Application Note

Substation Event Reporting

OT Event Collection for Substations

Synopsis: The Radiflow 3180 secure gateway enables the collection of events from multiple types of devices at remote sites, converting them to Syslog format and sending them in a reliable manner to a central SIEM. This type of architecture increases the efficiency of the central SIEM in OT networks.

Energy companies have recently become a prime target for cyber-attacks by a variety of hostile organizations and governments. In order to assure the safety and reliability of their operation, new cyber-security measures need to be implemented.

Utility companies use Security Information and Event Management **(SIEM**) tools to protect their IT networks. The SIEM receives events from devices across the network using the Syslog standard, then analyzes and displays them for the purpose detecting violations.

Following the success of SIEM tools in protecting IT networks, utilities are considering the expansion of their scope to also protecting their operational technology (OT) assets. However, SIEM tools are not suitable for protecting OT networks, since not all OT devices are able to send Syslog events. Such devices include:

- IP devices that send events in another format rather than Syslog (e.g. HTTP, SNMP)
- IP devices that generate an internal events table that needs to be polled
- Serial devices that are unable to send events over IP

Another problem is reliability: Syslog messaging uses UDP, which does not provide verification upon message reception. Thus, in case the link from the remote site to the SIEM becomes unstable, some events may be lost, causing inconsistencies in the SIEM presentation.

To meet both challenges, the Radiflow 3180 is deployed as an event collector at remote sites, which allows it to receive events directly from the local OT devices. The 3180 receives events in multiple formats (Syslog, SNMP, HTTP) and even polls event tables from IP and Serial devices. The 3180 converts all the events received to Syslog format, appends them with supporting fields (e.g. location, source sub-system, severity) and forwards the events to the central SIEM. The additional information simplifies the processing of the events in the SIEM tool, resulting in higher scalability.

Furthermore, the 3180 can implement several resiliency functions on the link to the central SIEM:

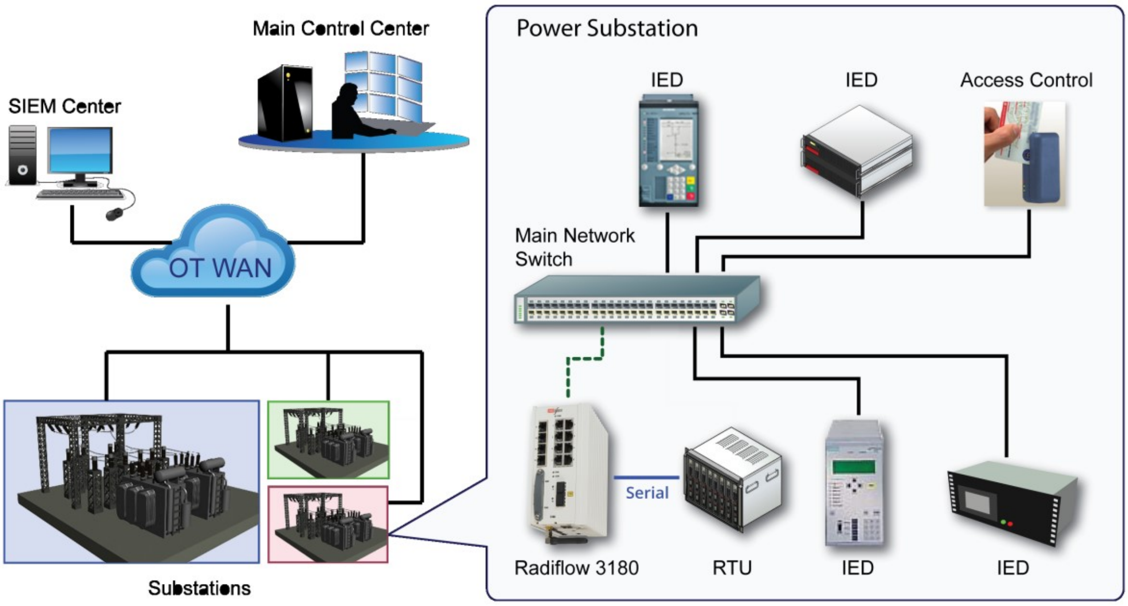
- Use of Syslog over TCP with re-transmits, instead of UDP
- Redundant links (e.g. cellular as a backup to the main landline link)
- Duplication of data, allowing the use of multiple SIEM tools
- Local event storage for audits
- Encrypted tunnel to the SIEM

radiflow
Secure your Assets

Application Note

Substation Event Reporting

OT Event Collection for Substations



Radiflow 3180 Unique Benefits for the Event reporting process

- *Conversion of a wide range of event protocols to Syslog events*
- *Polling of event tables from IP and Serial devices, and converting them to Syslog events*
- *Addition of custom data fields to raw data, including location, severity and more*
- *Use of network resiliency functions on the SIEM link for increased reliability*
- *Ruggedized platform compliant to IEC 61850-3/IEEE 1613 for HV/MV substations*

Radiflow 3180 complete tool set

- Up to 16x10/100 and 2x100/1000 Ethernet ports with L2/L3 networking features
- Up to 8xRS-232 ports for interfacing with legacy devices
- 2G/3G/LTE Cellular modem with dual SIM cards for operator redundancy
- User Authentication (APA) for restricting access to end-devices
- Per-port DPI SCADA firewall (DNP3, ModBus, IEC 104/101/61850)
- VPN tunnels using IPSec and X.509 certificates

radiflow
Secure your Assets