Building an Architecture Based on IP-Multicast for Large Phasor Measurement Unit (PMU) Networks

Maik Seewald
Cisco

Abstract: **The document describes a distributed, scalable, secure and standard-based approach for the transmission of synchrophasor data over long distances in order to determine the condition of the electrical power network. With the integration of a high number of renewable and distributed energy resources and the resulting ramifications, such information becomes more and more relevant for the stability of the power grid. The paper focuses on the utilization of IP (Internet Protocol)-based network technologies as the foundation for the transport of synchrophasor data defined by the standard IEC 61850-90-5 in order to support the underlying use cases and applications of the domain such as WAMPAC (Wide Area Monitoring Protection and Control).**

Introduction: Grid modernization efforts and the integration of the renewables along with the growing demand of energy are the main drivers to establish greater situational awareness of power grid state. Higher visibility into the power grid is important to maintain reliability and stability in order to prevent power outages as well as other critical situations. This demand leads to new use cases and applications that must be supported by the underlying network infrastructure and the connected systems. Synchrophasor data, measured and calculated by PMUs, provides visibility by delivering information on the condition of the electrical power network. With the on-going trend towards combined functionality, PMU's are already integrated in modern Intelligent Electronic Devices (IEDs). Synchrophasor data, a basic mathematical element for AC power systems, must be time-synchronized to be combined and can be used in variety of use cases such as:

- WAMPAC (Wide Area Monitoring Protection and Control)
- State Determination
- Real time Congestion Management
- Distributed Protection (Schemas)

All data produced and sent by PMU's needs one or more consumers. Today, Control and Data Centers typically receive and process this data which can be used in the following applications:

- Online Analytic applications and tools
- Data Historians
- Visualization and State Estimator applications
- SCADA applications and Energy Management System (EMS)

In order to connect systems and devices, data formats must be standardized to achieve interoperability. For PMU data, the following standards exist:

- IEEE C37.118-2005
- IEC 61850-8-1 (GOOSE)
- IEC 61850-9-2 (Sample Values)
- IEC TR 61850-90-5

As of today, the component architecture for PMU networks typically consists of Phasor Data Concentrators (PDC) and often so-called "Super-PDC's" that encompass certain additional functionality. A PDC receives synchrophasor measurements from one or more PDU's based on IP-Unicast network transmission. PDC's aggregate and correlate the data (time-stamp wise) and might send it to another PDC. This type of a chain is often referred to as *PDC stacking*. Finally, the synchrophasor measurements are received by the predefined subscribing applications that are typically located in the control and operations center. Other forwarding paths to additional subscribing entities may exist. Typically, such forwarding mechanisms use middleware solutions and introduce additional jitter and delay to the transmission of the measurements.

New functional and non-functional requirements such as the growing number of PMU's, the related subscribing entities for synchrophasor data as well as their geographical location and extension reveal the limitations of the existing architecture:

- Limited scalability
- Missing concepts for intra- and inter-domain traffic
- Latency and limited throughput caused by PDC stacking
- Lack of standards for data transport and security
- Resulting issues regarding interoperability

An IP Multicast Architecture for PMU data transport

A new network and system architecture is needed to meet the main functional and non-functional requirements listed by the subsequent bullet points:

- Low latency
- Quality of Service (QoS)
- Predictable fail-over and network convergence
- Scalability and agility
- Strong security

The proposed architecture addresses these requirements comprehensively and meets important quality attributes like extensibility, flexibility, and robustness. It allocates critical functionality to proper places in the system, avoids the definition of new system entities and is built on open standards (e.g.: IETF, IEC). The underlying network architecture addresses the fact that a PMU is a classical multicast streaming source. It sends a continuous stream of measurement data to a number of subscribers. It is a logical step to consider IP-Multicast as the proper network architecture to implement this communication pattern. In this regard, the utilization of IP-multicast supports efficient bandwidth utilization and minimizes packet replication. This results in a major benefit because a PMU does not have to replicate traffic or manage subscribers. Figure 1 depicts a generalized network architecture using IP-multicast technologies to send PMU data over a Wide Area Network (WAN). Main components are PMUs, routers (FHR, LHR) and subscribing entities that consume the PMU data. The proposed architecture in this document refers to IP Multicast PIM-SSM (Protocol Independent Multicast – Source Specific Multicast) in order to provide an optimal delivery path for low latency traffic. PMU messages are sent to the First-Hop-Router (FHR) on the local network to which the PMU is connected. In the terminology of IP-Multicast, the FHR is the first node in a multicast "tree". To become a receiver, a subscriber which intends to receive data from a specific PMU needs to signal that request at its local gateway - the Last-Hop-Router (LHR). This request will be implemented based on the Internet Gateway Management Protocol (IGMP). Multiple steps follow in order to build a Multicast Tree or to join an existing one. The term tree refers to the resulting structure between sender and receivers where paths are branching out to reach the member of a particular multicast group. At a router where such a tree branches off, replications of the multicast packets are sent out towards the subscriber. This is a major advantage of IP multicast because it does not implement multiple copies of the same data from a publisher (PMU). A PMU or IED is not burdened with replication and management of traffic or subscriber lists, which allows an efficient utilization of computation and communication resources. From the architectural perspective, the network replicates packets at optimal points – a huge leap towards scalability and efficient network utilization. From the gateway router (LHR), the synchrophasor data is forwarded onto the LAN, typically a substation bus, to which the receiving PMU's are attached.

Besides the data plane capabilities, management and control commands must be supported by PMU's or IED's encapsulating PMU functionality. An IP unicast-based control plane is the preferred solution to achieve effective separation for control, management and security.

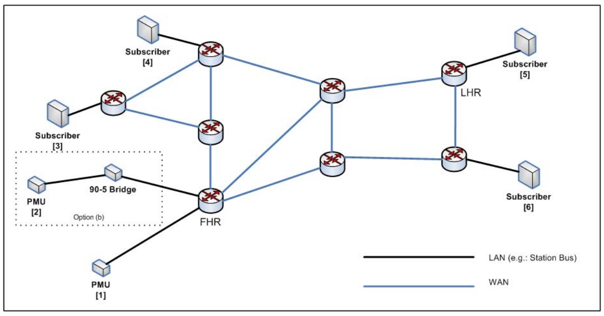

Figure 01

The handling of inter-domain traffic is an important requirement when multiple entities with their own network domains are sharing data from PMU's. Inter-domain multicast must be supported and enabled in the gateway routers (FHR, LHR) at the network edge. PIM-SSM provides the means to enable traffic to traverse domain boundaries.

A receiver of a synchrophasor data stream needs to know contextual information about the source, the sending PMU. A PMU registry is the functional entity to provide this type of information like the multicast source and the group address for IP multicast traffic as well as other metadata. In the scope of the NASPI initiative in North America, which is briefly discussed later in this document, the IEC Common Information Model (CIM) is used to integrate the phasor data information into the operational environment. This approach allows a direct integration with alarms, events and historical data for alarm handling and system analysis.

From the application perspective, the IP multicast architecture without PDC-stacking allows an allocation of functional blocks with PDC functionality directly to dedicated application server or data historians. In other words, functionality is assigned to proper places in the architecture. This leads to a much cleaner system architecture and provides an extension path for additional functionality.

Near and mid-term, PMU network installations need to provide capabilities to integrate PMU's which do not support IP multicast (a) or not even the IP protocol itself (b). The following options are already available to achieve this:

- In the case of (a): Modern routers implement Unicast-to-Multicast conversion capabilities. The FHR in figure 1 can receive multiple IP/UDP unicast connections and then convert these streams to IP multicast
- In the case of (b): An IEC TR 61850-90-5 bridge allows encapsulated GOOSE/SV data into IP multicast messages (see figure 1, PMU [2]). If the receiving end of the stream expects Layer 2 – GOOSE/SV data as well, a bridge with receiving functionality needs to restore GOOSE/SV messages onto the destination LAN.

The role of IEC TR 61850-90-5

Besides the pure network consideration, use cases, protocol and application specific definitions, and standards are necessary. The most important contribution in this regard is the Technical Report (TR) IEC 61850-90-5 with the title: *Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118.* Synchrophasor message formats and transmission over long distances are already defined in IEEE C37.118. Further development regarding harmonization with the concepts of IEC 61850 in terms of control (event driven capabilities) is the main achievement of IEC TR 61850-90-5. The TR defines a protocol for the exchange of synchrophasor data between PMUs, PDCs WAMPAC (Wide Area Monitoring, Protection, and Control), and between control center applications. Several major events and high-level requirements such as the blackout in the Northeastern part of the United States in 2003 as well as strict cyber security requirements triggered the preparation of the TR. The following use cases are described in the document in detail:

- Wide Area Applications Utilizing Synchrophasors
- Synchro-check
- Adaptive relaying
- Out-of-step (OOS) protection
- Situational awareness
- State Estimation and on-line security assessment
- Archive data (event & continuous)
- Wide Area Controls

The TR combines the capabilities of the comprehensive object model defined in the IEC 61850-series with a new mapping to IP-Multicast technologies. A security model specifies cryptographic functions and credential (key) management. Use cases already supported by the definition of GOOSE and SV are reused and refined. The object model enhancements in the TR allow synchrophasor data to be properly represented. The Logical Node (an IEC 61850 specific term) *MMXU* is used to represent the synchrophasor measurements that are generated as defined in IEEE C37.118.1. The IEC 61850 Calculation Method *ClcMth* is extended to include the Protection Class (P-Class) and Measurement Class (M-Class) information. Two new control blocks are defined to specify the sending of the following data:

- Information streams (e.g. Sampled Values)
- Event driven information (e.g. GOOSE)

Depending on the control block, a message is generated according to the standard IEC 61850-9-2 (Sample Values) and IEC 61850-8-1 (GOOSE).

The Substation Configuration Language (SCL), defined in IEC 61850-6, is extended to describe the IEC 61850 UDP/IP profile and the new synchrophasor functions. It also provides mechanisms needed to allow IEEE C37 migration and to express the configuration of PDC's. Furthermore, SCL extensions are defined to specify the security capabilities based on the options of the security model. Annex C of the TR provides a migration path for implementations based on IEEE C37.118 to the architecture specified in IEC TR 61850-90-5.

In terms of communication, IEC TR 61850-90-5 specifies the usage of the Internet Group Management Protocol, Version 3 (IGMPv3; RFC 3376) to enable multicast path determination. Message transmission is defined based on Multicast UDP/IP. In the terminology of TR, it is called R-SV (Routable Sample Values) and addresses the requirement for high throughput rates with the boundary condition that those applications tolerate infrequent losses of single samples. The use of TCP/IP is not ruled out but only recommended if a loss of sample data can't be tolerated. In this case, IEC TR 61850-90-5 recommends the TCP based reporting mechanism of IEC 61850-7-2 and IEC 61850-8-1 which defines point–to-point associations between client and server.

Furthermore, transport profiles for IPv4 and IPv6 exist. A SCL extension for IPv6 is foreseen. Annex E provides the IPv6 specific definitions and lists the normative references (IPv6 related RFC's). Currently, the SCL definitions in IEC 61850-6 do not support the notions of an IPv6 address. This needs to be updated in IEC 61850 in general to meet the requirements of new domains with a high number of end devices where the limitations of IPv4 would be counterproductive.

Finally, it is important to mention that IEC 61850-90-5 provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets in general. This enables new options to overcome the limitations of "native" GOOSE/SV traffic, encapsulated directly into Ethernet frames, between substations and control centers and especially in many new use cases in Distribution Automation (DA) and Distributed Energy

Resources (DER). In order to foster a fast adoption of this promising standard, SISCO and Cisco Systems have initiated an open source project regarding IEC 61850-90-5[4].

Security considerations

Security is a critical success criterion for applications and systems that use synchrophasor information for control and protection. Manipulated synchrophasor data could cause tremendous damage to the electric power system. Sound architectural definitions must consider security an important requirement from the very beginning. The security for the proposed architecture is built on two pillars:

- Scalable network security based on GetVPN
- Protocol security as specified in the security model defined in IEC TR 61850-90-5

Cisco's GetVPN is a technology, which is developed on open industry standards for both, Control and Data planes. Group Domain of Interpretation (GDOI) is used to distribute crypto state to group members and to keep them synchronized. In a typical architecture as depicted in figure 01, GetVPN encrypts the synchrophasor-data streams between the edge routers (FHR, LHR). The tunnel-less VPN technology of GetVPN provides advanced features and a scalable security model:

- Any-to-any instant connectivity to high-scale
- No overlays – native routing
- Advanced QoS
- Efficient Multicast replication

The security model specified in section 8 of IEC TR 61850-90-5 defines information authentication and integrity as mandatory and confidentiality as optional. It also considers the security definitions in IEC 62351-6:2007 to address end-to-end security. The security standard IEC 62351-6 (Security for IEC 61850) specifies the security for IEC 61850 GOOSE and SV messages. The security model is very flexible in order to meet typical requirements in the context of definitions like Physical Security Perimeters (PSP) and Electronic Security Perimeters (ESP). Furthermore, the Technical Report IEC 61850-90-5 defines group-key management based on GDOI (RFC 3547). The concept of "perfect-forward" security is built on key rotation and the usage of one or more Key Distribution Center (KDC), in a centralized or decentralized manner. The availability of the KDC is an important factor and must be thoroughly considered regarding deployment and redundancy. The SCL of IEC 61850 is extended to allow access point definition of where the KDC function is located. The TR slightly amends GDOI in order to address use cases where more than one subscribing entity may reside on a single IP-address. More specifically in the terminology of IEC 61850, it allows DataSet specific keys. The key management concept used in IEC TR 61850-90-5 is a candidate to get reused within the security standard series of IEC 62351.

In order to achieve a scalable and performant security architecture, a combination of GetVPN and the security model defined in IEC 61850-90-5 provides several options to achieve security-in-depth. It also addresses the implementation status of IEC 61850-90-5 and IEC 62351-6 and helps to protect IED's and PMU's with limited or no security capabilities. Figure 02 depicts such a combination where GetVPN is used to provide encryption for data packets travelling between the FHR and LHR and the IEC TR 61850-90-5 data model to protect the data going onto the LAN. In order to build a multi-layer defense, more technical security controls like PMU specific firewalls, Multicast Access Control Lists (ACL), PMU-based intrusion protection and strict port security should be applied. Finally, the capabilities of the IP network provide the necessary measures for segmentation and path isolation to protect PMU traffic and to separate it from other data.

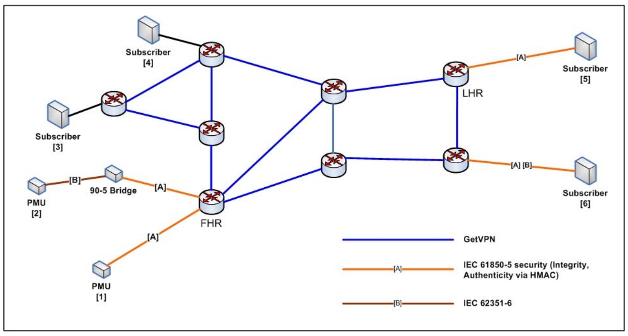

Figure 02

Conclusion and Outlook

The proposed network architecture allows a maximum of visibility into the power grid and scales perfectly with a growing number of subscribers within a single or between multiple network domains. It makes maximum use of necessary elements (standard network gear), exploits the network to a maximum, since it must be there anyway, and provides a flexible security architecture. The consequent use of standard network devices reduces the cost for communication equipment. The architecture avoids PDC-stacking and operation in a cascaded fashion. The network handles the aggregation with very low latency. A proof of concept and life demonstration is developed in the scope of the NASPI initiative. NASPI is a collaborative project between the U.S. Department of Energy (DOE), the North American Reliability Corporation (NERC) as well as North American utilities, vendors, academics and consultants. The objective of this effort is to create a robust, secure, distributed, widely available, scalable and standardized data communications infrastructure to support synchrophasor applications in North America.

But this is just the beginning. With the automation of the Distribution Grids and the integration of DER, new applications are needed in these domains to manage instability from adding variable energy resources to the power grid. IP-multicast network architecture as described in this paper provides a scalable platform for new applications and services. On top of the network infrastructure, the new routable profile for IEC 61850 GOOSE/SV messages addresses the requirements and specifics of the domains perfectly. It can be expected that this profile as specified in IEC TR 61850-90-5 will lead to a new IEC 61850 mapping defined in a standard document. The availability of a complete solution stack will enable new applications. Typical examples are:

- Distribution grid state determination
- Power flow monitoring
- Fault detection, classification and location
- Asset utilization monitoring
- Microgrid protection schemes

In the future, more systems and applications will consume and process synchrophasor data. The subsequent bullets list some:

- Distributed Management Systems (DMS)
- Regulation and stabilization controllers
- Microgrid controls and DER controllers
- Fault isolation system controllers

A robust network and system architecture based on IP-Multicast for large PMU networks will support the efforts to prevent large-scale blackouts by giving system operators, personnel or automated systems more time to respond to disruptive events and much more visibility into the electrical power grid.

One important paradigm applied in the proposed architecture is the principle of exploiting existing infrastructure (the IP network) to meet the requirements and to implement the functionality in an extensible and scalable way. The understanding of a PMU as a multicast "source" is the bottom line. The network infrastructure can already fulfil important requirements because it scales more efficiently and provides robustness and flexibility. Critical devices like PMU's or IED's are not burdened with management, complex communication and security tasks. Large deployments with similar requirements are already in place in other industries. The same approach can be used for further main use cases in the power industry. Security is a perfect example in this respect. Existing network security appliances and technologies are often already in place to deliver all services needed to ensure that critical installation and components can fulfill their core functions regarding protection and control.

References

[1] ISO-IEC 61850-90-5 - Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

[2] ISO-IEC 62351, Data and communication security – Part 6: Security for IEC 61850

[3] Myrda, Taft, Donner, Recommended Approach to a NASPInet Architecture, 2012 45th Hawaii International Conference on System Sciences, 2012

[4] Cisco- SISCO announcement: Cisco and SISCO Collaborate on Open Source Synchrophasor Framework
Available:
http://www.cisco.com/web/strategy/docs/energy/cisco-SISCO_factsheet.pdf

[5] Whitepaper: Cisco Whitepaper, PMU Networking with IP Multicast, Cisco Systems 2012
Available:
http://www.cisco.com/en/US/prod/collateral/routers/ps10967/ps10977/whitepaper_c11-697665.pdf

Biography

Maik G. Seewald was born in Dresden, on May 1, 1964. He graduated from Gymnasium in Dresden, and studied at the University of Applied Science in Dresden. His employment experience includes Advanced Micro Devices (AMD), Sunnyvale and Dresden, AUDI, Ingolstadt, Siemens, Munich and Nuremberg, and Cisco Systems, San Jose and Hallbergmoos. He is an active member of several IEC TC 57 working groups with the focus on IEC 61850 and IEC 62351, of IEEE P1901.2 working group (Low-Frequency Narrow-Band Power Line Communications) as well as of various security groups and initiatives. His special fields of interest comprise cyber security, system and software architecture as well as smart grid architecture. He is an expert in energy automation and grid communication and control. In this regard, Maik's focus is on the change from rather isolated systems into large inter-connected networks based on distributed intelligence.