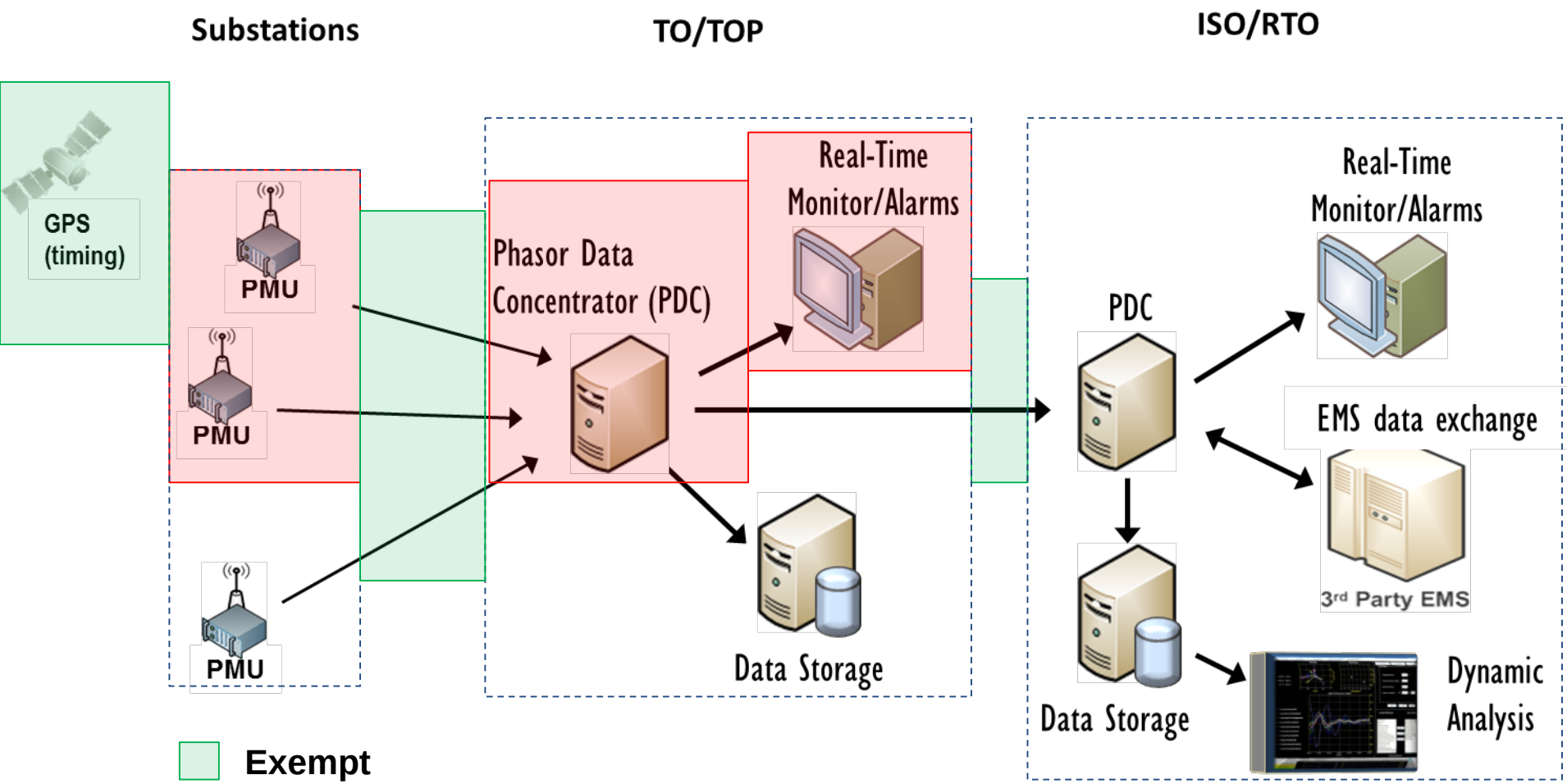
Example Scenarios



Source: Ken Martin, EPG

Example Scenario 1a: Oscillation Analysis at TOP Level

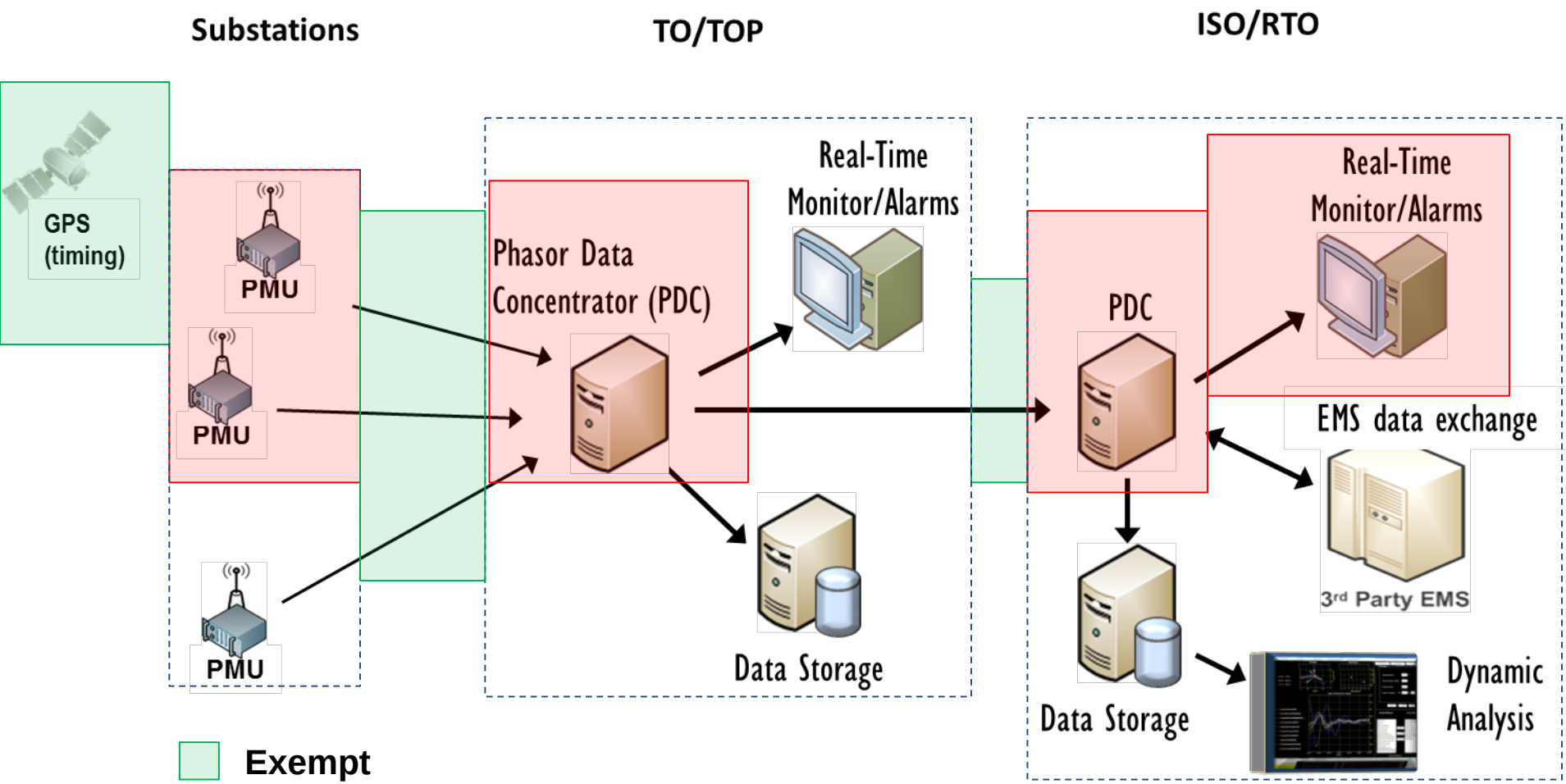
Illustrative Example Only



Source: Ken Martin, EPG

Example Scenario 1b: Oscillation Analysis at ISO Level

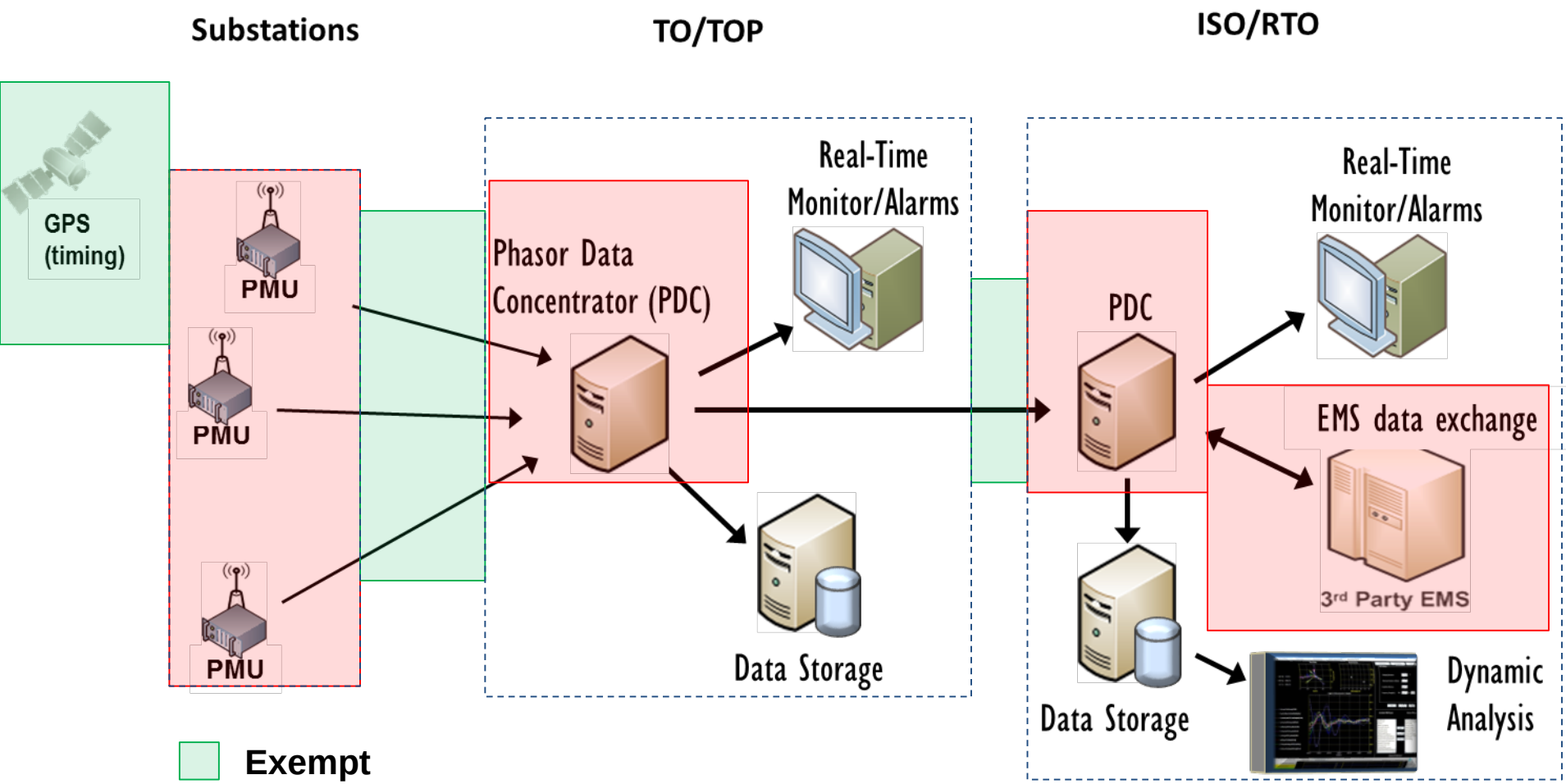
Illustrative Example Only



Source: Ken Martin, EPG

Example Scenario 2: State Estimation at RC Level

Illustrative Example Only



Source: Ken Martin, EPG

Applicability

- Applicability applies to all listed functional entities
- Entity categorizes BES Cyber Systems and Cyber Assets according to criteria
- Related to BES reliability operating services

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Questions?