Application Note

Low-Impact Substation Security

Securing Small Substations using a Central IDS

Synopsis: Radiflow's iSID is an Industrial Intrusion Detection System (IDS) that delivers a comprehensive cyber-security solution for distributed SCADA networks, while overcoming the innate challenge of network overloading.

Supervisory Control and Data Acquisition **(SCADA)** systems are used for controlling operations in utilities such as electric power, water and oil. In power utilities, SCADA systems control the remote distribution sites, which contain PLCs, RTUs, IEDs and other devices.

Over the last decade, remote substations have become a prime target for cyber-attacks, which has led to the requirement for utilities to install security measures on their SCADA networks. However, many utilities refrain from implementing such measures, fearing that they would disrupt operating processes or overwhelm their networks.

Radiflow's iSID is a non-intrusive Industrial Intrusion Detection System **(IDS)** designed to protect critical infrastructures against cyber-attacks, by detecting abnormal behavior, such as topology changes and variations in the operational processes sequence.

This is achieved through real-time analysis of all network traffic, which is validated against a normal (baseline) network behavior model automatically created by the IDS using passive network monitoring. Once the operator approves the normal behavior model, the iSID is able to detect anomalies in the operational network's behavior, and alert the operator. Such anomalies may indicate an insider attack (e.g. a malware on one of the PLCs) that couldn't have been detected by the secure gateway at the entry to the site.

Typically, IDSs are implemented as local systems. However, while this type of deployment is suitable for large sites, it is not scalable over a distributed network of multiple small sites. To this end, Radiflow's Smart Probe enables implementing the iSID at a central location, for analyzing feeds (received over the WAN) from multiple small remote sites. The Smart Probe optimizes the data-stream sent from each site to the central iSID, overcoming the challenge of collecting and sending data to the IDS without overloading the network.

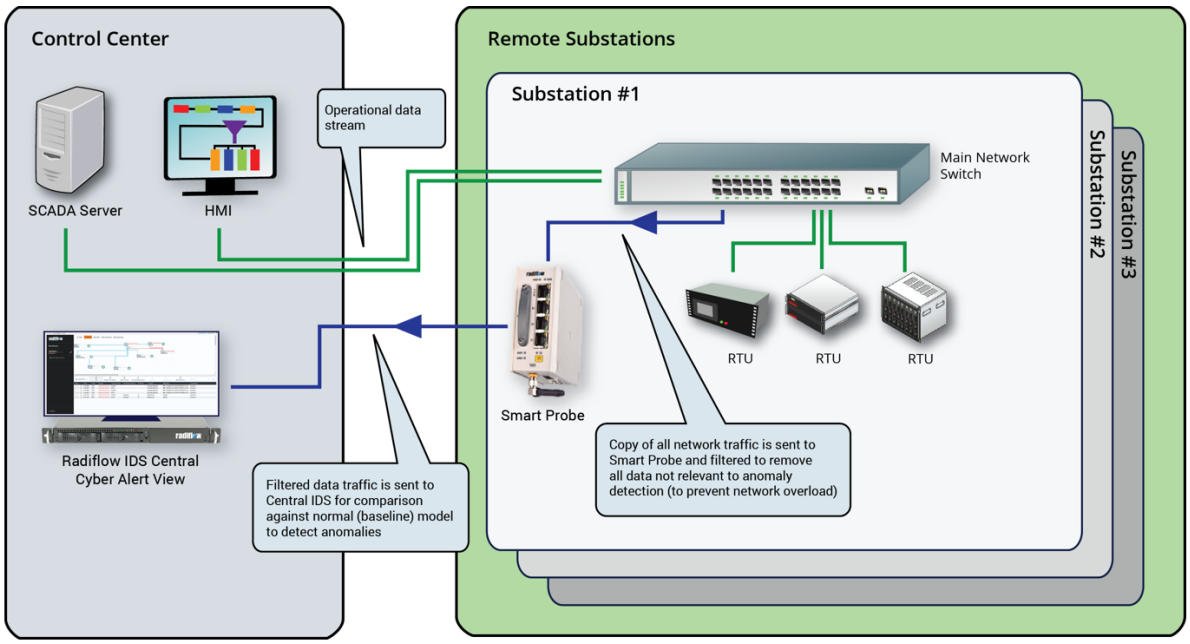
To optimize the data-stream, Radiflow's Smart Probe includes a traffic filtering mechanism: it receives a copy of all network traffic, filters it to remove all data that is irrelevant to the network behavior analysis, compresses the filtered data, and sends it over to the Central IDS over a secure tunnel that can be unidirectional or encrypted.

Beside filtering and compressing data, the smart Probe also enables the analysis of Serial traffic by collecting it from remote sites and converting it to Ethernet format. This gives the iSID full coverage of all devices, including serial devices that would have been otherwise ignored, at each and every site.

Application Note

Low-Impact Substation Security

Securing Small Substations using a Central IDS



Key Features

iSID

- Network visibility: Display of all network assets and any changes in connectivity, based on self-learning of the SCADA network through passive scanning of all data transactions.
- Maintenance management: Monitoring and logging of activities performed during maintenance sessions according to pre-configured policies.
- Anomaly detection: Detection of abnormal activity such as changes in the SCADA process sequence, abnormal memory access and firmware changes, based on the normal application behavior model created by the IDS.
- Policy Monitor: creation of virtual firewall rules on each link, based on Deep Packet Inspection (DPI) for SCADA protocols.

RF 2120

- Filtering out of irrelevant data and compressing the data prior to sending it to the control center.
- Support for Ethernet and Serial interfaces, for connecting modern and legacy devices.
- Unidirectional or encrypted tunnel for secure connectivity.
- Ruggedized Smart Probe hardware is compliant to IEC 61850-3/IEEE 1613 requirements for operation in harsh environments such as HV/MV substations.

radiflow
Secure your Assets