Vulnerability Analysis of 2013 SCADA issues

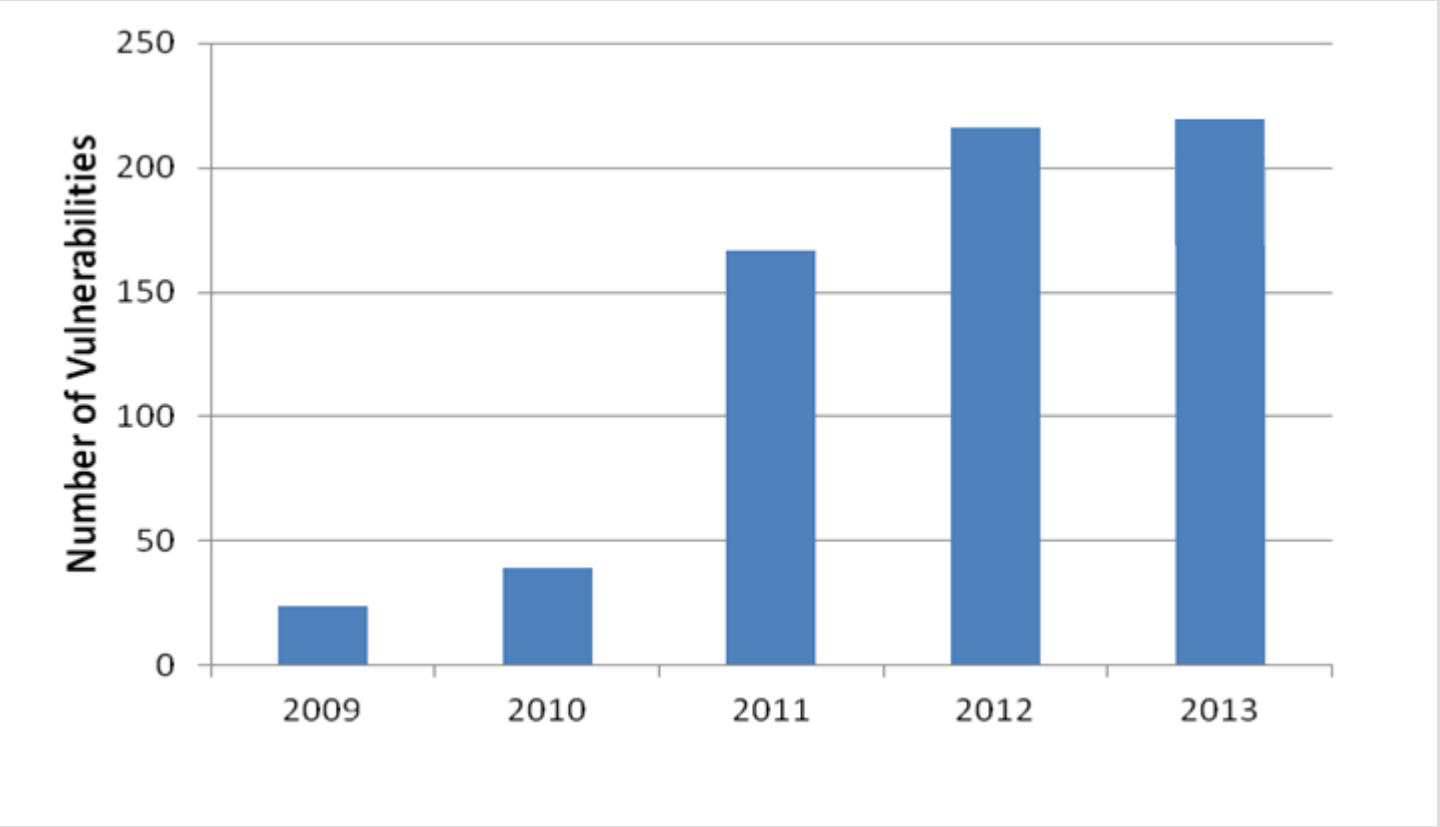
Amol Sarwate

Director of Vulnerability Labs, Qualys Inc.

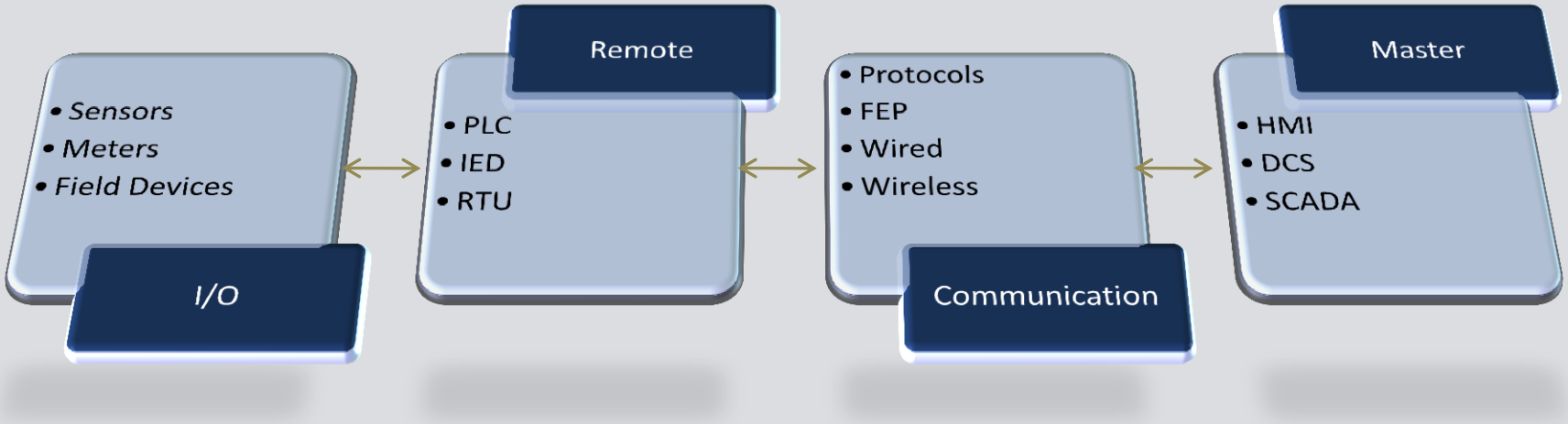
Agenda

SCADA components
2013 Vulnerability Analysis
Recommendations and Proposals

2009 - 2013 SCADA Vulnerabilities

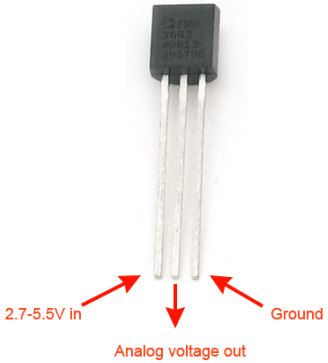


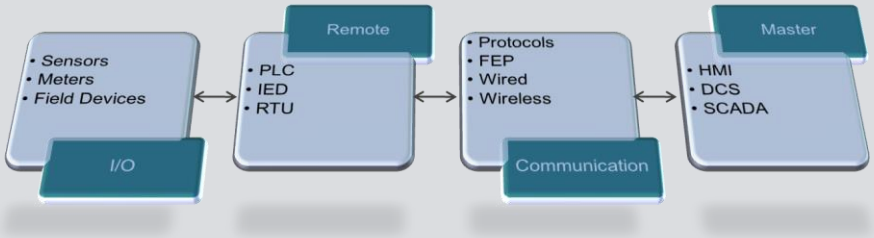
Components


• Sensors
• Meters
• Field Devices
I/O
Remote
• PLC
• IED
• RTU
• Protocols
• FEP
• Wired
• Wireless
Communication
Master
• HMI
• DCS
• SCADA
Field
Control Center

Acquisition

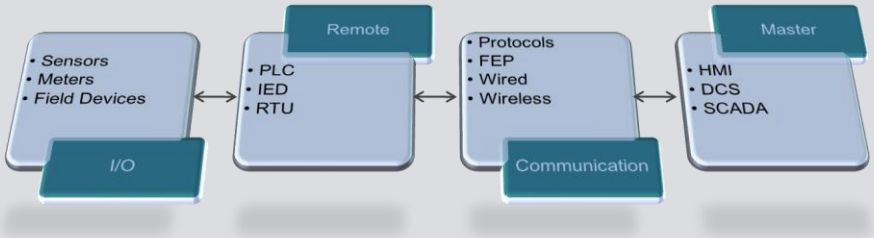
Convert parameters like light, temperature, pressure or flow to analog signals





Conversion

Converts analog and discrete measurements to digital information

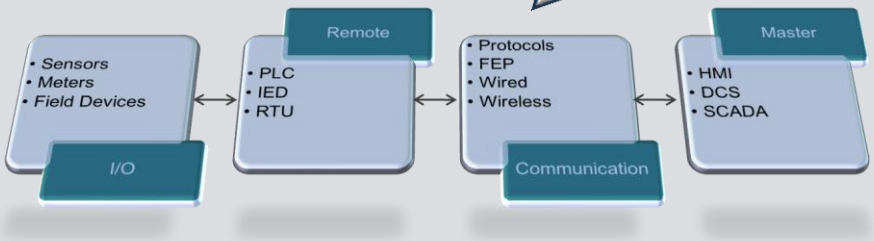


Communication

Front end processors (FEP) and protocols
Wired or wireless communication

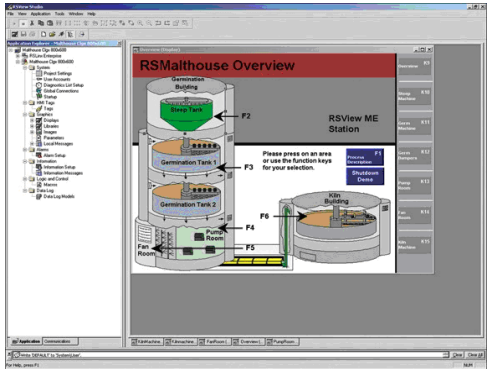


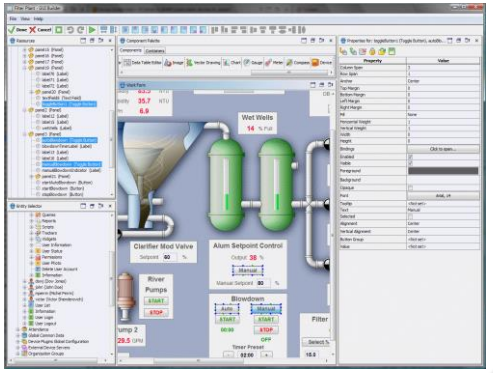
Modbus	DNP 3	OPC
ICCP	ControlNet	BBC 7200
ANSI X3.28	DCP 1	Gedac 7020
DeviceNet	DH+	ProfiBus
Tejas	TRE	UCA

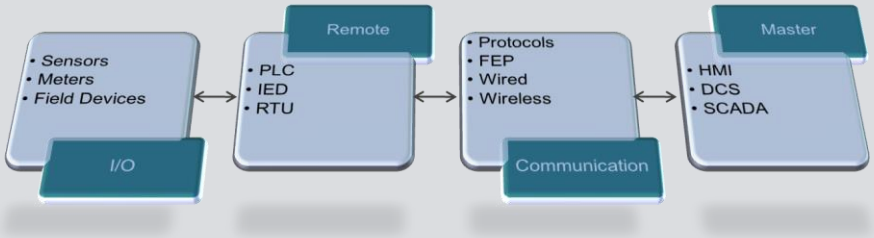


Presentation & Control

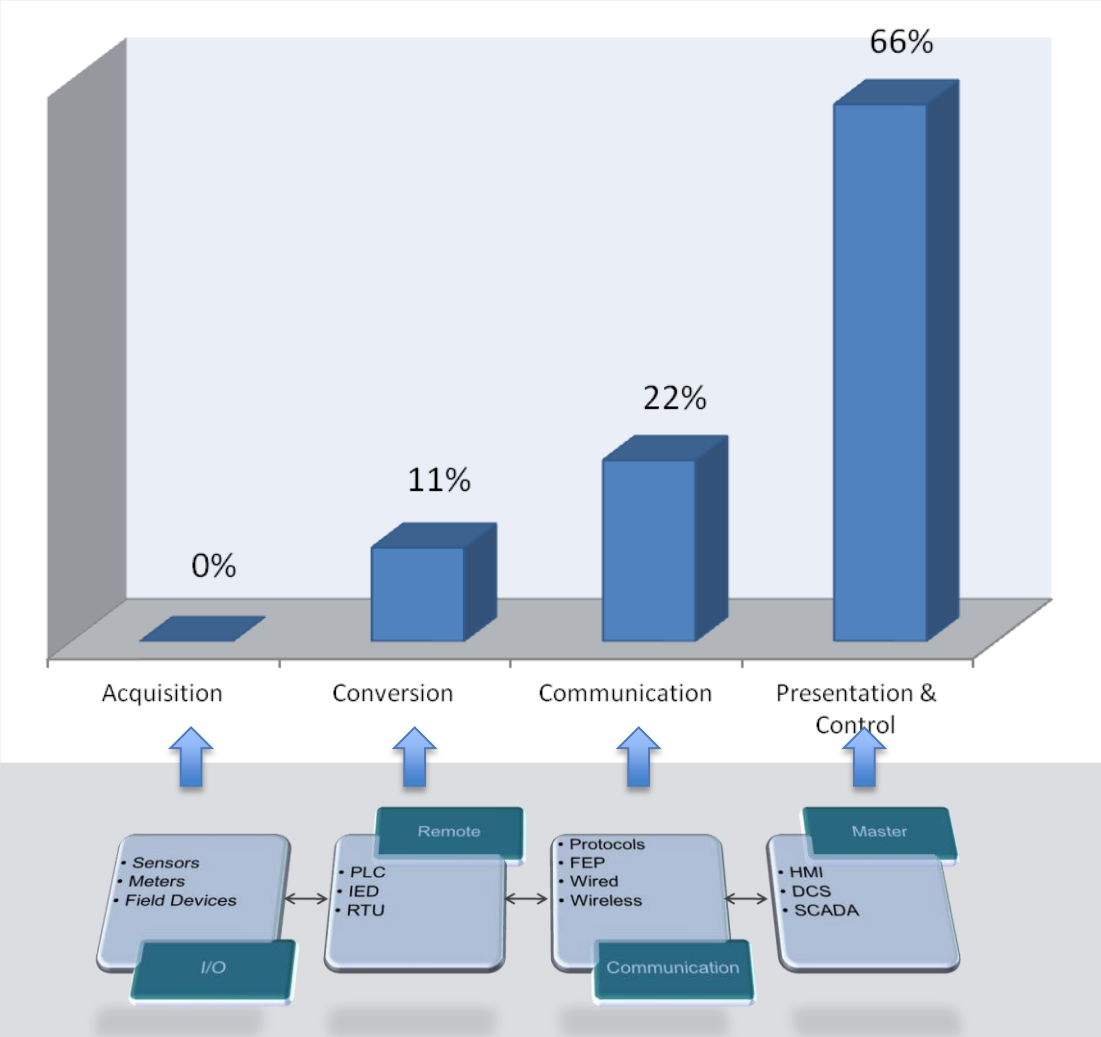
Control, monitor and alarming using human machine interface (HMI)





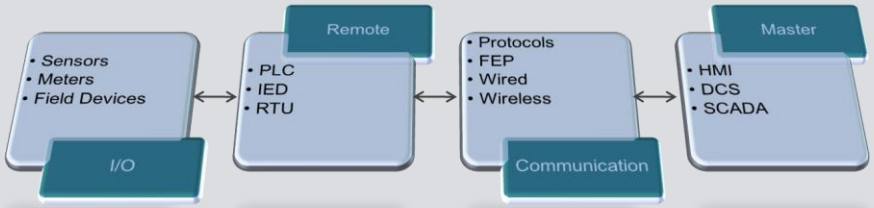


2013 Vulnerabilities by category



Acquisition

- Requires physical access
- Field equipment does not contain process information
- Information like valve 16 or breaker 9B
- Without process knowledge leads to nuisance disruption

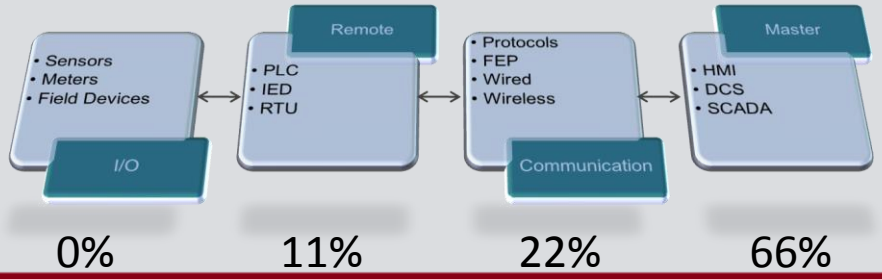


0% 11% 22% 66%

Emerson ROC800 Vulnerabilities

- CVE-2013-0693: Network beacon broadcasts allows detection
- CVE-2013-0692: OSE Debug port service
- CVE-2013-0694: Hardcode accounts with passwords
- Access: AV:N, AC:L, Au:N
- Impact: C:C, I:C, A:C

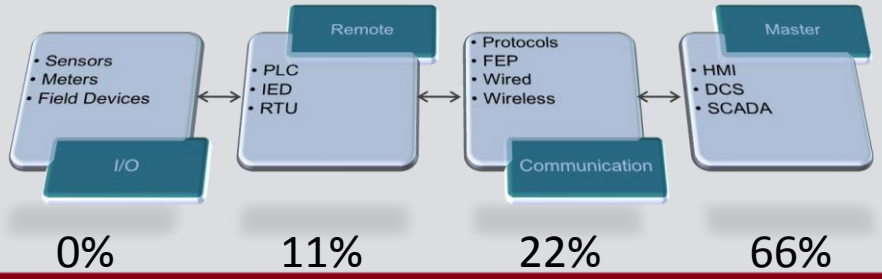
- **Patch available from Emerson**



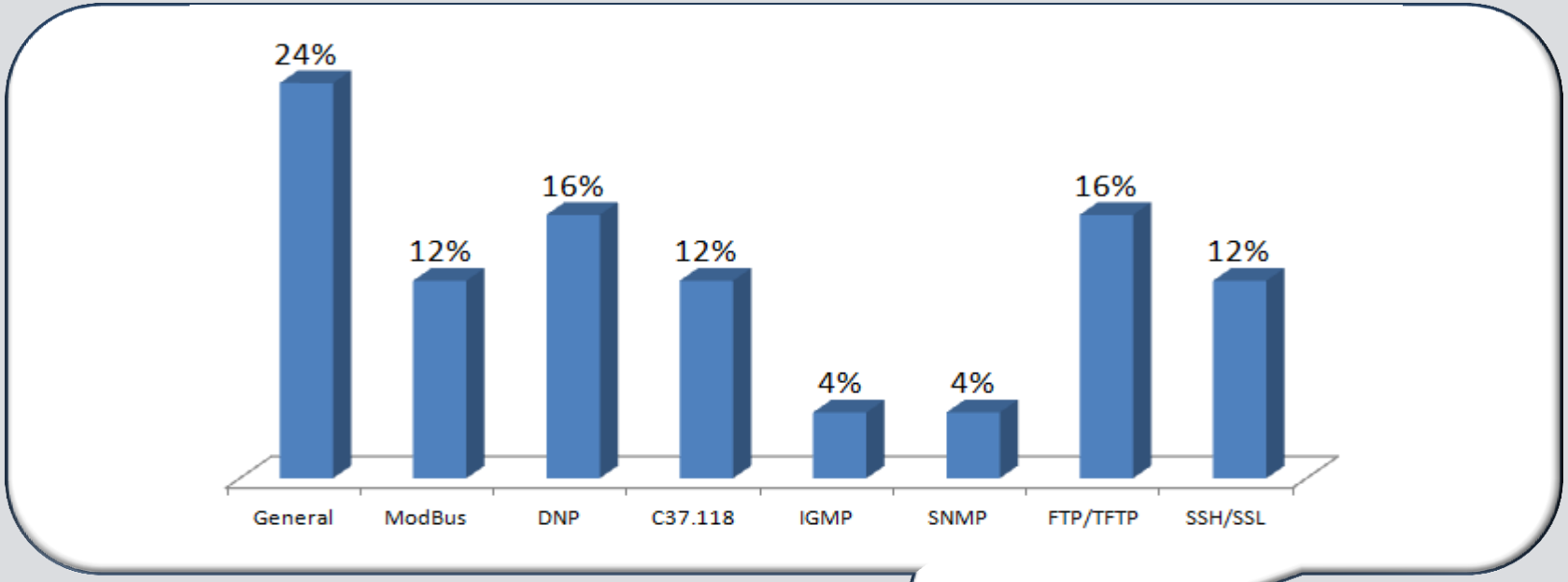
Siemens CP 1604 / 1616 Interface Card Vulnerability

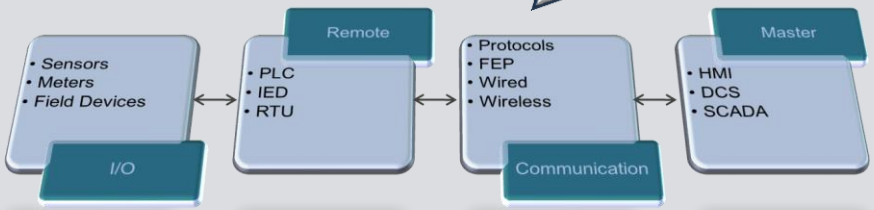
- Siemens security advisory: SSA-628113
- CVE- 2013-0659: Open Debugging Port in CP 1604/1616
- UDP port 17185
- Access: AV:N, AC:L, Au:N
- Impact: C:C, I:C, A:C

- **Patch available from Siemens**



Communication





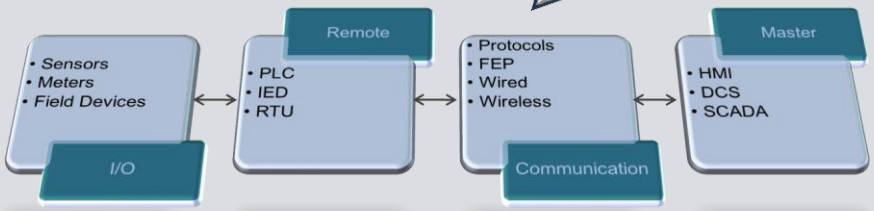
0% 11% 22% 66%

ModBus Vulnerabilities

- CVE-2013-2784: Triangle Research Nano-10 PLC Crafted Packet Handling Remote DoS
- CVE-2013-0699: Galil RIO-47100 PLC Crafted Modbus Packet Handling Remote DoS
- RBS-2013-003: Schneider Electric Multiple Modbus MBAP DoS and RCE

Nano-10 PLC

RIO-47100 PLC

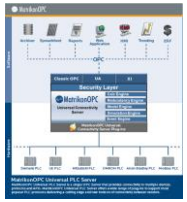


0% 11% 22% 66%

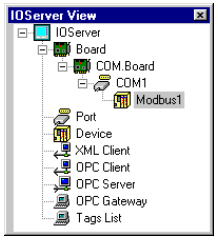
DNP Vulnerabilities

- CVE-2013-2791: MatrikonOPC Server DNP3 Packet Handling buffer overflow
- CVE-2013-2798: Schweitzer Real-Time Automation Controllers (RTAC) Local DoS
- CVE-2013-2788: SUBNET SubSTATION Server DNP3 Outstation Slave Remote DoS
- CVE-2013-2783: IOServer DNP3 Packet Handling Infinite Loop

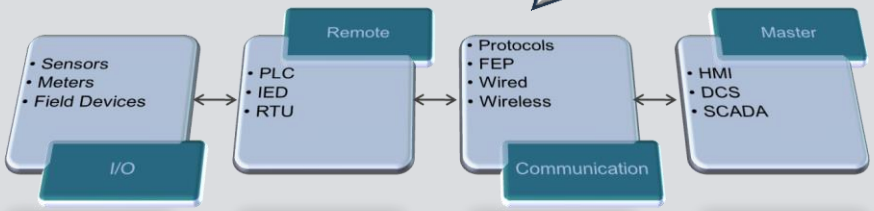
Schweitzer RTAC



Matrikon OPC Server



IOServer

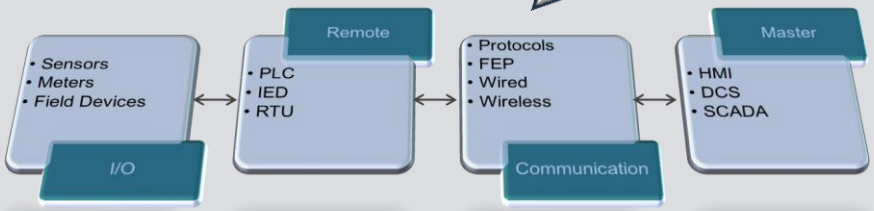


0% 11% 22% 66%

Security Analysis of SCADA protocols

Modbus and DNP free tool:
http://code.google.com/p/scadascan/

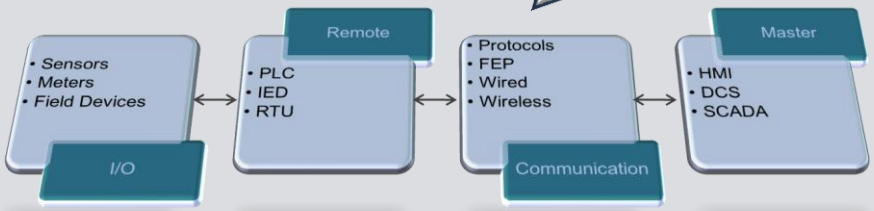
```
C:\SCADA>perl scadascan.pl

Usage: scada_scan.pl [-m|-d] (-r|-t) target_IP
Options:
        -m : Modbus bruteforce slave ID
        -r : Rate at which Modbus packets are sent.
             1 = fastest, 5 = slowest. Possible values 1 to 5
        -d : Scan for DNP 3.0 TCP
        -t : Read timeout in seconds.
```



0% 11% 22% 66%

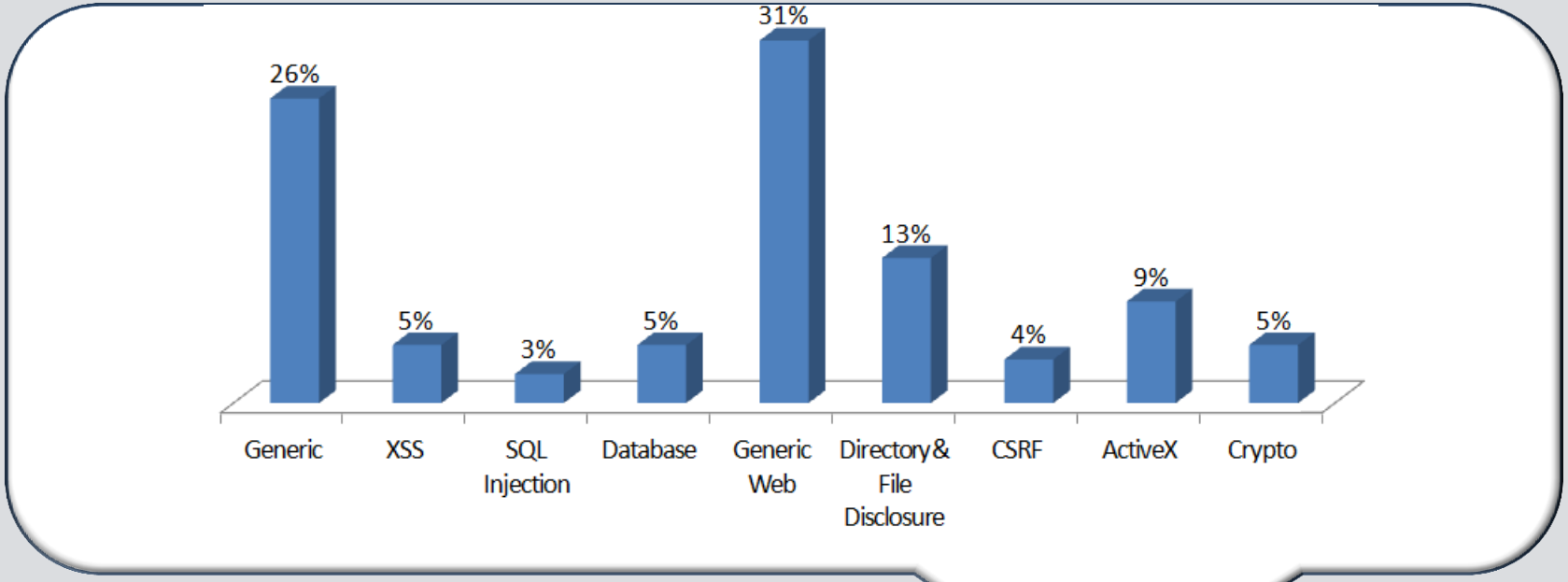
SSH, FTP, TFTP, IGMP, SNMP

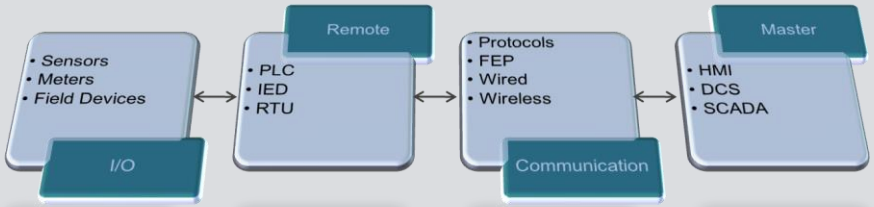
- CVE-2013-0137: Monroe Electronics Default root ***SSH*** Key Remote Access
- CVE-2012-4697: TURCK BL20 / BL67 ***FTP*** Service Hardcoded Admin Credentials
- CVE-2013-2800: OSIsoft PI Interface for ***IEEE C37.118*** Memory Corruption
- CVE-2013-0689: Emerson RTU ***TFTP*** Server File Upload Arbitrary Code Execution
- CVE-2013-3634: Siemens Scalance X200 IRT ***SNMP*** Command Execution
- Korenix Multiple JetNet Switches ***TFTP*** Server Arbitrary File Creation
- RuggedCom ROX-II ***IGMP*** Packet Saturation RSTP BPDU Prioritization Weakness
- Korenix Multiple JetNet Switches SSL / SSH Hardcoded ***Private Keys***



0% 11% 22% 66%

Presentation & Control

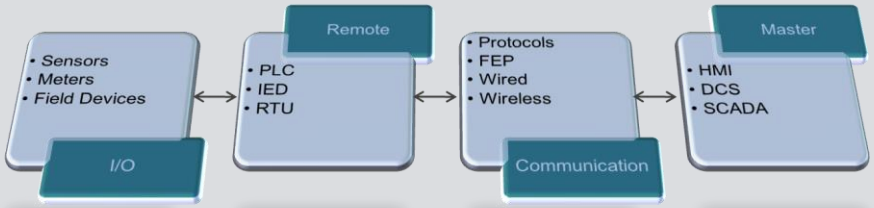




0% 11% 22% 66%

Presentation & Control

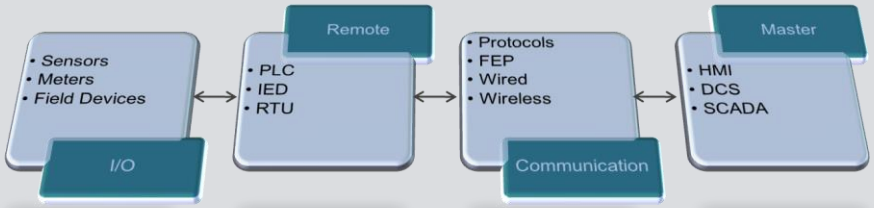
- CVE-2013-2299: Advantech WebAccess /broadWeb/include/gAddNew.asp **XSS**
- CVE-2013-0684: Invensys Wonderware Information Server (WIS) **SQL Injection**
- CVE-2013-3927: Siemens COMOS Client Library Local **Database *Object Manipulation***
- CVE-2013-0680: Cogent DataHub Crafted **HTTP** Request Header Parameter Stack Overflow
- CVE-2013-0652: General Electric (GE) Intelligent Proficy **Java** Remote Method Invocation
- CVE-2008-0760: SafeNet Sentinel Protection Server HTTP Request ***Directory Traversal*** and ***Arbitrary File Access***
- CVE-2012-3039: Moxa OnCell Gateway ***Predictable SSH / SSL*** Connection Key Generation
- Weidmüller WaveLine Router Web Interface config.cgi Configuration Manipulation ***CSRF***



0% 11% 22% 66%

Real world issues

Control system network connected to corporate network or internet

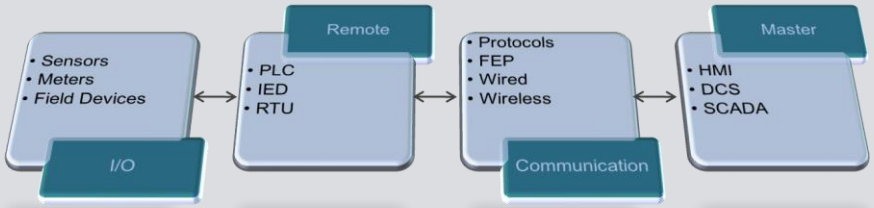


0% 11% 22% 66%

Real world issues

No authentication

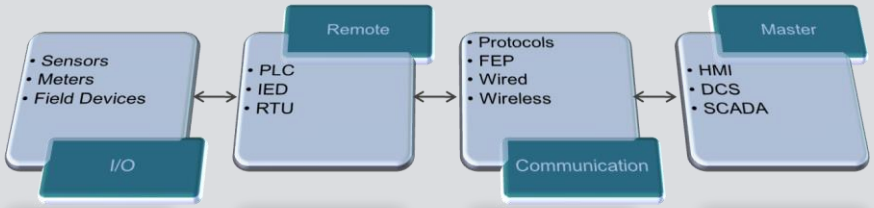
No per user authentication



0% 11% 22% 66%

Real world issues

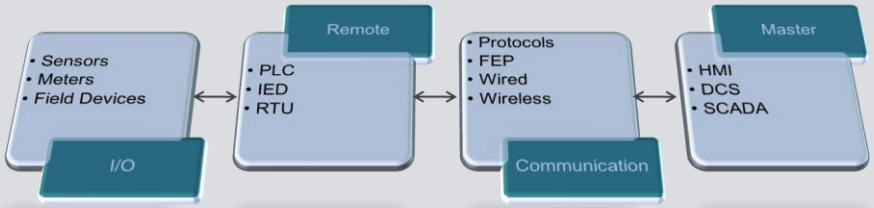
Delayed patching if any



0% 11% 22% 66%

Real world issues

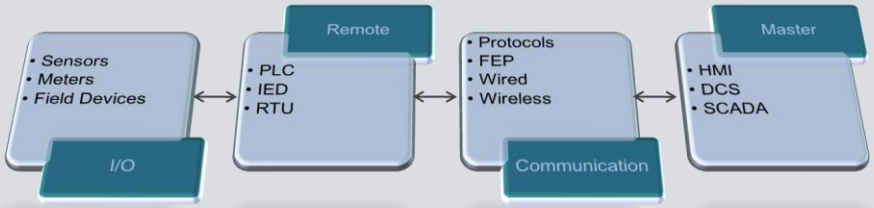
Default passwords
Shared passwords
No password change policy



0% 11% 22% 66%

Real world issues

Systems not restarted in years

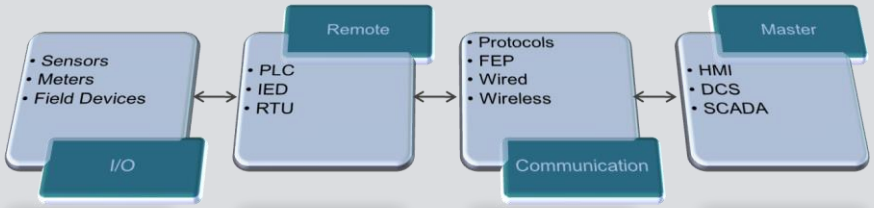


0% 11% 22% 66%

Real world issues

Off-the-shelf software

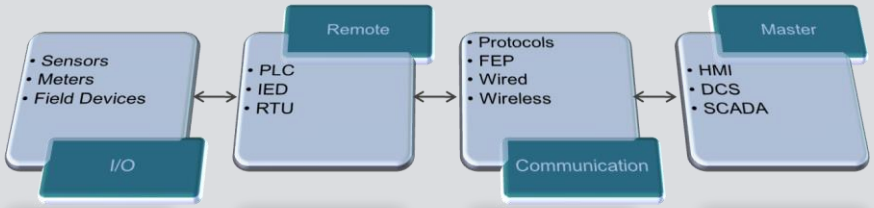
Operating system, Database, Browser, Web Server



0% 11% 22% 66%

Real world issues

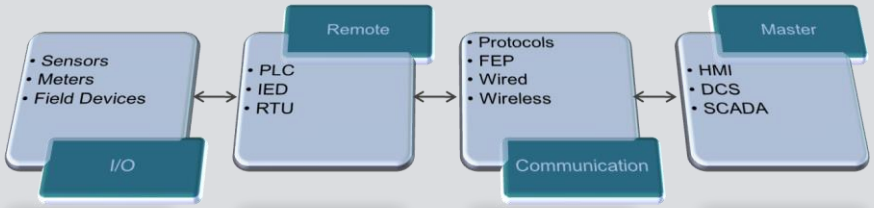
Un-necessary services



0% 11% 22% 66%

Real world issues

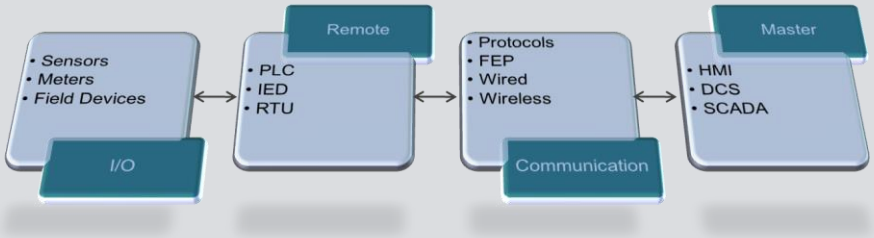
Internal differences between IT and SCADA engineers



0% 11% 22% 66%

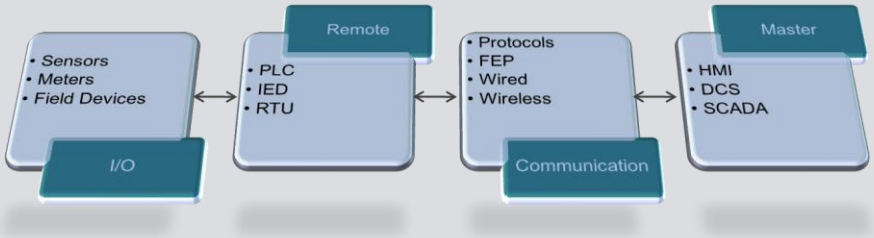
System Wide Challenges

Long life cycle of a SCADA system

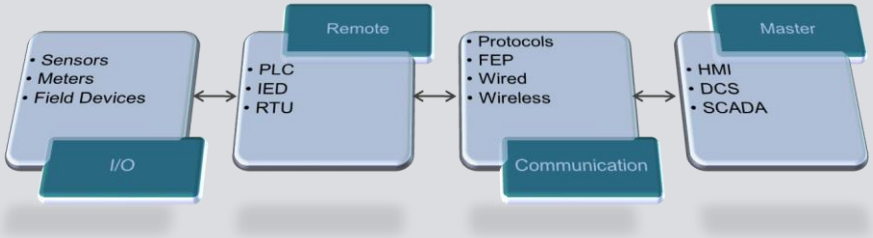


System Wide Challenges

Cost and difficulty of an upgrade

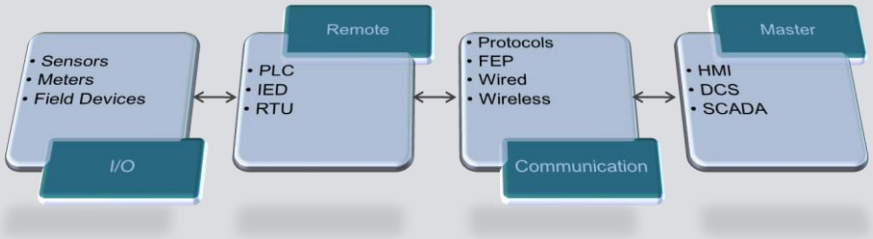


Proposals



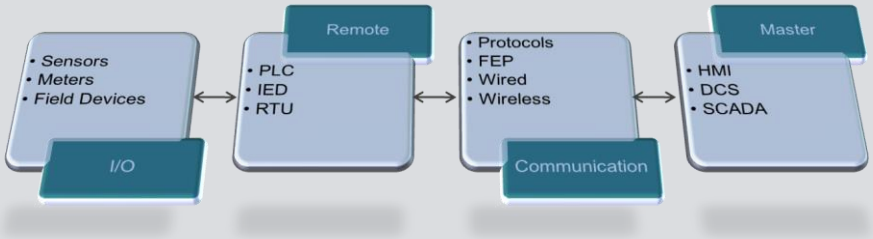
SCADA network auditing

Proposals



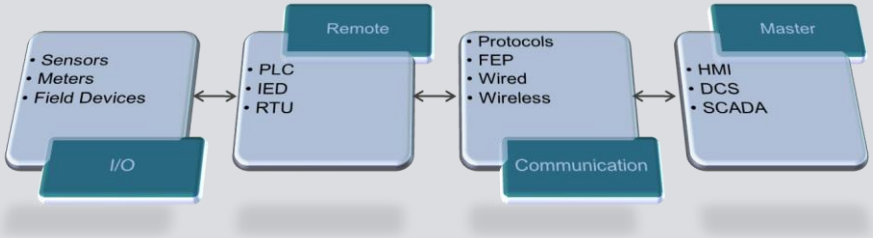
Is you SCADA system exposed on the internet?

Proposals



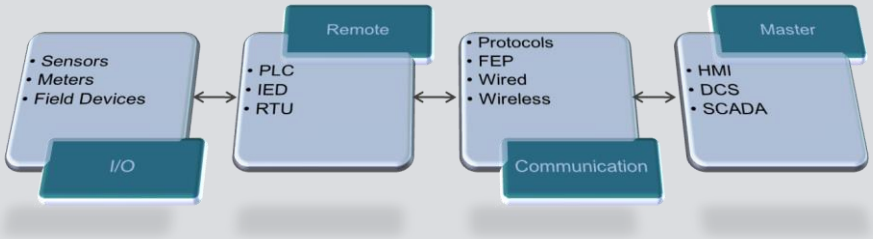
Password policy, access control and access roles

Proposals



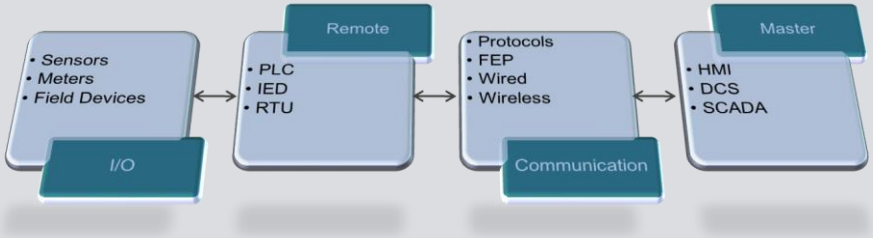
Are all services necessary?

Proposals



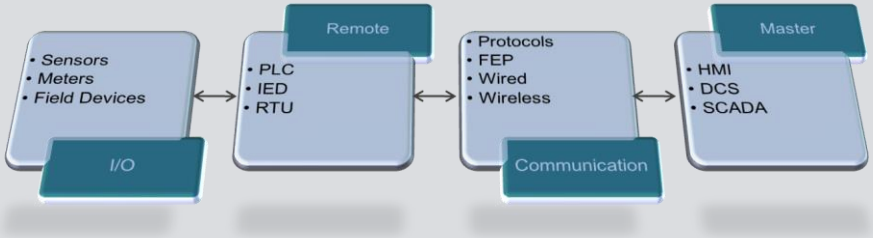
Use secure protocols

Proposals



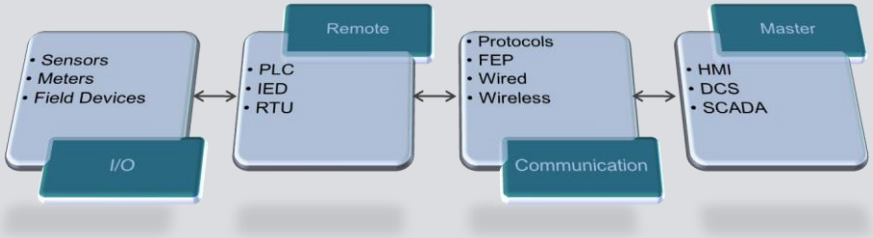
Strategy for Software Update and patching

Proposals



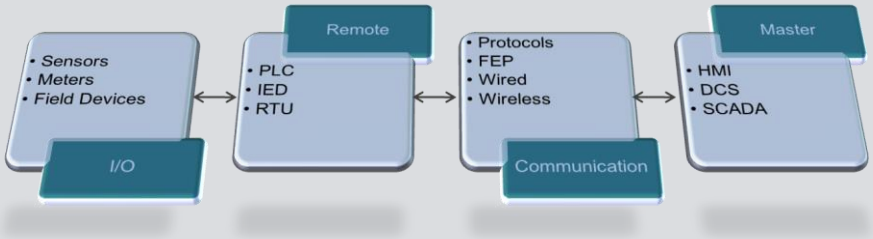
SCADA test environment

Proposals



Keep up-to-date with vulnerabilities

Proposals



Apply experience from IT network management

Thank You

 @amolsarwate