Nebras

CyberSecurityExpert

OT Cybersecurity

Fundamentals

Nebras
CyberSecurityExpert

Introduction to OT

Introduction to OT Cybersecurity - Part 3

Contents

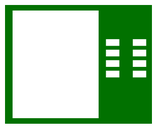
SCADA

MTU

RTU

PLC

PAC



IED

Nebras
CyberSecurityExpert

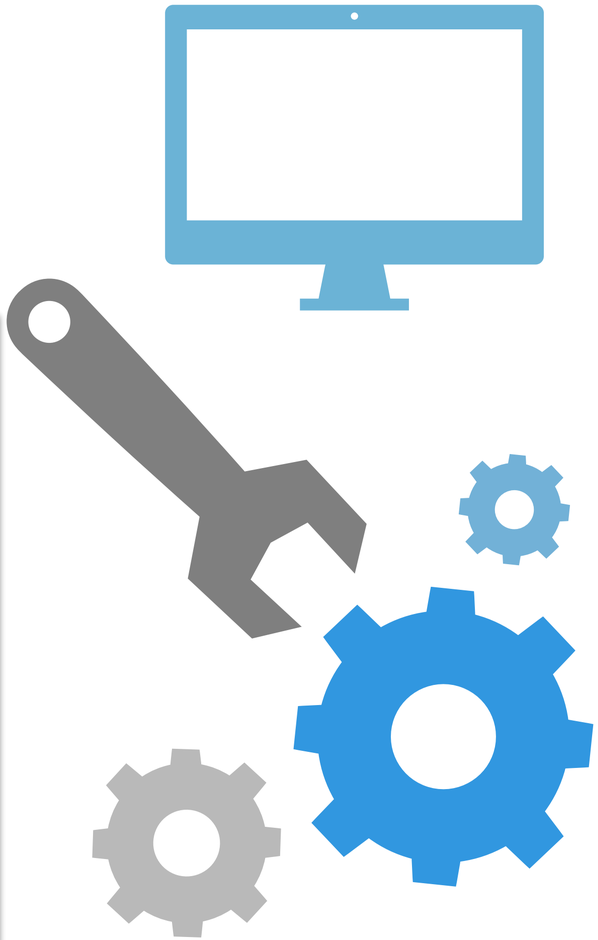
SCADA

Supervisory Control And Data Acquisition

In DCS it’s focused on specific process, provided by same vendor, preloaded with required functions for that particular process, within a local plant.

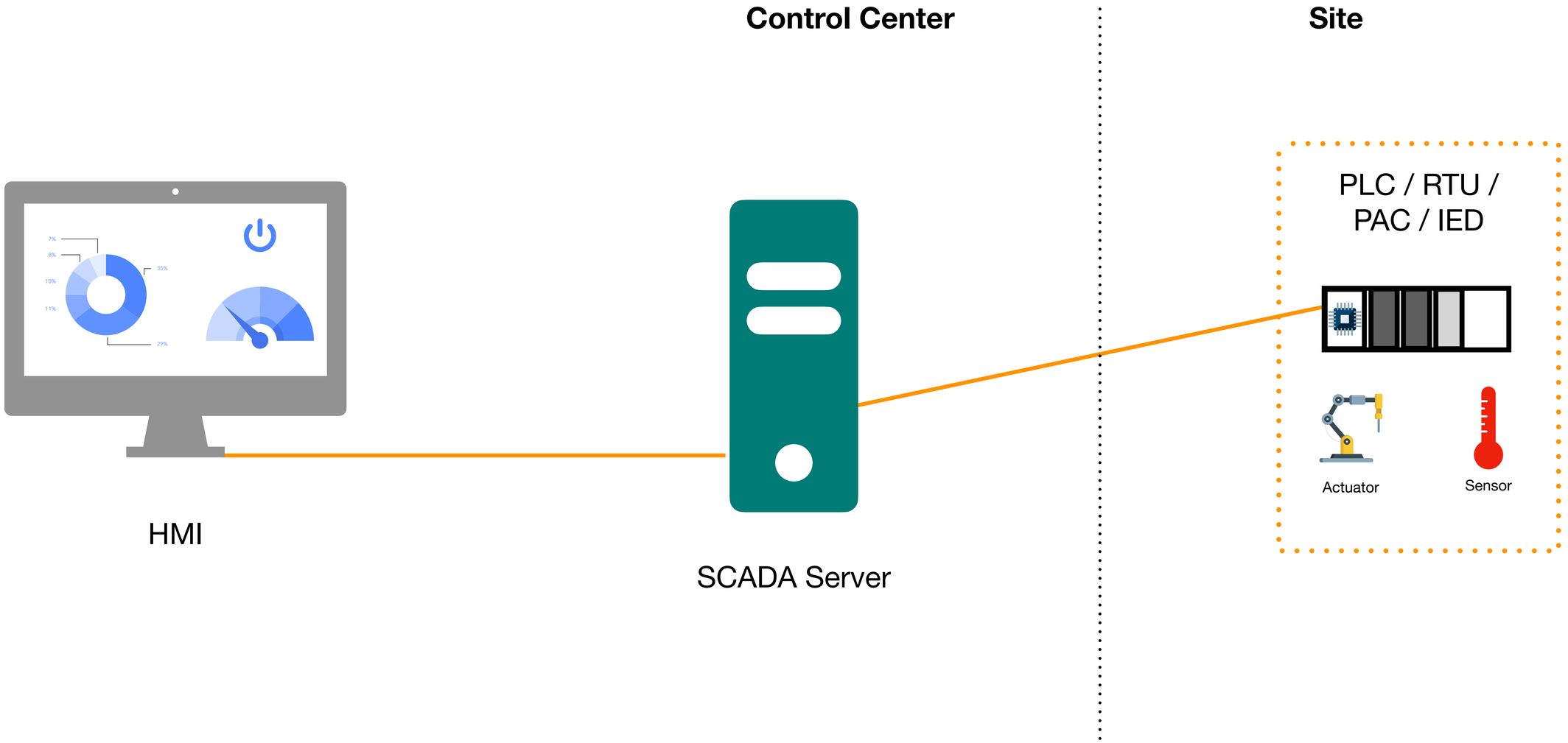
In SCADA, it’s another system that performs monitoring and control but with some differences:

1. SCADA comes empty, and the engineer needs to program everything.
2. It’s often used in large geographic locations, and remote locations.
3. It works on slower connectivity.
4. Where DCS is Process driven, SCADA is Event driven.
5. SCADA is focused on the acquisition of continuous telemetry information. (To spot an error and know how long it has been there).
6. SCADA provides sending Control commands to remote operations to correct the errors.
7. SCADA often referred by the remote HMI



Nebras
CyberSecurityExpert

SCADA



Nebras
CyberSecurityExpert

SCADA

SCADA Server

Master Terminal Unit (MTU)

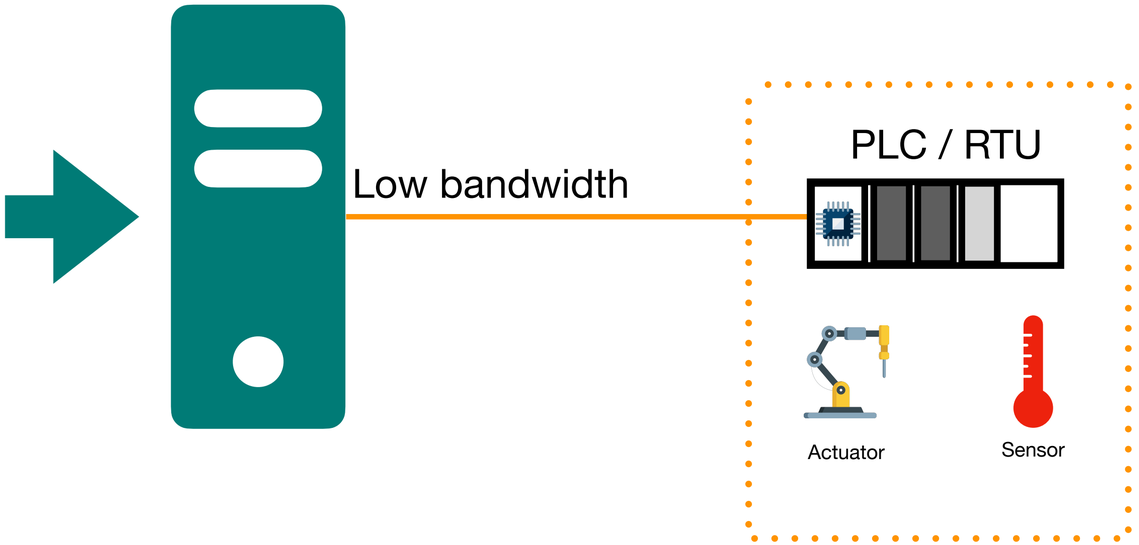
Located at the master Control Center

Collect information from RTUs/PLCs/PACs/IEDs

Send Commands to RTUs/PLCs/PACs/IEDs

Master / Slave communications (ex: OPC Server)

Communicate with Field devices over low bandwidth



Nebras
CyberSecurityExpert

SCADA

Programmable Logical Controller (PLC)

SCADA is commonly referred by the combination of PLC/HMI

PLC is a rugged Computer with I/O for Field devices

PLC has memory to store the programs

Programmed by same languages of DCS Controllers. (FBD, LLD, ST, ..etc)

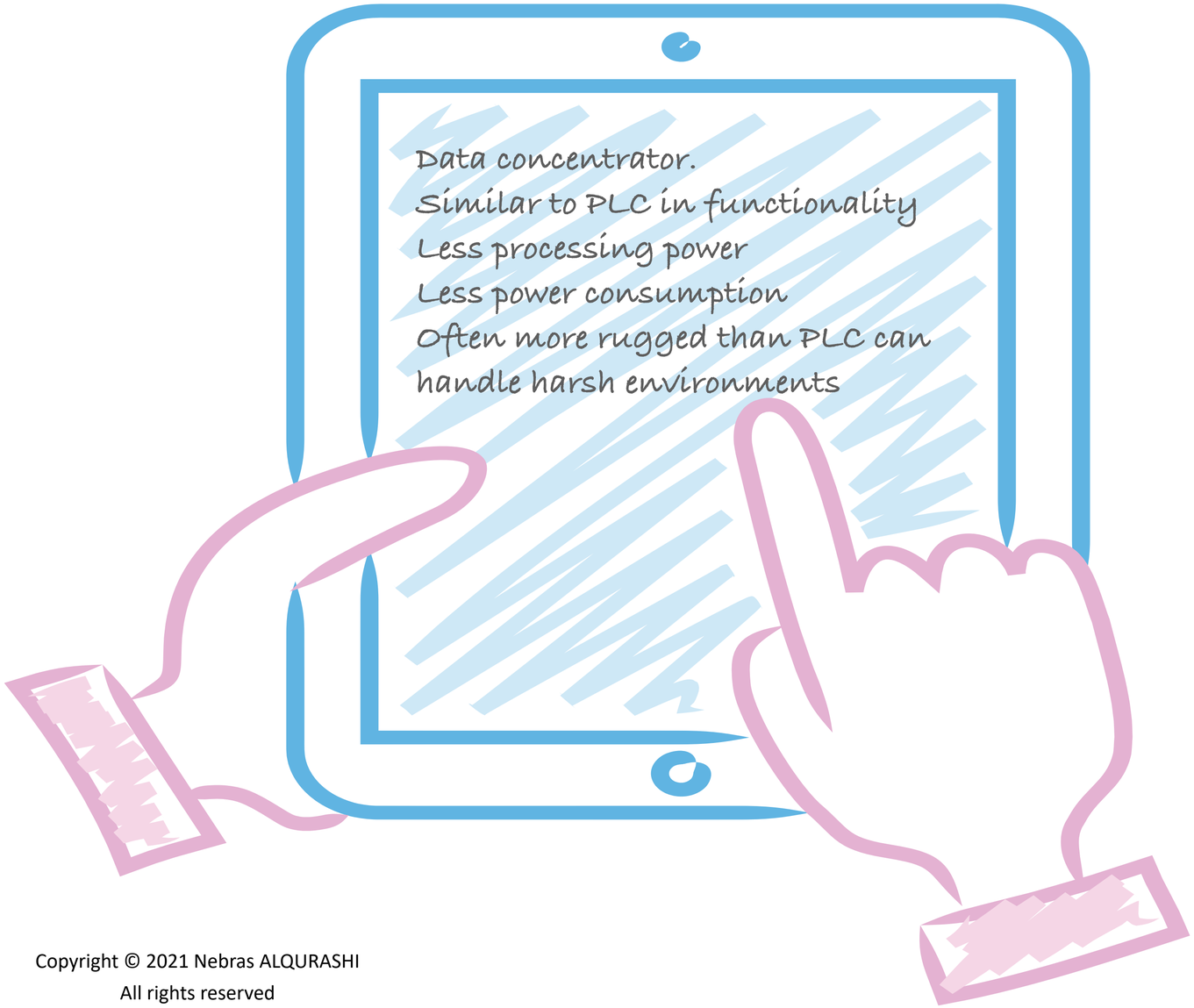
Communicate with SCADA Server (MTU) over different media, usually low bandwidth, and in the mean of Industrial protocols (Modbus, OPC, S7, ..etc)

* Also used in DCS

Nebras
CyberSecurityExpert

SCADA

Remote Terminal Unit (RTU)



Nebras
CyberSecurityExpert

SCADA

Programmable Automation Controller (PAC)

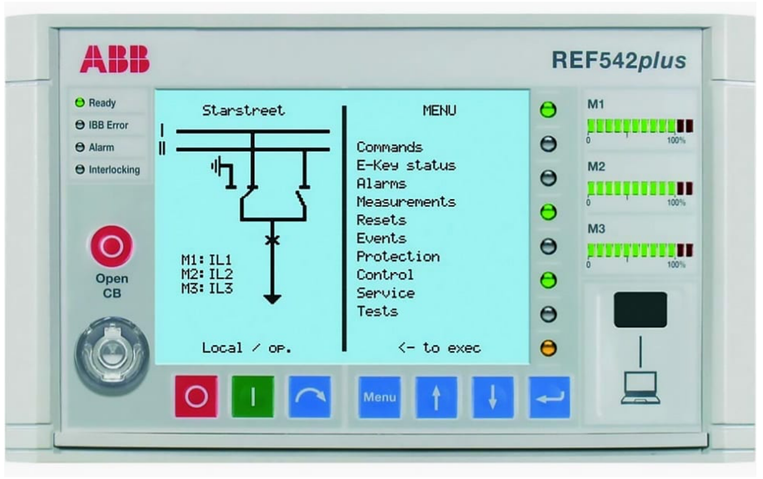
- Is similar to PLC
- Higher processing power
- Additional capabilities
- Integrate with organizational Database

Nebras
CyberSecurityExpert

SCADA

Intelligent Electronic Device (IED)

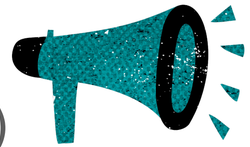
Provides direct connections to Field devices.
Connects directly to MTU or through RTU



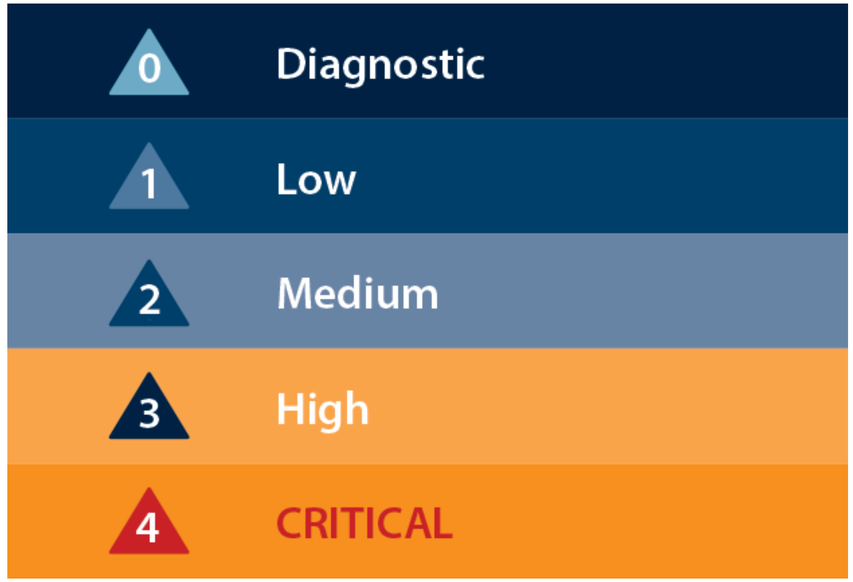
Nebras
CyberSecurityExpert

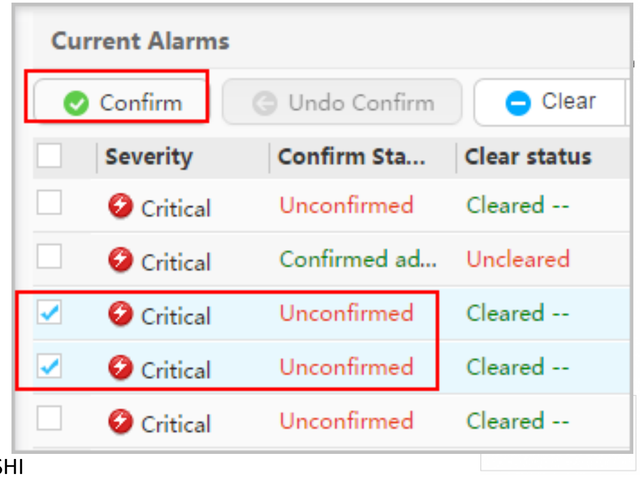
SCADA

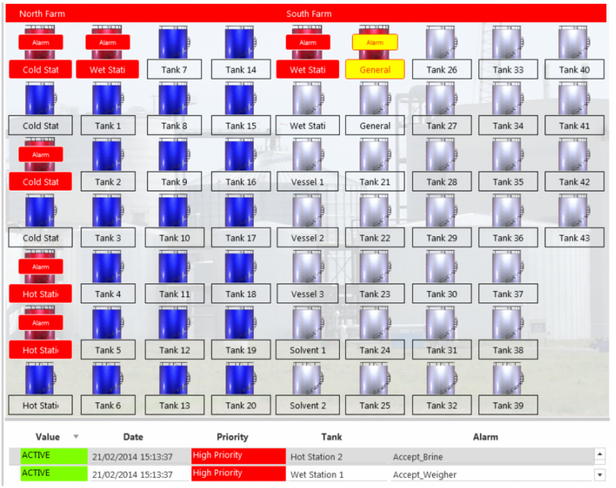
Alarms (Critical aspect of SCADA)



Alarms usually for actionable conditions. (Events don't always require attention).
Vendors / System Integrators usually work on defining important Alarms for the system.
Alarms are handled by concerned departments
Alarms can be fine tuned to avoid duplicates of known issues.
Often Alarms are ignored during maintenance
Programmed Actions can be: Email / SMS / Activation of procedure / trigger other alarms.



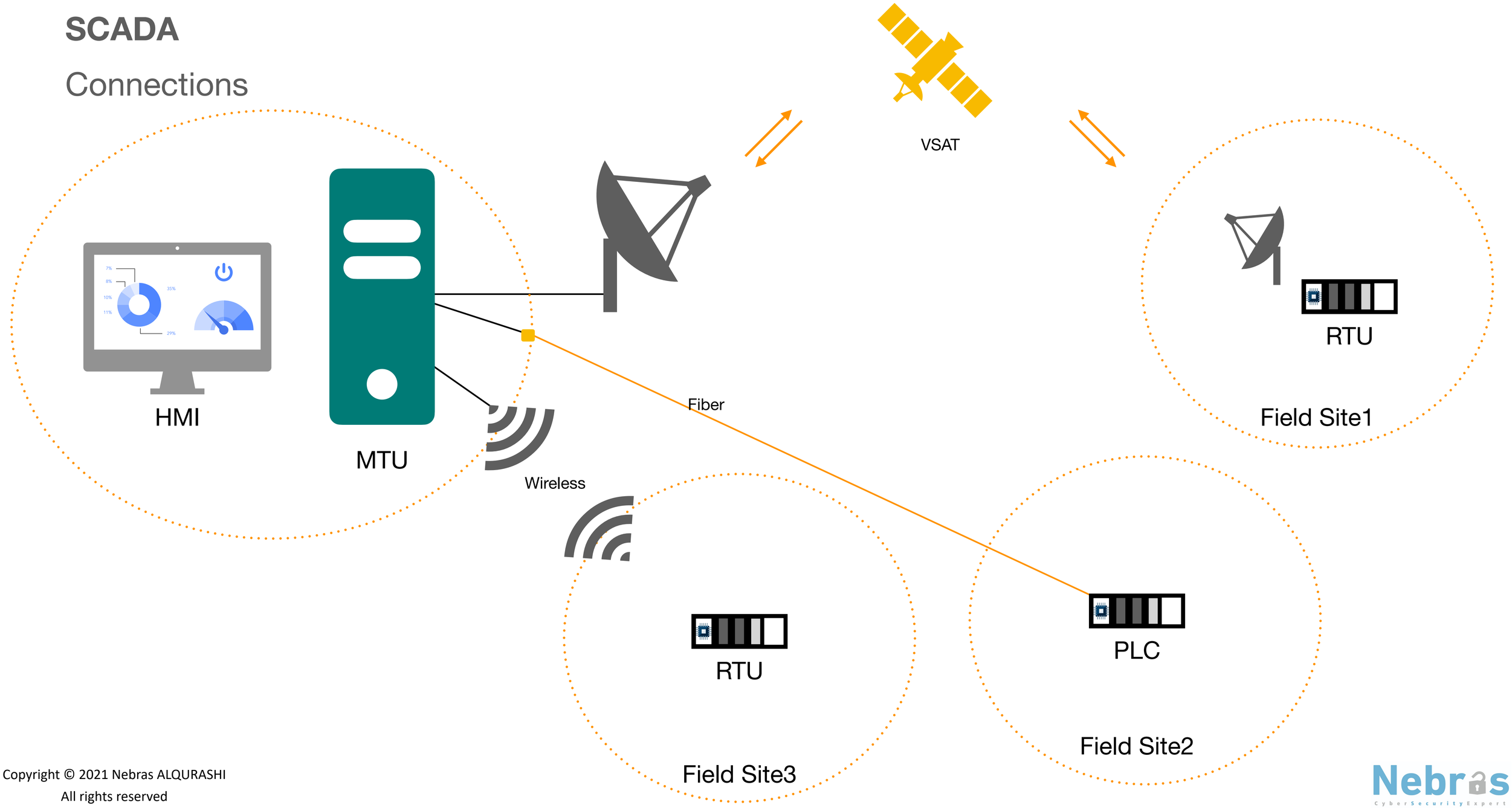




Nebras
CyberSecurityExpert

SCADA

Connections



Nebras
CyberSecurityExpert

Quick Summary

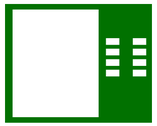
SCADA

MTU

RTU

PLC

PAC



IED

Nebras
CyberSecurityExpert