AMI Security

Introduction Through Advanced

Andrew Ginter

VP Industrial Security
Waterfall Security Solutions

2020

Data vs Monitoring vs Control

- IT history: leger books / accounting data / transactions
- Industrial network history
  - Gauges = 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

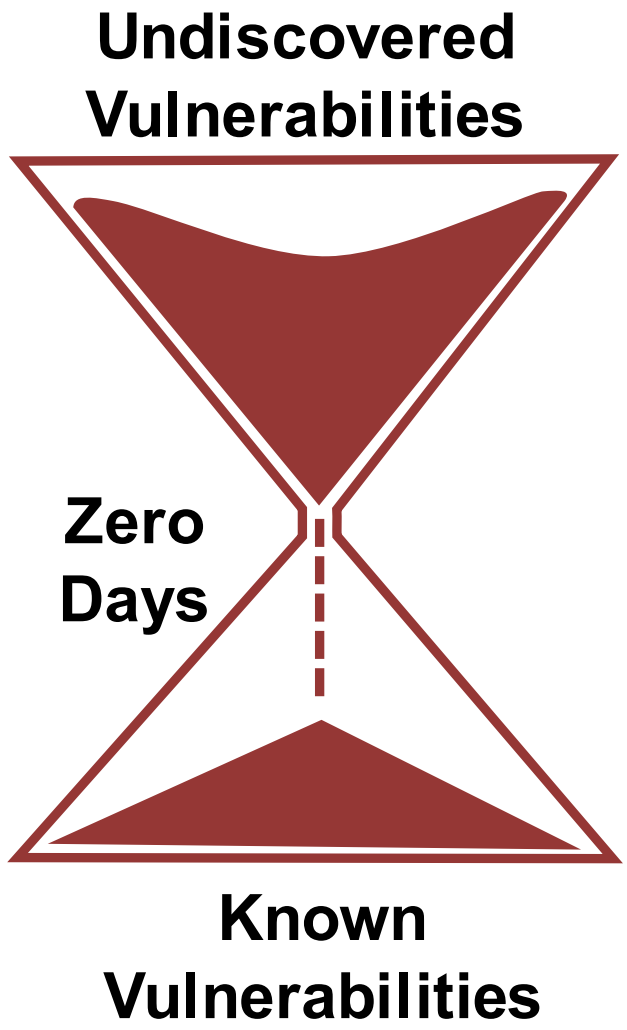
Control is not AIC, CIA or “IT data” – control is really important

VS

Too Much Focus On Vulnerabilities

- If we could only get rid of our vulnerabilities, then we would be *invulnerable!*
- “Vulnerabilities” are quickly confused with “known vulnerabilities”
- And the security program turns into “quick – patch everything!”

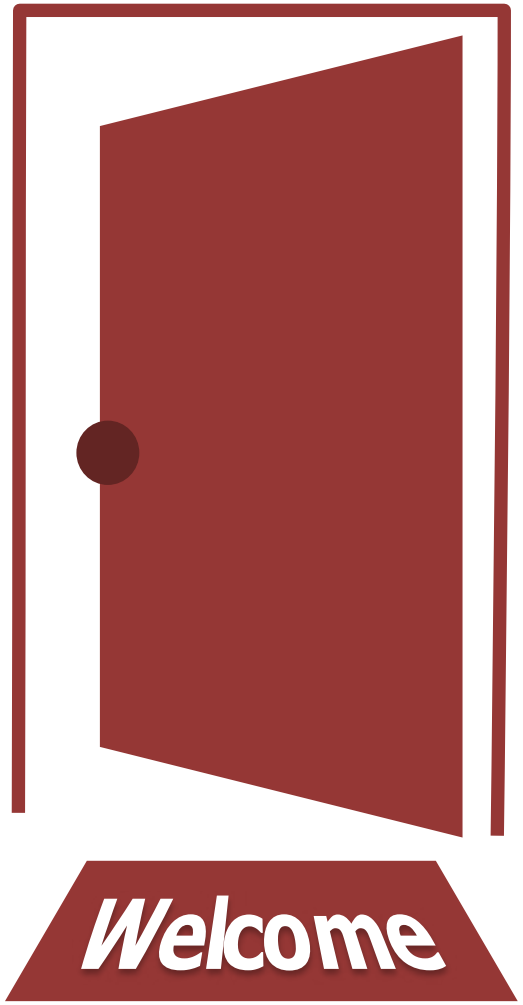
This is of course nonsense, and costly as well



Attackers Prefer Permissions

- Remote access attacks piggy-back on legitimate sessions /
  permissions, such as remote access sessions
- Phishing attacks steal credentials
- Pass-the-hash attacks re-use existing credentials
- Databases & other servers permit remote execution
- Remote Access Trojans (RATs) provide remote control to understand target, steal credentials & make next move

Why write code to exploit vulnerabilities when attackers can log in and execute what they want?



First Three Laws of SCADA Security

WATERFALL
Stronger Than Firewalls

- Nothing is secure
- All software can be hacked
- All cyber attacks are information, and every bit of information can be an attack

In the worst case a compromised CPU will issue every unsafe instruction to the physical process that the CPU is physically able to issue

Firewalls Will Save Us

WATERFALL® Stronger Than Firewalls

- Many attacks: steal password, attack servers through the firewall with buffer overflows & sql injection, piggy-back on VPN, etc.
- Signature-based IPS is blind to new attacks – invent one with a fuzzer
- Hide exfiltrated data in legitimate web app NG firewall thinks it understands
- Attack servers outside firewall that are trusted by equipment inside firewall

Firewalls are porous. All firewalls forward messages from less-trusted networks to more-trusted ones

Photo credit: Red Tiger Security

Encryption Will Save Us

- Same key in each device is easily stolen
- Encryption protocols are frequently broken
- Encryption algorithms age and are broken
- Encryption software has bugs and are compromised
- Operating systems are software and are compromised, without compromising encryption
- Cryptosystems encrypt attacks just as happily as they encrypt legitimate comms

To defeat encryption, compromise an endpoint

Anti-Virus Will Save Us

- Signature-based defense – only effective against known attacks
- No signatures for “new” malware – no matter how simple or how sophisticated the malware
- No signatures for low-volume / targeted malware
- Have your malware turn off the AV tool

To defeat AV write your own bits of malware, and deploy them sparingly

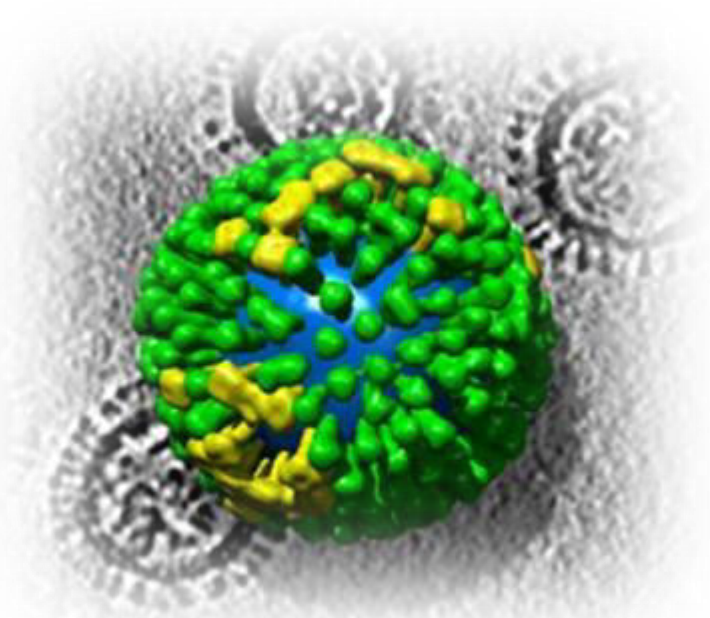


Photo credit: National Institutes of Health

Security Updates Will Save Us

WATERFALL
Stronger Than Firewalls

- All software has bugs, and some bugs are vulnerabilities, so all software can be hacked
- Security updates address known vulnerabilities, not zero-days
- Delay between vulnerability disclosure and update is opportunity to attack
- Security updates cannot defeat stolen or shared passwords or other permissions exploits

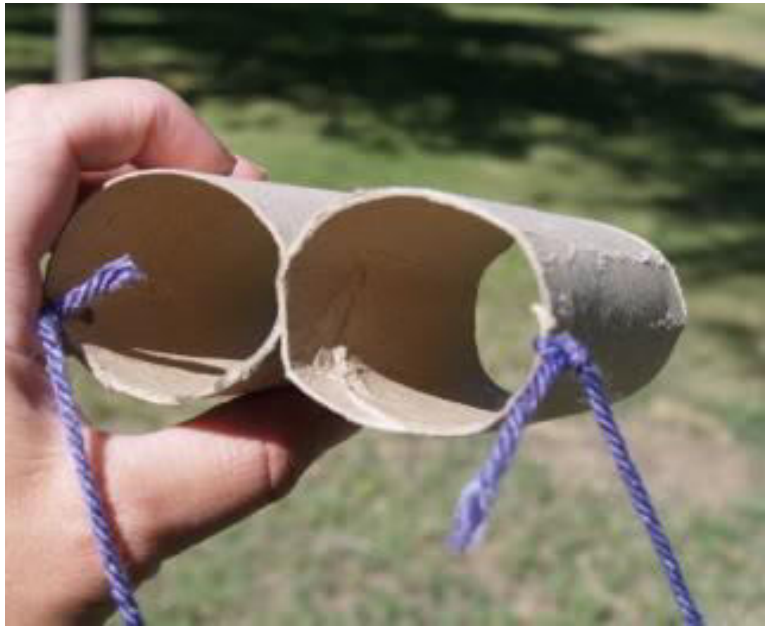
To defeat software updates, steal or create a password, then just log in

Intrusion Detection Will Save Us

WATERFALL
Stronger Than Firewalls

- Signature-based detection is blind to new attacks – invent one with a fuzzer
- Anomaly detection is defeated by low-and-slow attacks
- False alarm investigations cost time and talent
- Successful detection and remediation of real intrusions, assuming they are investigated to begin with, take time

How long can we let an intruder "stir the pot" in our power grid?



Information Sharing Will Save Us

WATERFALL
Stronger Than Firewalls

- Information sharing shares futures: threat actor tracking, black-market tools capabilities, indications of immanent targeting. Eg: Ukrainian utilities: Russians are likely to target you
- Shares past – indicators of compromise when compromise is discovered in an organization. Eg: 3 Ukrainian utilities were compromised and 225,000 people were without power, with these indicators of compromise…

When a sophisticated ransomware or other attack simultaneously compromises assets throughout a grid, information sharing is too slow

Classic AMI Security Advice

- Encryption
- Security Updates
- Firewalls
- Anti-virus & IPS – in back office
- Intrusion Detection / Security Monitoring
- Power / Billing Anomaly Detection
- Auditing & Surveillance

Problem: classic advice addresses low-impact power theft, but does not prevent sophisticated attacks, but may detect attacks after attackers have been in the system for some time

Limitations of Classic Advice

	Script Kiddies	Corp Insiders	Ransom ware	ICS Insiders	Hack-tivists	Targeted Rans-wre	Intel Agencies	Military Grade
Resources	Tools	Trust	Pros, $$	Trust	Amateur	Pros, $$	Pros, $$$	Pros, $$$, physical
Consequence	Low per incident	Med per incident	High	High	High	High	Very High	Very High
Frequency	High	Med	Med	Low	Low	Low	Low	Very Low
Corp Focus	High	High	High	Some	Some	Poor	Poor	Very Poor

Most organizations focus on High Frequency / Low Impact (HFLI) events, and expect the government to save them from HFLI events

But: the government cannot save industrial sites from nation-state-grade attacks – information sharing & incident response is too slow

High-Impact Consequences

WATERFALL® Stronger Than Firewalls

- Public safety: toxic releases, explosions near population centers, contaminated human consumables (water, food, medication), lack of access to essential services – electricity, water, fuel, transportation
- Environmental: damage, disasters, catastrophes
- Worker safety: toxins, explosions, asphyxiation
- Equipment damage: turbines, pipelines, HV transformers
- Downtime: lost production & revenues, restart delays & costs
- Reputation damage: due to all of above

There was a time when only "accidents" could cause high impact consequences – nowadays, generally all these consequences can have cyber causes as well

High-Impact Consequences

Class	Consequence	Mitigation
Public Safety	Cascading Outage	Design time
	Compromised Stovetop	Software only
Environmental		
Worker Safety		
Equipment Damage	Destroy millions of meters	Design time
Downtime	Widespread theft	Software only

Physical Mitigation

Only physical access to process/device can defeat physical mitigation

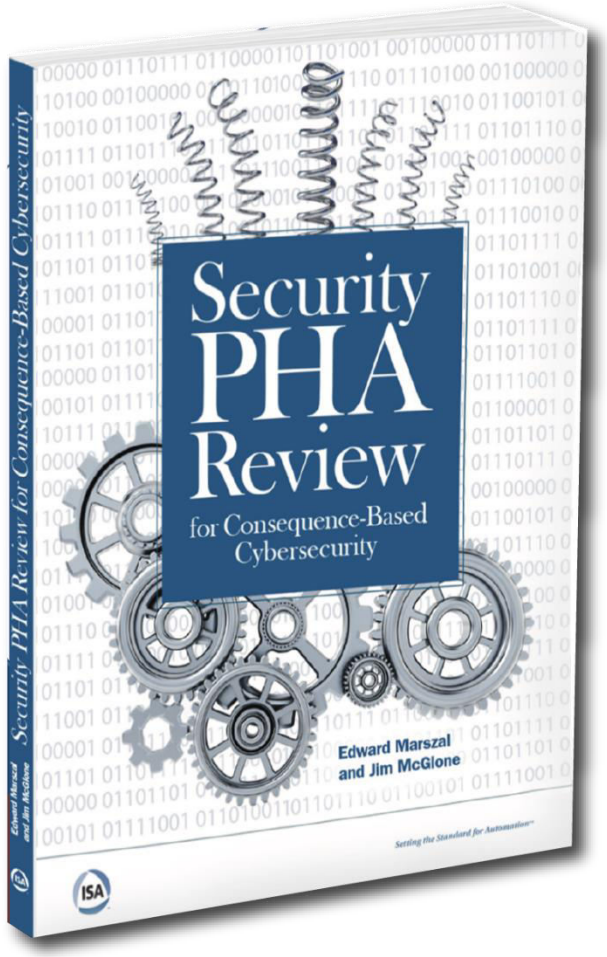
Software Mitigation

Mitigation can be defeated remotely

New: Security PHA Review

WATERFALL
Stronger Than Firewalls

- PHA = Process Hazard Analysis = safety analysis
- Focus: preventing safety incidents
- All cyber systems with direct or indirect access to a routable network are deemed “hackable”
- If safety system is hackable, deploy physical mitigations – over-speed governors, over-pressure valves



With physical mitigations in place, no cyber attack can compromise safety

Coming Soon: CCE

- Consequence-driven, Cyber-informed Engineering
- Focus: safety & equipment-damaging incidents
- Identify your 3-5 most serious potential consequences of cyber assault
- Deploy physical mitigations for them: over-pressure valves, custom digital logic

Idaho National Laboratory

"We can tolerate disruption, but not destruction"

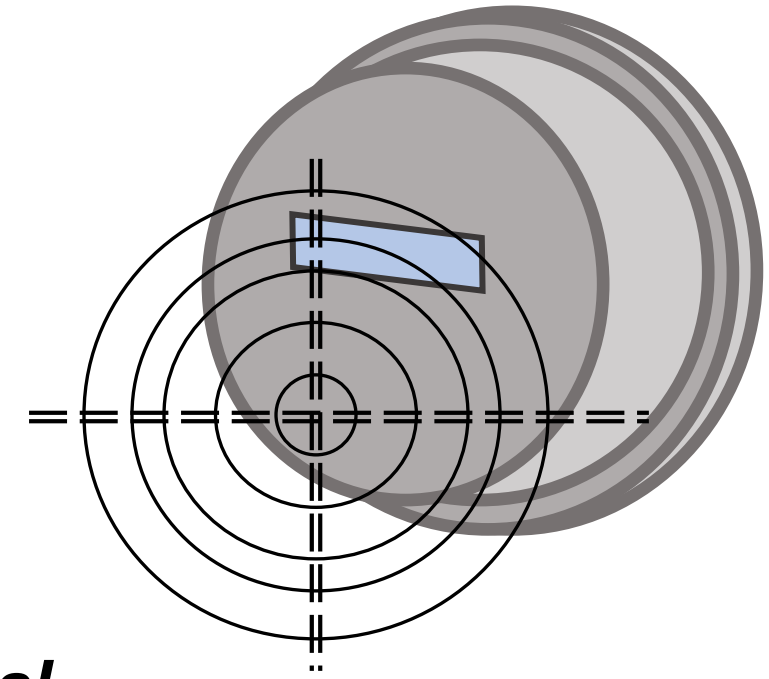
New: SEC-OT

- Secure Operations Technology
- Focus: continuous, correct, efficient operations
- Inventory all online and offline information flows into control-critical networks
- Apply physical discipline to all such flows – disable removable media, apply unidirectional gateway technology

All cyber attacks are information – control the flow of information and we control the attacks

Use Case: Damaging AMI

- Scenario:
  - Worm propagates automatically to most meters in a geography
  - Turns off consumer power
  - Damages meter, or erases firmware
  - 3M meters must be replaced
- Physical mitigations:
  - Design/modify meter to prevent damage
  - Design/modify meter to permit manual firmware restoration



Service should always be restorable via physical access or proximity, no matter what the compromise

Use Case: Cascading Outage

- Scenario:
  - Worm propagates to most meters in a geography
  - Turns all consumers' power off and on again - synchronized
  - Underload – trips generators, overload – trips relays
  - Cascading failure for at least the distribution region
- Physical mitigations:
  - Design/modify meter hardware to introduce random delays into power disable/enable operations
  - Physically disable software power control for most meters

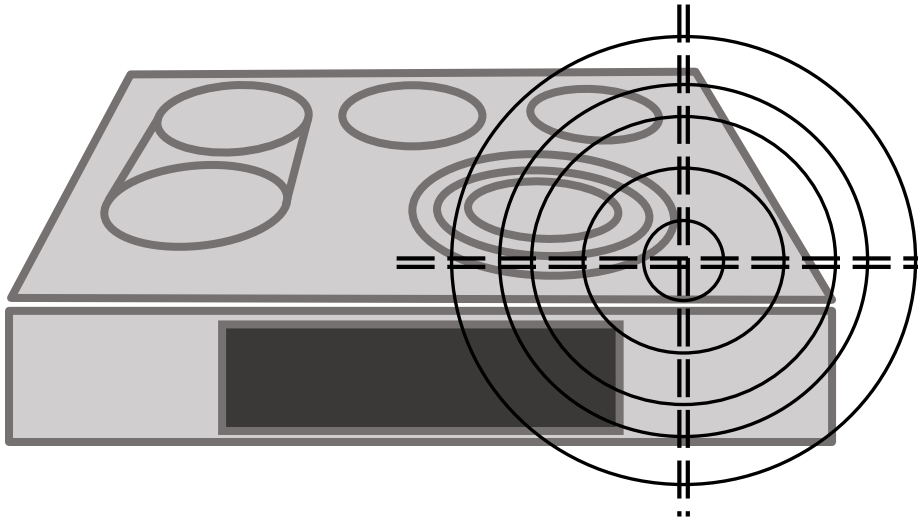
Unacceptable physical conditions should be physically impossible

Photo credit: National Oceanic and Atmospheric Administration / Defense Meteorological Satellite Program image

National Oceanic and Atmospheric Administration / Defense Meteorological Satellite Program image

Use Case: Smart Home/Stove

- Scenario:
  - Targeted attack reaches into smart meter network
  - Compromises meters with memory-resident remote-control malware
  - Malware uses home network to target “smart” touch-screen stovetops
  - Uses one vendor’s stovetop vulnerability to take over 10,000 stovetops
  - Turns on all burners at 2 AM – fires, casualties
- Physical mitigations:
  - 2 CPUs in stovetop – one able to sense & report, other able to control
  - Unidirectional connection between home network and smart meter



But – neither mitigation exists at this time

High-Impact Consequences

Class	Consequence	Mitigation
Public Safety	Cascading Outage	Design time
	Compromised Stovetop	Software only
Environmental		
Worker Safety		
Equipment Damage	Destroy millions of meters	Design time
Downtime	Widespread theft	Software only

Physical Mitigation

Only physical access to process/device can defeat physical mitigation

Software Mitigation

Mitigation can be defeated remotely

Summary

- Sophisticated LFHI attacks are most likely to pose existential threats to electric utilities
- Physical protections are the most robust – governments cannot respond quickly enough to sophisticated attacks
- There must always be a way to recover from the most serious attacks on AMI installations
- *And do still deploy* appropriate sw-based HFLI protections

More information: Industrial Security Podcast, visit WF booth for free book, follow us on Twitter, LinkedIn & Facebook & sign up for our newsletter:

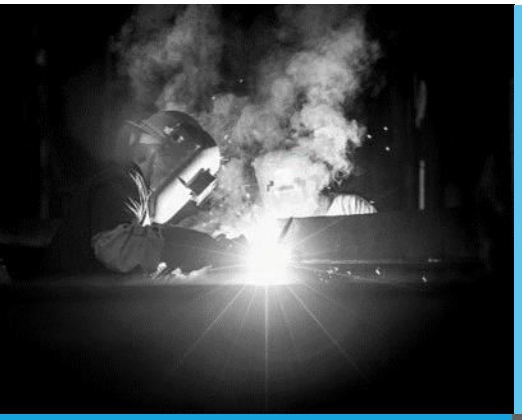
Industrial Security Podcast

Secure Operations Technology

waterfall-security.com

About Waterfall

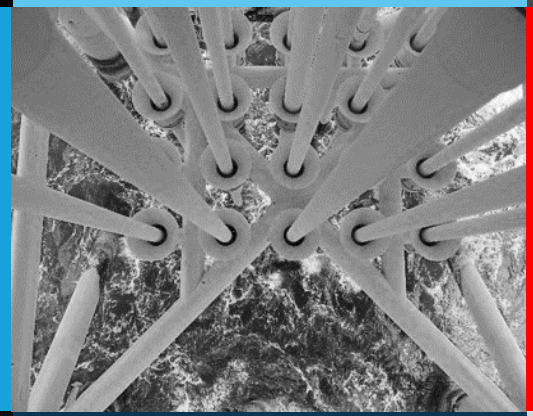
WATERFALL®
Stronger Than Firewalls



Founded in 2007

1000+ sites worldwide

Headquarters in Israel



Deployed in all critical infrastructure sectors

Sales & operations in the USA, EU & APAC

Multiple registered US patents

Technology & sales collaboration with global partners