February 20, 2019

DETERMINISTIC PROCESS NETWORKS BASED ON ADAPTIVE TRAFFIC POLICING AND FILTERING

Maik Seewald

Robert Barton

DETERMINISTIC PROCESS NETWORKS BASED ON ADAPTIVE TRAFFIC POLICING AND FILTERING

AUTHORS:
Maik Seewald
Robert Barton

ABSTRACT

Techniques are described herein to facilitate deterministic networking based on Time-Sensitive Networking (TSN) for Substation Automation Networks (SANs). The use of adaptive configuration of filtering and policing for TSN-streams allows the implementation and operation of a secure converged process bus architecture and supports the approach of a fully digital substation.

DETAILED DESCRIPTION

Within the electrical power grid, electrical substations are an essential component. Electrical substations typically contain primary (transformer, electrical switching gear) and secondary equipment (automation, control, and communication gear). Automation and control networks interconnect these devices and system and enable critical functions. Reliability and availability are key concerns that can impact the safety and overall functionality of the automation system. TSN can provide hard isolation and network slicing for control networks. This is especially important for the process bus, connecting substation devices to the field equipment. Current process bus deployments do not allow a multi-service architecture. Instead, because of security and reliability concerns, they simply transport the measurement data (sampled values).

The Institute of Electrical and Electronics Engineers (IEEE) 802.1 TSN standards are new to power automation. They exist as a network technology only with no integration and orchestration with the upper-layer protocols (e.g., International Electrotechnical Commission (IEC) 61850) and applications. The techniques described herein close this gap. They specify a method to configure and orchestrate an adaptive policing and filtering mechanism to protect critical process traffic and to allow best-effort communication over the same physical network.

Substation Automation Networks (SANs) based on IEC 61850, the leading standard in this domain, consist of two Ethernet-based segments: the station bus and the process bus. The process bus is the time and mission critical part connecting the Intelligent Electronic Device (IED) (controller/protection relays) and Merging Units (MUs). In operation, the IEDs receive a stream of data (so-called 61850 sampled values) from the MUs. Based on the sampled values, processes and controls are triggered by the IEDs to protect and automate the electrical substation.

Requirements regarding throughput, performance, and reliability are high and critical. In today's installation, this is typically achieved by over-provisioning and isolation (no other traffic is allowed on the process bus - sampled values traffic only). In some cases, utilities (the operators of these electrical substations) do not implement the process bus and instead use direct cabling. This is because of concerns that network failure or congestions could hinder or disrupt the delivery of sampled values. It comprises a substation network (Local Area Network) which is partitioned into a station bus and a process bus.

Provided herein is a mechanism to apply TSN technologies to an IEC 68150-based process bus and to enable stream-based policing and filtering in the switches. The technology and sub-standard IEEE 802.1Qci defines policing and filtering on ingress ports to protect time-sensitive flows. As described herein, IEEE 802.1Qci policies are applied to protect the process bus in a domain-specific manner, rendering the switches and the TSN network application-aware.

This may involve several measures, components, and procedures. First, the process bus is built on deterministic Ethernet using TSN technologies (as defined in IEEE 802.1 TSN). Second, end devices (end-stations in the nomenclature of TSN) such as MUs and IEDs are TSN-enabled. Third, sampled values are sent from the MUs to the IEDs encapsulated in TSN streams. Fourth, in the network switches, policing and filtering functions are applied. Fifth, the stream configuration is based on the IEC 61850 definitions. These are well-defined in syntax and stored in Substation Configuration Language (SCL) files.

In operation, the method to enable application-aware filtering may proceed as follows. First, the engineering of the Substation Automation System (SAS) contains process steps that comprise the configuration of the process of sending and receiving sampled values over the process bus (MUs = Sender; IEDs = Receiver) and the network components (switches). The engineering may be established by the connection between the IEC 61850-Engineering tool (which embeds the CUC) and the network configuration controller.

Second, in operation, the MUs continuously send measurement data (sampled values) to the receiving IEDs on the process bus. The MU data transmission is configured according to IEEE 802.1 TSN as streams using specific header information (e.g., VLAN, Multicast MAC Address, etc.). The configuration is based on the process of substation engineering. In existing installations using standard Ethernet (best effort), sampled values are sent using multicast addresses which requires complex filtering on the switches.

Third, the network switches in the process bus are pre-configured according to the step in the process of substation engineering. They are aware of sending entities (end-stations), amount of traffic, and timing (scheduling) aspects. In operation, the switches are fully application aware. Being application aware and having detailed information on the traffic allows the application of granular security policies.

Fourth, based on the pre-configured awareness, the switches implement IEEE 802.1Qci (per-stream filtering and policing). Using the provided information, the switches may identify any defective or intrusive talker (e.g., MU, IED, switch in the process bus, etc.). The applied ingress policing uses filters that can block or limit excessive amounts of sampling data. There are configurable options such as per stream filtering. In essence, this application-aware policing and filtering mechanism ensures that any faulty device, defective or intrusive, does not impact the pre-configured critical sampled-value-traffic/stream.

Fifth, filtering, frame-counting, and policing may be defined in IEEE 802.1Qci (per-stream filtering and policing). Using the engineering data to configure the filtering and policing enables granular detection of faulty, defective or hostile devices. Engineering and configuration of a TSN-enabled process bus allows the operation of a converged multi-service network. In other words, it is possible and secure to place other traffic (e.g., best effort, Internet of Things (IoT), etc.) on the process bus without any impact on the critical sampled value transmission.

Sixth, the entire configuration process and setup is agile and highly configurable and adaptive. Any change in the measurement configuration of the MUs and in the resulting transmission is performed and captured in the engineering tool, and triggers a change in the configuration of the end devices and the network components.

Figure 1 depicts an example overall architecture of a deterministic process bus. Switches and IEDs are TSN-enabled. The CUC is part of the IEC 61850-Engineering tool. The network controller updates the TSN-configurations each time a change in the SAS occurs. Stream filtering ensures critical sampled value transmission.

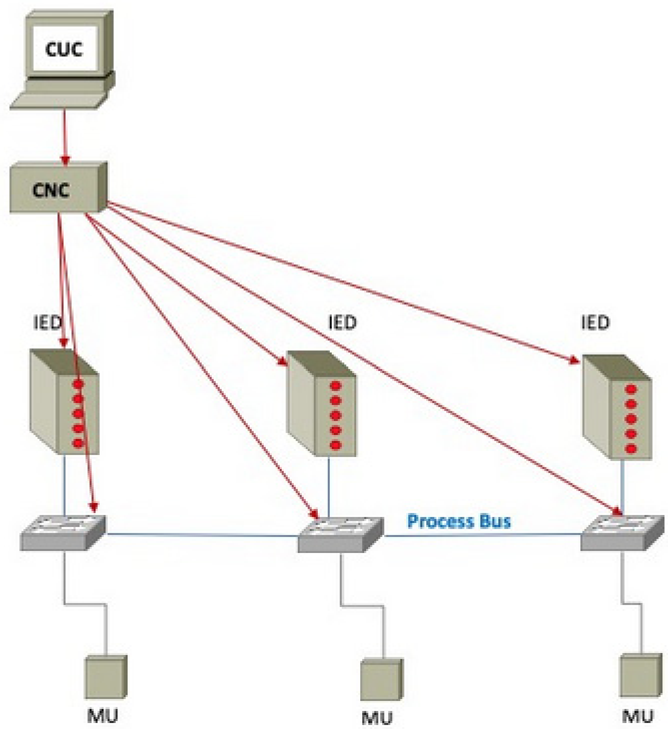

Figure 1

Figure 2 below depicts the adaptive and application driven filtering and policing for one gate within a switch.

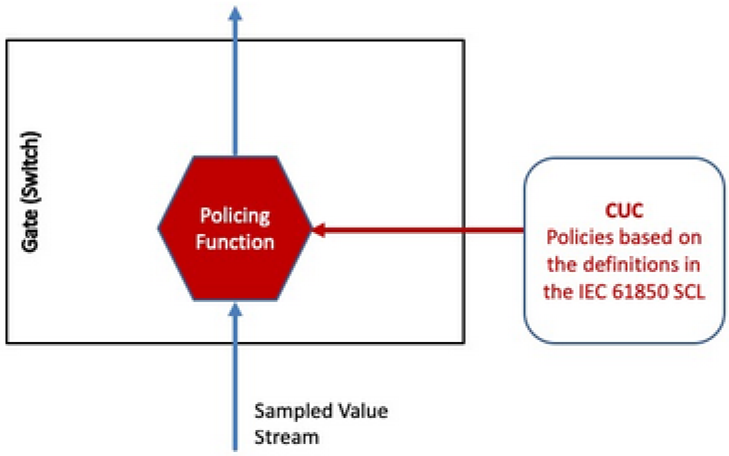

Figure 2

The techniques described herein provide protection from misconfiguration in end devices (IEDs, MUs) and switches, security incidents/attacks (e.g., Denial of Service (DoS), Distributed DoS (DDoS), etc.), babbling MUs, and/or network congestion. They also enable a converged process bus to share the network with other traffic (e.g., IoT traffic, video, voice, etc.).

In general, the use of deterministic networking technologies to protect critical automation and control traffic and to ensure high availability and reliability can help increase the adoption of the process bus in networks based on IEC 61850. This may help overcome concerns regarding use of Ethernet for underlying critical processes. Indeed, this is exactly the concern (and requirement) raised by the IEC 61850 user group (utilities) regarding the use of process bus technologies in substation automation.

In summary, techniques are described herein to facilitate deterministic networking based on TSN for SANs. The use of adaptive configuration of filtering and policing for TSN-streams allows the implementation and operation of a secure converged process bus architecture and supports the approach of a fully digital substation.