WATERFALL®

Stronger Than Firewalls

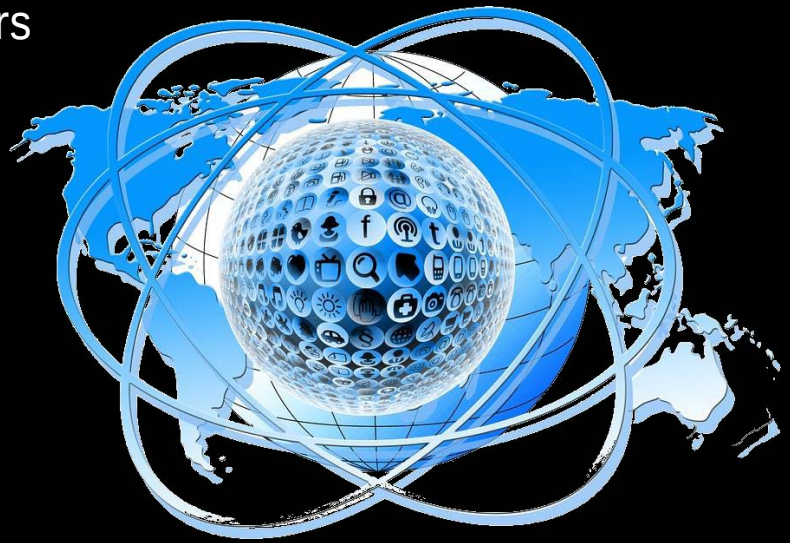
Research Area:
Securing Inbound Cloud/IIoT Information Flows

Andrew Ginter, VP Industrial Security

WATERFALL®
Stronger Than Firewalls

Industrial Internet of Things

- GE Predix – claim $6B annual revenues already
- Microsoft Azure has significant IIoT push
- Industrial Internet Consortium – 270 members
- Vision: flat networks, universal connectivity, remote operation, and edge/fog/cloud computation



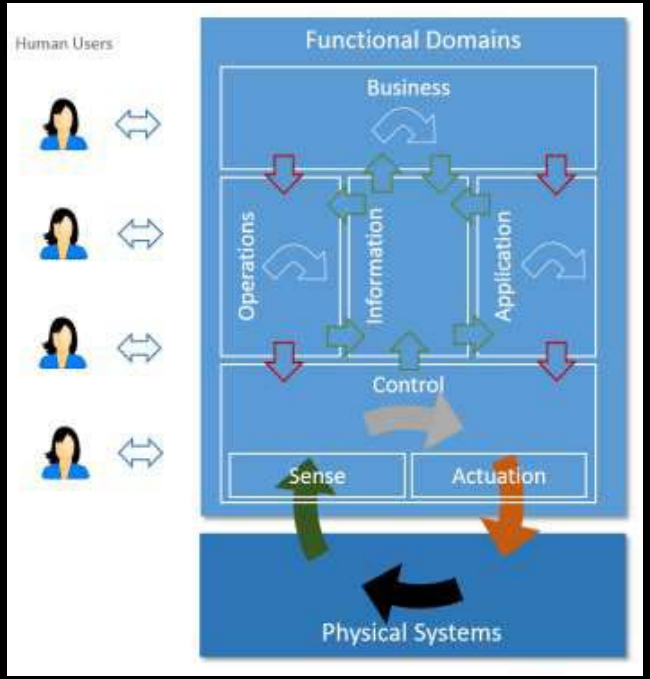
The IIoT makes everything easier – for us, and for our enemies

WATERFALL®
Stronger Than Firewalls

Industrial Internet Consortium Reference Architecture

- Distinguishes “data” (green) flows from “command / request” flows (red)
- Consequences of mis-control are often much more serious than of monitoring data breaches
- But – no advice as to how to treat different flows
- IIoT security focus: cryptosystems, TPM, “secure boot,” root-of-trust, strong authentication

IIC SF: “…stolen credentials may allow attackers to control physical infrastructure remotely”



IIoT Security Fundamentals

- Nothing is “secure.” All software can be hacked.
- All cyber-attacks are information, and every bit of information can be an attack
- Residual risks after universal encryption & authentication:
  - Compromised endpoints & remote access
  - Platform vulnerabilities, mem-resident / scripted attacks
  - Errors & omissions in IT systems

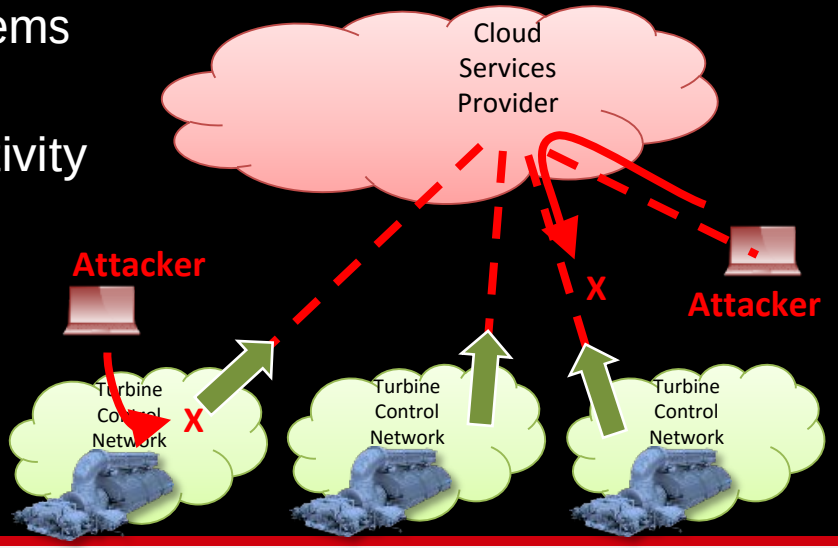
For most practitioners, connecting reliability-critical networks to the Internet through only a firewall is heresy

WATERFALL®
Stronger Than Firewalls

Unidirectional CloudConnect = Safe Monitoring

- Unidirectional hardware makes outbound attacks practically impossible, and inbound attacks impossible without insider help
- Control-system-to-cloud data format / protocol translations make connections directly from control systems to the Internet / cloud safe
- Unidirectional CloudConnect as only connectivity means only compromise path is physical

If every bit can be an attack, prevent any bits returning into critical networks



Online Control *Can* Be Essential

- Eg: when substation is on fire, have to tell neighboring substations to redirect power flows
- Can we limit the damage that can be done by encrypted, authenticated, and *compromised* control sources?
- Classes of attacks:
  1. Seemingly-benign message triggers autonomous, pre-seeded malware
  2. Unauthorized or incorrect remote control
  3. Malware propagation

Open question: what can be done about these?

WATERFALL®
Stronger Than Firewalls

To Prevent Compromise Via Control Signals – Can We…

1. … randomize control signals to prevent activation of pre-seeded malware?
2. … permit remote users / apps only to select between known-safe/reliable operating modes rather than specify arbitrary controls? *Is such a design always possible – in theory? In practice?*
3. … eliminate the possibility of malware propagation or other platform compromise? Eg: through communications equivalent to a 4-20 mA loop? *How would we encrypt or authenticate such control signals?*

Other Possible Protections – Can We …

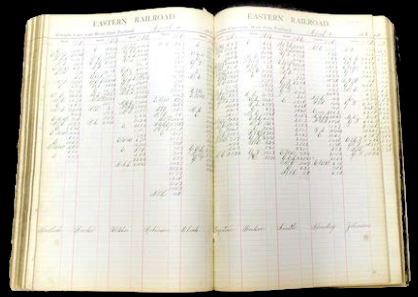
- … structure controls to ensure they are, as "inspectable" as possible for correctness, reliability and safety?
- … have sets of cooperating, independent control systems detect and reject incorrect controls – eg: to prevent cascading failures?

WATERFALL®
Stronger Than Firewalls

Data vs Monitoring vs Control

- IT history: leger books / accounting data / transactions
- Industrial network history
  - Guages = monitoring = IT data
  - Switches & dials = control = safety/reliability critical
- IT experts say “it’s all data,” but this blinds us to crucial difference between monitoring and control
- Correct control is vital to physical safety and physical reliability

We cannot restore human lives, or damaged turbines “from backups”



VS