RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Why is SCADA Security an Uphill Battle?

Amol Sarwate
Qualys Inc.

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

Agenda
议程

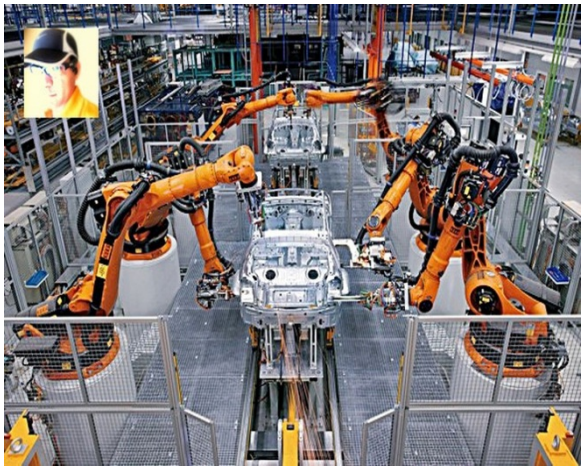
- SCADA Basics
- Threats (where, why & how)
- Challenges
- Recommendations and Proposals
- ScadaScan tool

What are SCADA systems?

RSA CONFERENCE CHINA 2012








QUALYS®

accidents

liquid pipeline failures

http://www.ntsb.gov/doclib/safetystudies/SS0502.pdf

power failures

http://www.nerc.com/docs/docs/blackout/Status_Report_081104.pdf

other accidents

http://en.wikipedia.org/wiki/List_of_industrial_disasters

vandalism

vandals destroy insulators

http://www.bpa.gov/corporate/BPAnews/archive/2002/NewsRelease.cfm?ReleaseNo=297

insider

disgruntle employee

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

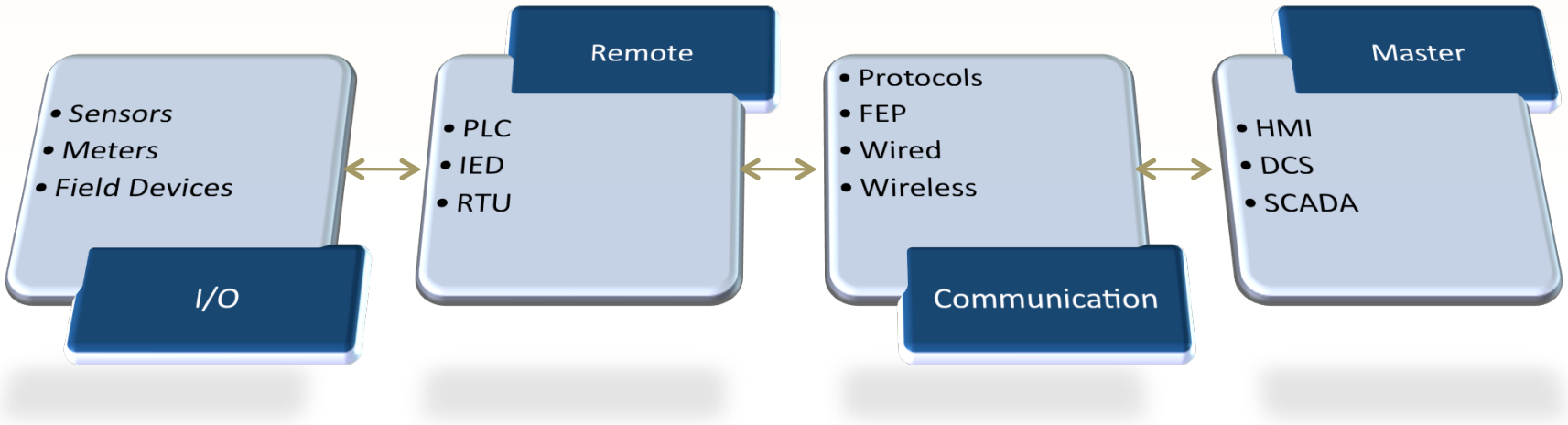
APT

(advance persistent threats)

terrorism or espionage

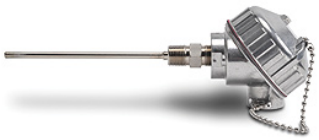
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

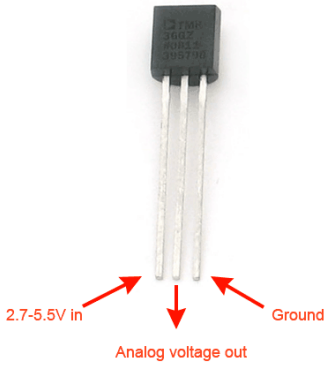
basics

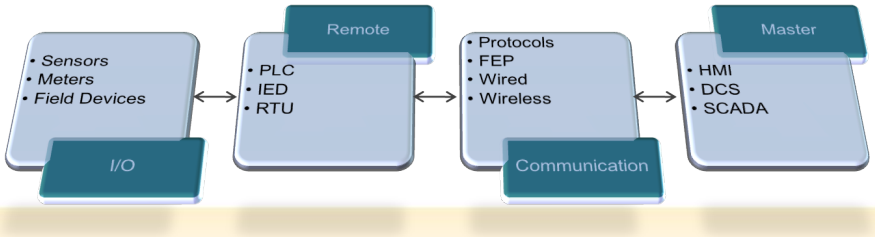

• Sensors
• Meters
• Field Devices
I/O
Remote
• PLC
• IED
• RTU
• Protocols
• FEP
• Wired
• Wireless
Communication
Master
• HMI
• DCS
• SCADA
Field
Control Center

acquisition

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



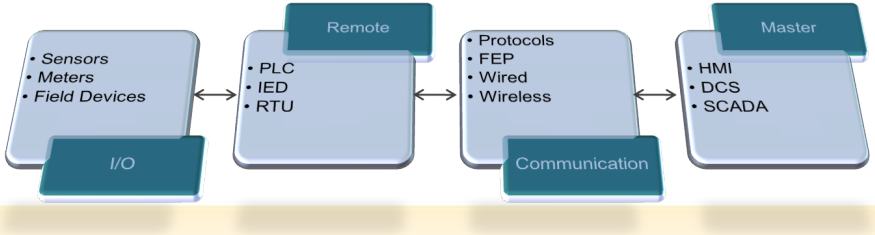




conversion

Converts analog and discrete measurements to digital information



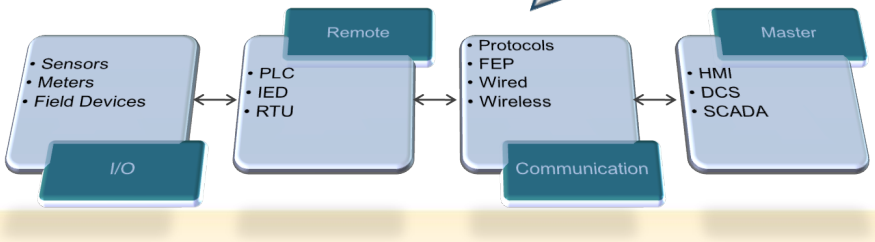



communication

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

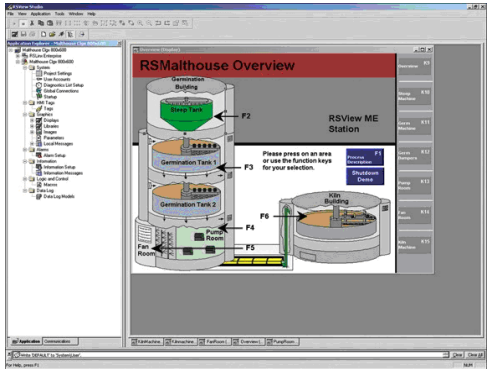


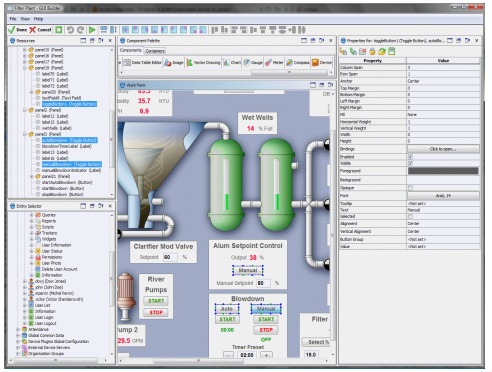
Modbus	DNP 3	OPC
ICCP	ControlNet	BBC 7200
ANSI X3.28	DCP 1	Gedac 7020
DeviceNet	DH+	ProfiBus
Tejas	TRE	UCA

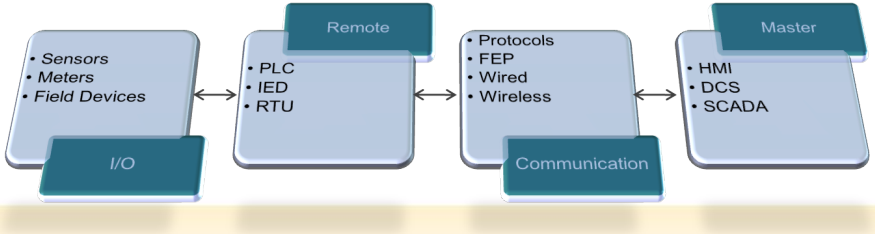


presentation & control

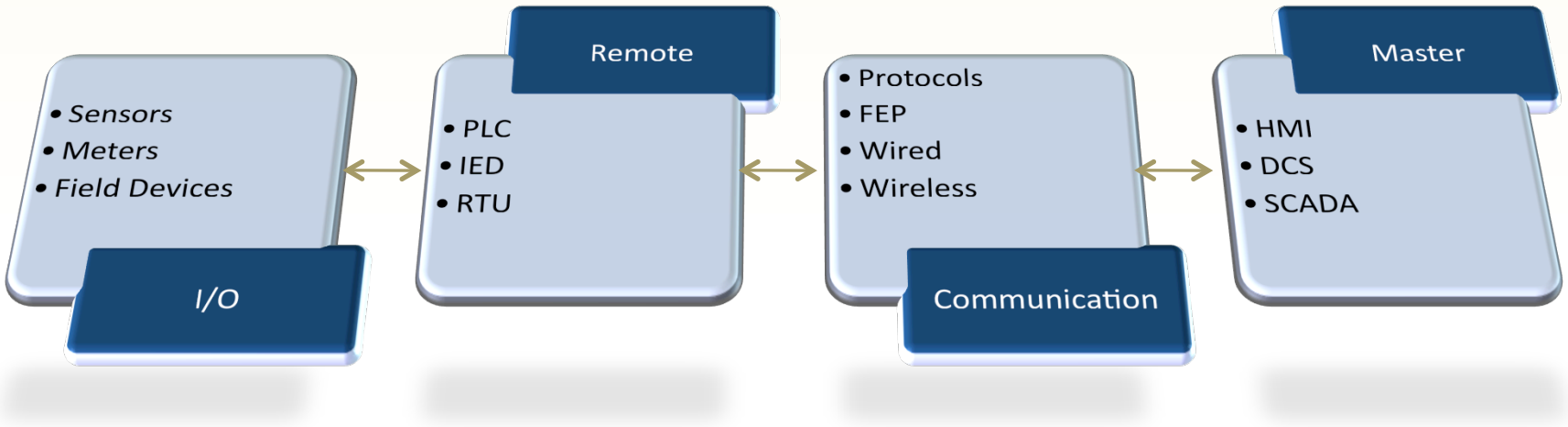
Control, monitor and alarming using human machine interface (HMI)

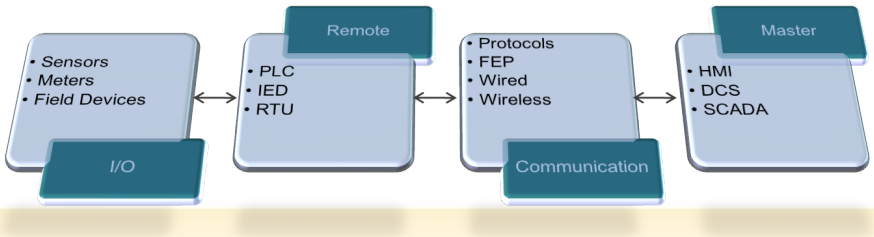




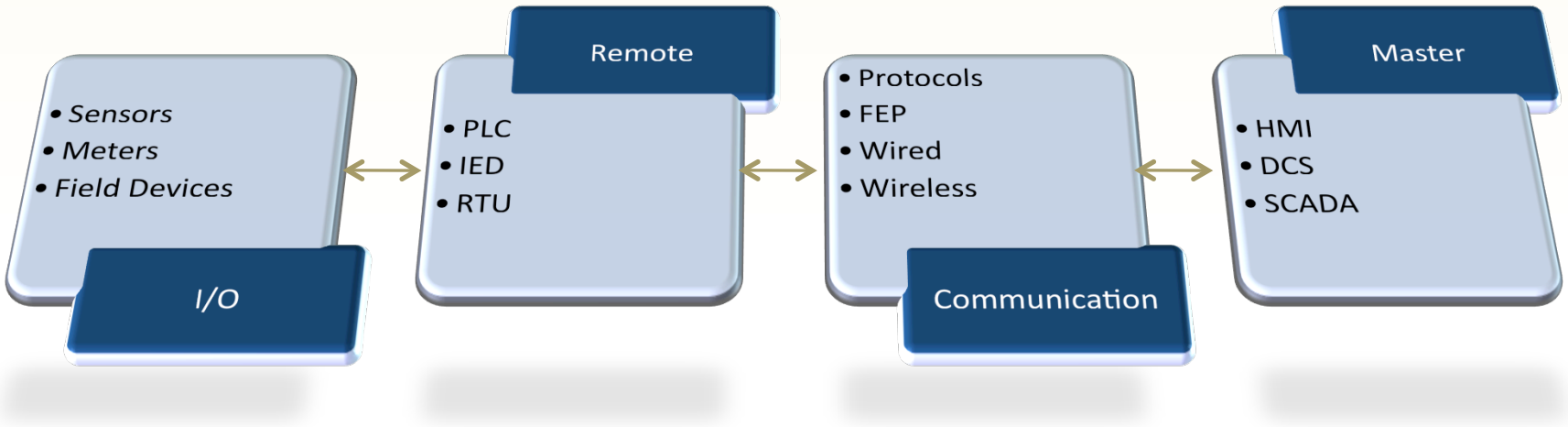


threats?


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

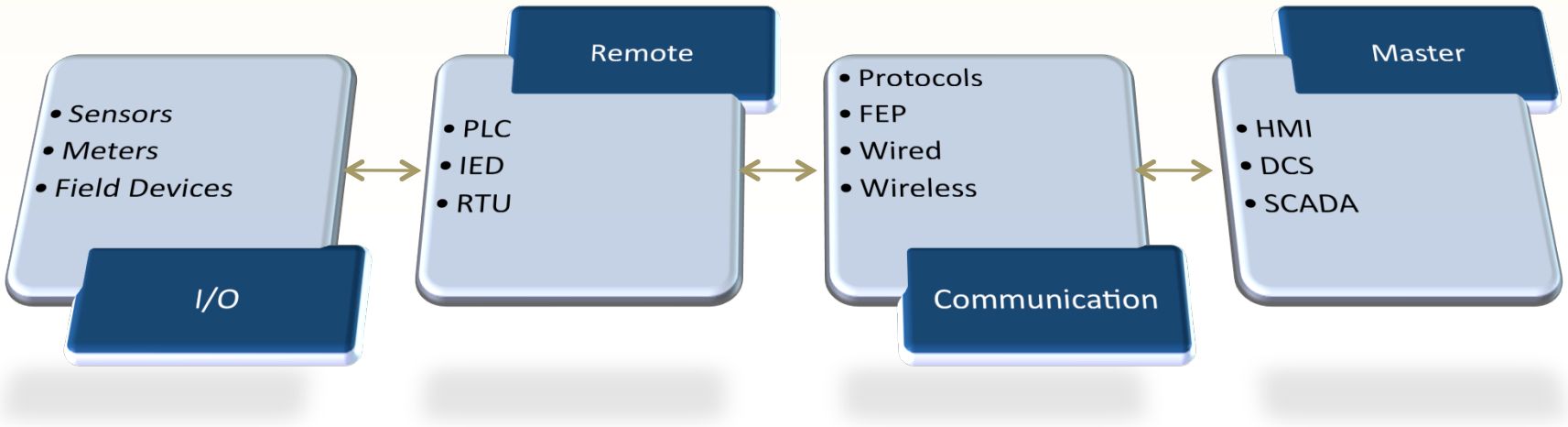

• Sensors
• Meters
• Field Devices
I/O
Remote
• PLC
• IED
• RTU
• Protocols
• FEP
• Wired
• Wireless
Communication
Master
• HMI
• DCS
• SCADA

io & remote



- Requires physical access
- Field equipment generally does not contain process knowledge
- Without process knowledge leads to nuisance disruption

communication



- Change FEP output which is HMI input
- Protocol threats

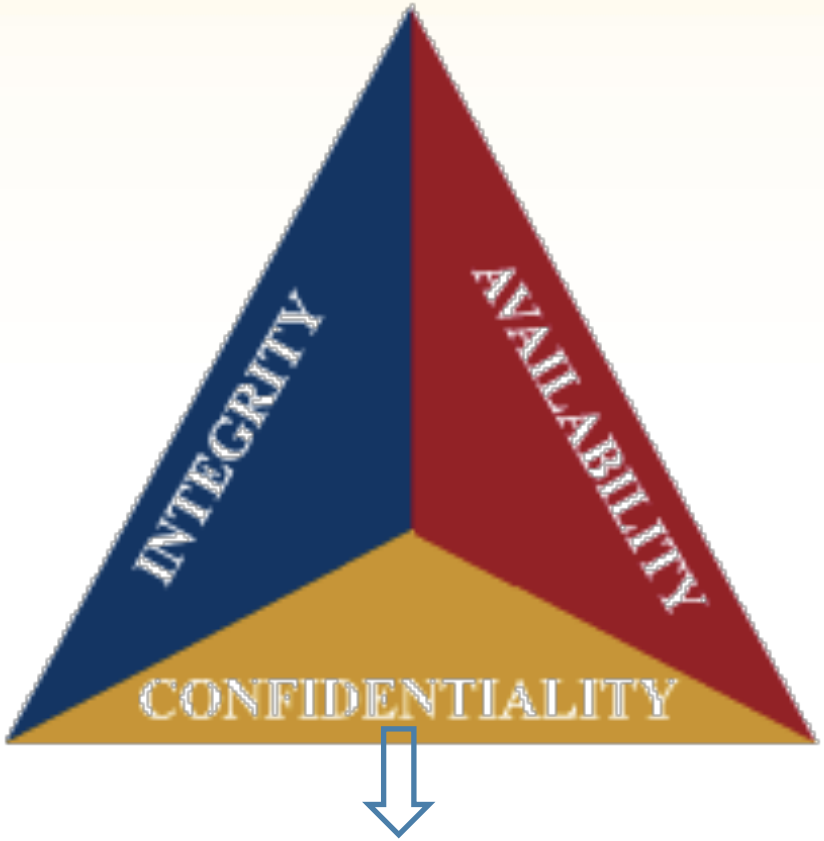
ScadaScan (an example)

```
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.
```

```
C:\SCADA>perl scadascan.pl -m 10.40.1.182

Working on 10.40.1.182.......................... Modbus unit ID 28 found
```

Protocols

What do SCADA protocols like modbus or DNP 3 provide?



Authentication and Authorization

Secure DNP 3.0

Version 1.0 specification released in Feb 2007

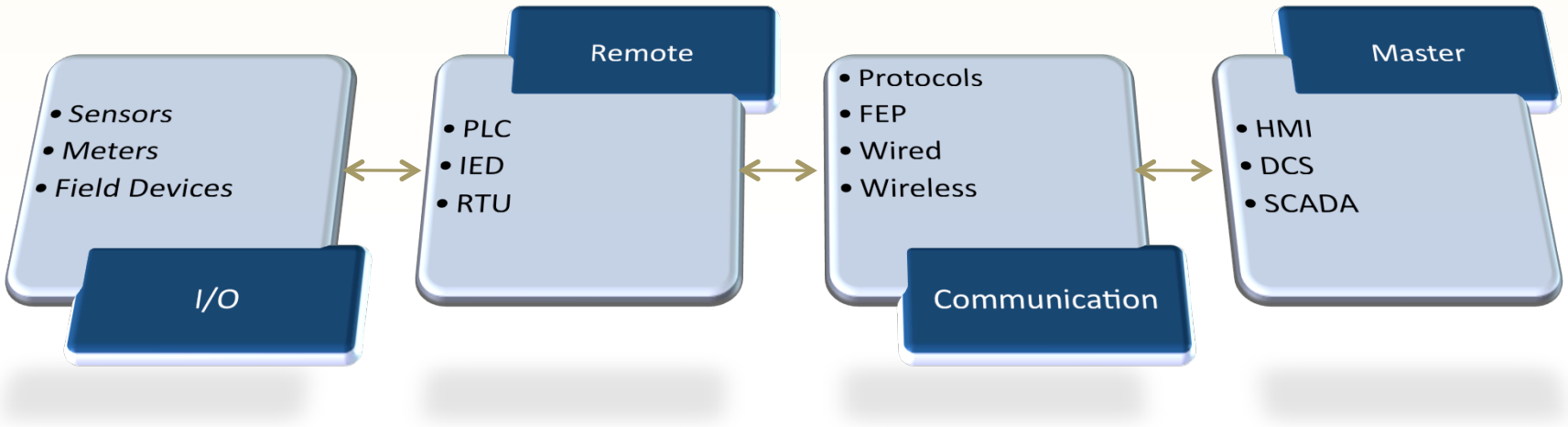
Authentication
- Initialization
- Periodic
- Critical Function Code Requests
- Implementation Specific

Cryptography
- Keyed Hashing for Message Authentication (HMAC)

Key Management

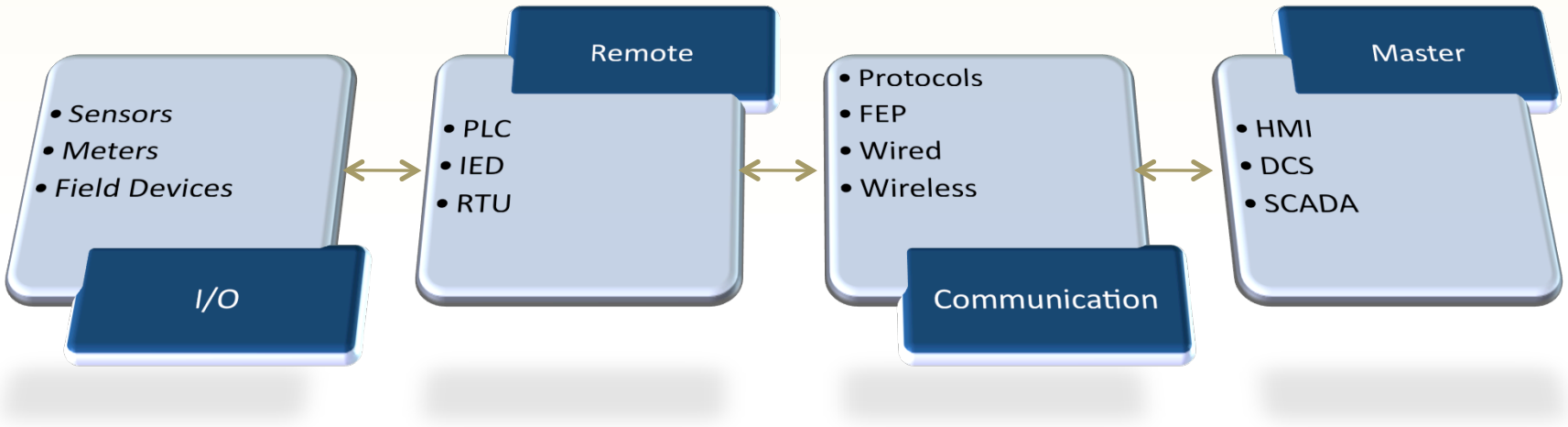
New Function Codes

master threats



- Control system network connected to corporate network or internet
- No authentication or per user authentication
- Shared passwords or default passwords
- No password change policy

master threats



- No patching
- Not restarted in years
- Unnecessary services
- Off-the-shelf software

challenges
挑战

- SCADA system long life cycle
- Difficulty and cost of upgrading
- No testing or guidance about OS patches from SCADA vendors
- Some systems managed by SCADA vendors
- Data historians and other systems on the SCADA network
- Wrong mentality - SCADA too obscure for hackers

idea
主意

- Strategy for password policy, access control, access roles
- Strategy for software upgrades and patches
- SCADA Test environment
- Demand from SCADA vendors:
  - Expedite testing and approval of OS patches
  - Newer and secure protocols
- Apply experience from IT network management and security
- SCADA vendors Auditing and Scanning

Thank You

Twitter: @amolsarwate
http://code.google.com/p/scadascan/

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012