i-PCGRID - 2013

Alternative to Patching Firmware for CyberSecurity: Adaptive Anti-Malware Protection

Presented by Eric MacDonald, GE Digital Energy

In association with:

Mike Ahmadi, Wurldtech

Nate Kube, Wurldtech

Daniel Thanos, GE Digital Energy

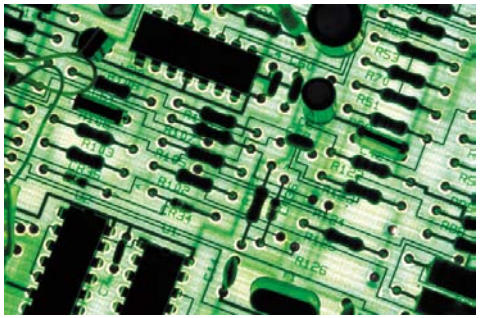
Alexander Damish, Wind River

Agenda

- What Cyber Security Means… in the context of this presentation
- Innovations , Progress and Cyber Security
- Vulnerabilities and Exploits
- Patches and the problems they present
- Adaptive Anti-Malware Protection
- Discussion

What is Cyber Security?

Cyber Security is enabling technology that allows us to take advantage of innovations in communications and electronics to improve our ability to do business by mitigating risks that come with those innovations.



Innovations that Deserve Cyber Security

Innovation	Benefit
Wide area protection and management	Improve power system stability with real time communications between widely dispersed geographical sites
Remote Access	Save time and money by not having highly skilled resources physically travelling to remote sites
Predictive maintenance through non-operational data management	Take advantage of data generated by intelligent electronic devices by maximizing asset life and managing outages proactively
Centralized Remedial Actions Schemes	Maximize the use of assets by deploying widely dispersed and highly integrated protection schemes

Unfortunately, there are those that would get in the way of progress…

STUXNET

FINANCIAL POST

Hackers to exploit new avenues of attack in 2012

The emergence of new hacker strategies to target physical infrastructure, financial institutions and mobile devices made 2011 a transformative year for digital security, says a report released Wednesday. In 2012, the risks will get worse, making everyone from state actors to individual smartphone users a potential target

December 28, 2011

WORLD

NATIONAL POST

Insiders suspected in massive Shamoon virus cyber-attack that wiped 30K Saudi oil company computers

September 7, 2012

Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers

By Michael Riley - Feb 24, 2011 12:26 AM PT

0 COMMENTS

Bloomberg

February 24, 2011

'Shamoon' Virus That Devastated Saudi Oil Co. Likely to Have Done More Damage

CIO

September 18, 2012

BloombergBusinessweek
Technology

Flame Virus Is Part of Cyber Espionage, White Says

May 29, 2012

PCWorld

SECURITY

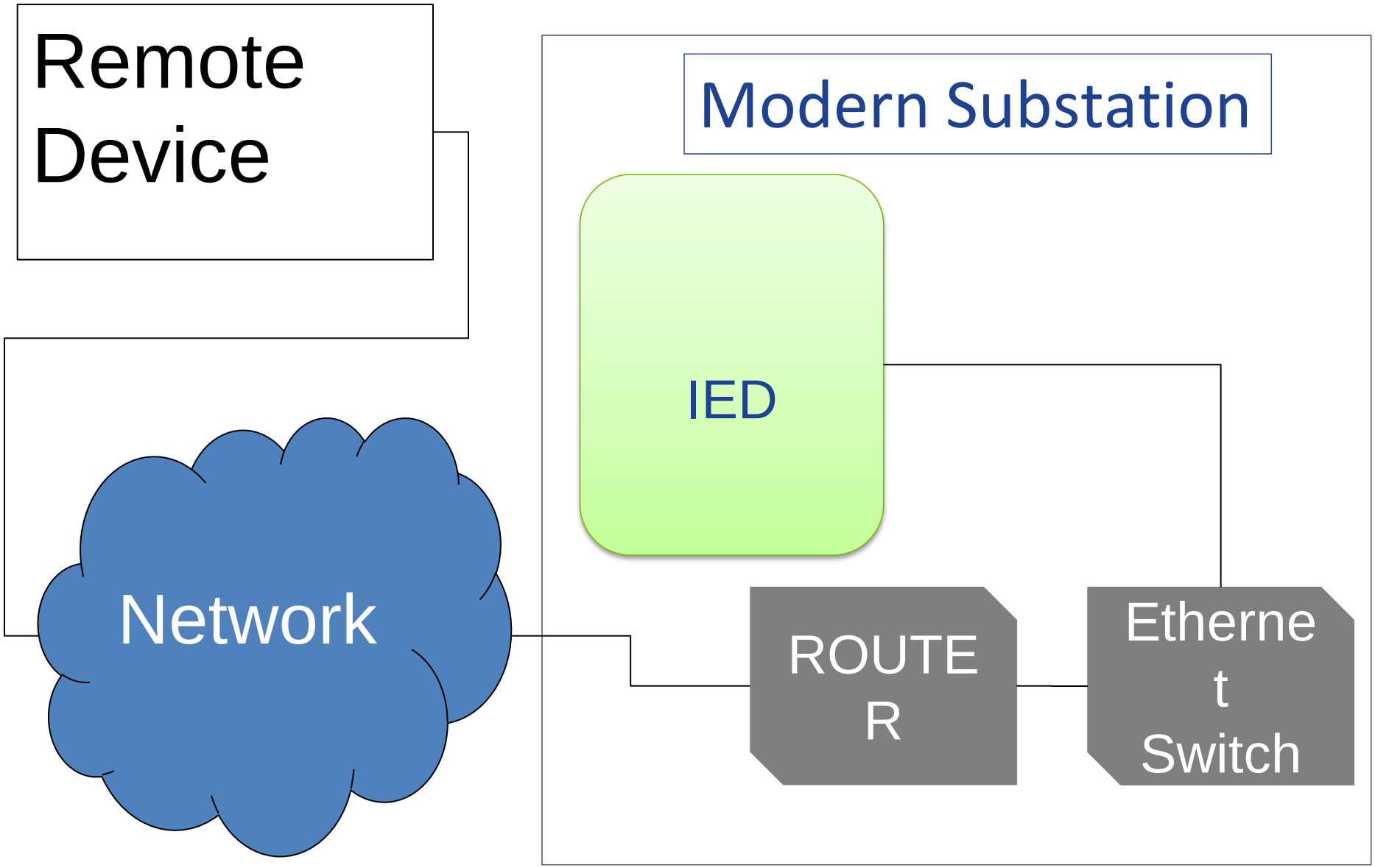
'Night Dragon' Attacks From China Strike Energy Companies

February 10, 2011

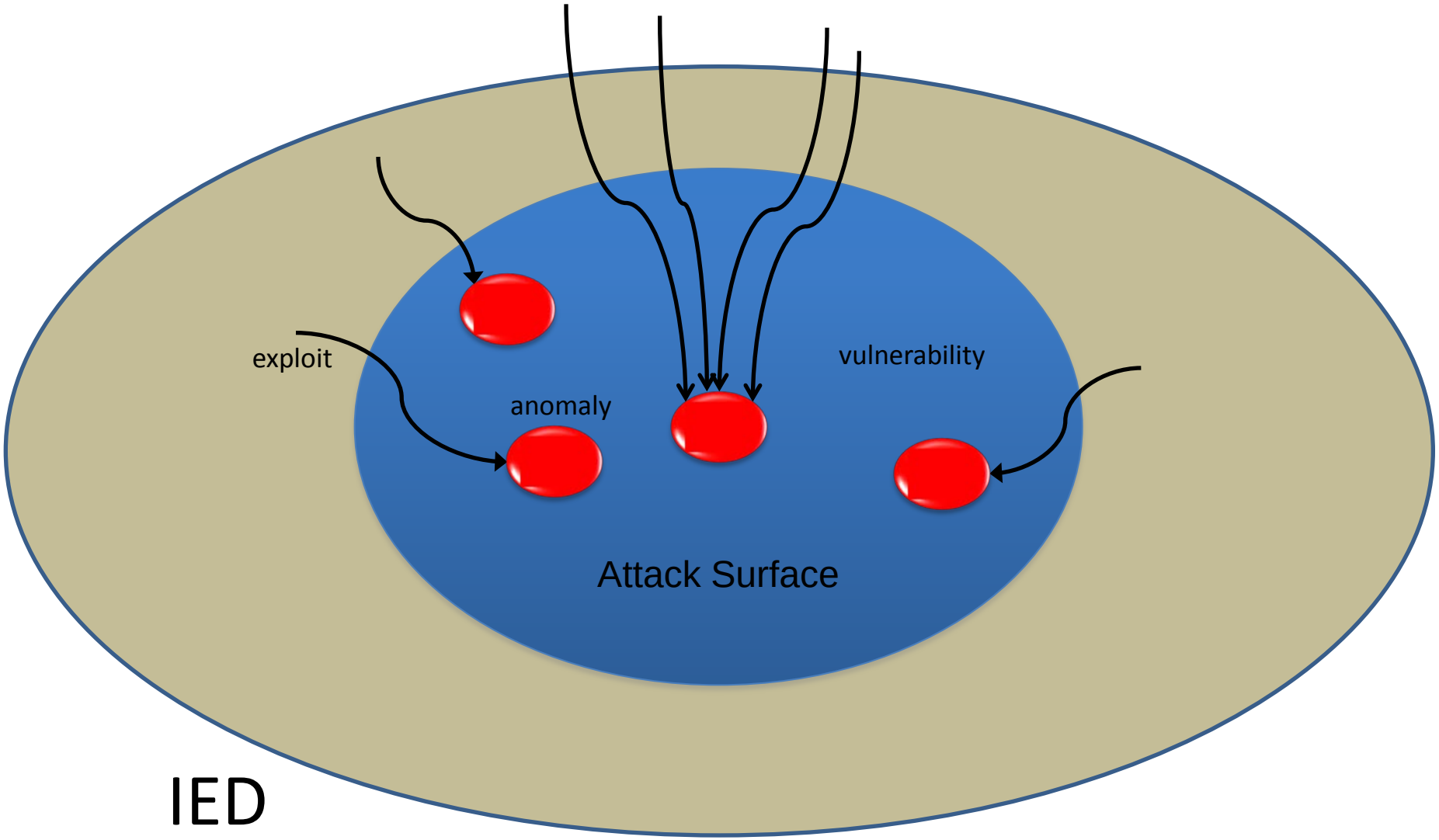
Simplified Terminology

- **Vulnerabilities** – weaknesses in code or architecture design and implementation that offer opportunities for skilled hackers to alter the operation of a system
- **Exploits** – the method in which a vulnerability is utilized to gain access or control over the system
- **Zero Day** – an exploit that has been newly released which the system manufacture has had zero days to address
- **Firmware** – execution code running in an embedded device
- **Software** – computer programs and data
- **Patch** – an update made to running software or firmware

Simple Architecture



Vulnerabilities and Exploits



Cyber Security Challenges

- There are always new threats

- No vendor has ever made a perfect product
  - < 1 flaw per 1000 lines of code (kLoC) is world class
  - e.g. 0.1 flaw per kLoC for Shuttle Code
  - 30-100 flaws per kLoC typical for commercial software

- Updates are costly

Patching in Utilities: Large Scale Problems

- Devices are usually related to critical systems, and downtime is costly (or unfathomable).
- Changes to firmware and configurations demand re-commissioning.
- Locations are widely dispersed geographically
- Patches may or may not be necessary.

Utilities need to manage constantly changing Cyber Security in a traditionally Static World

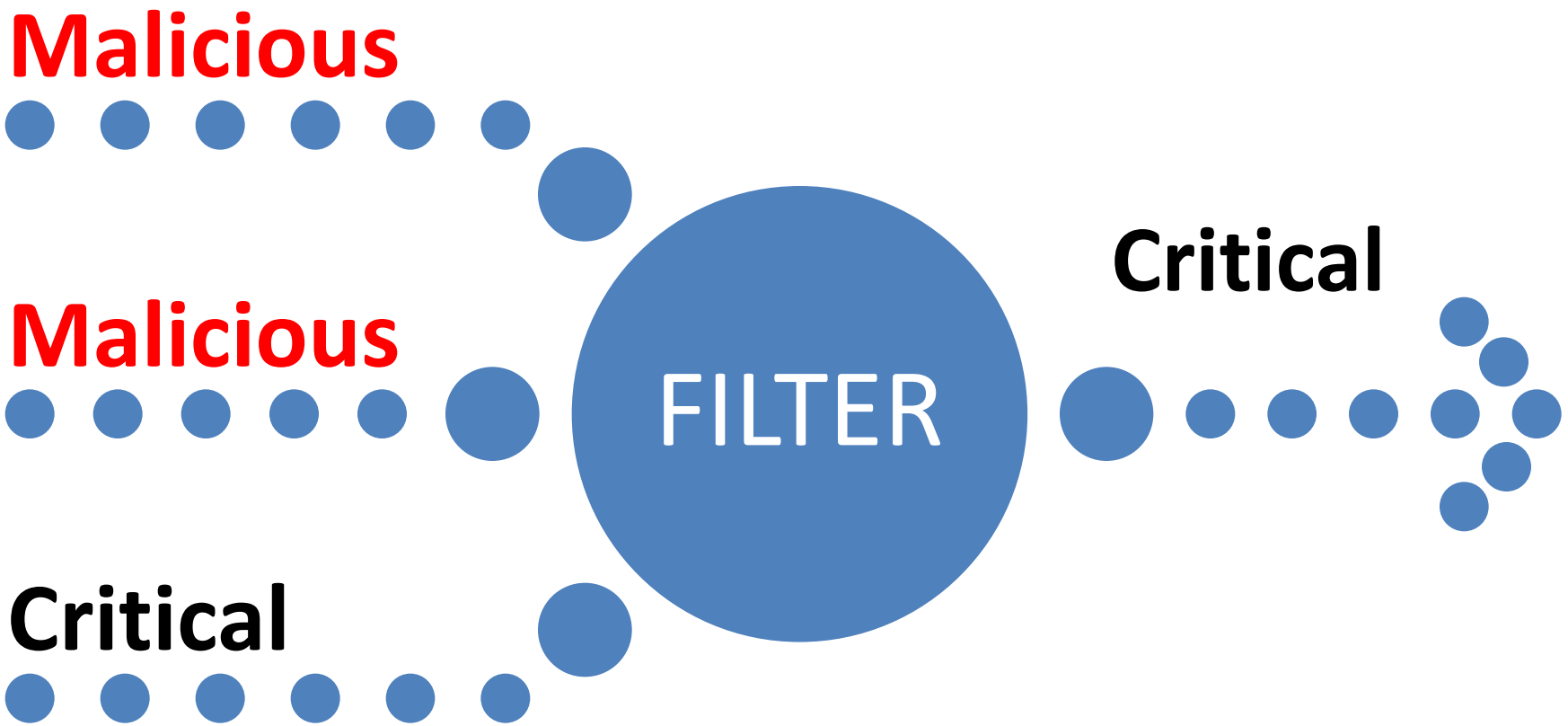
It is important to remember whose problems you are trying to solve. If you set out to provide security generically to all devices in all places and all applications you are sure to fail.

Concentrate on the devices you need to secure first. Your own!

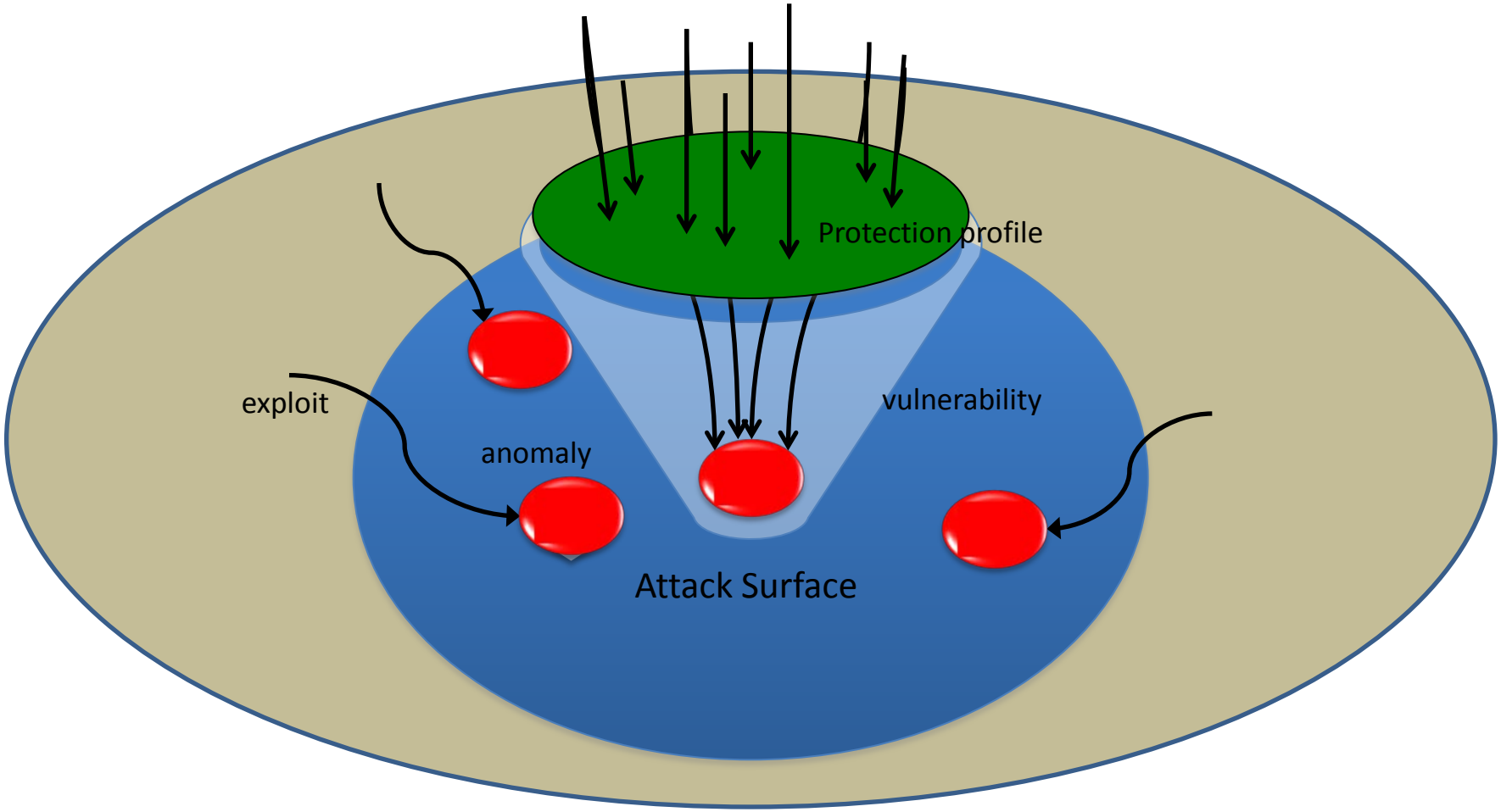
Anatomy of a solution

- Provides Security to chosen devices
- Can be updated in rapid response to new threats (zero day vulnerabilities)
- Does not change the real time operating system
- Does not change the configuration of commissioned devices
- Operates in time critical environments without adverse performance
- Can be maintained remotely and simply

We need a “critical-pass filter”!

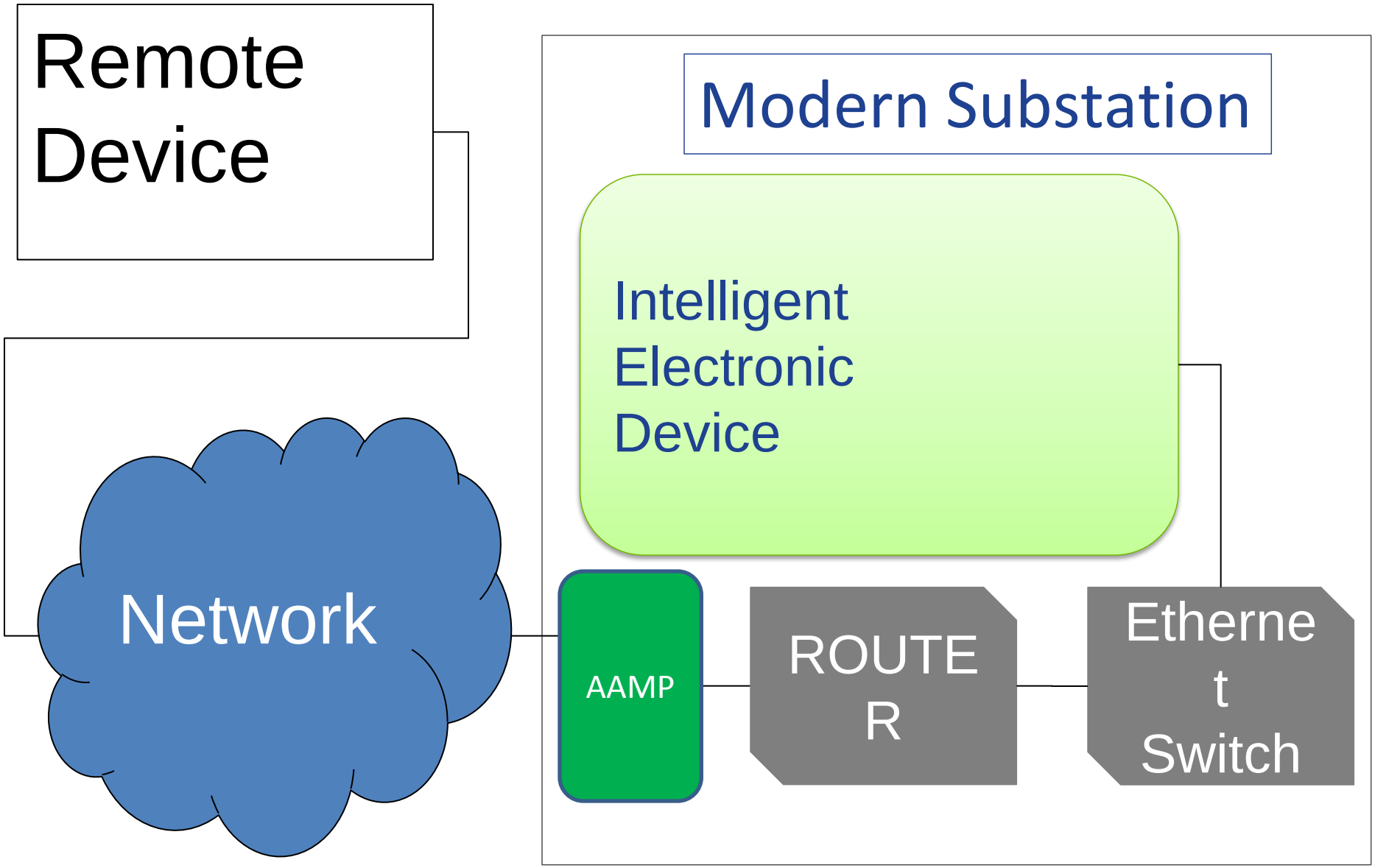


Vulnerabilities and Exploits

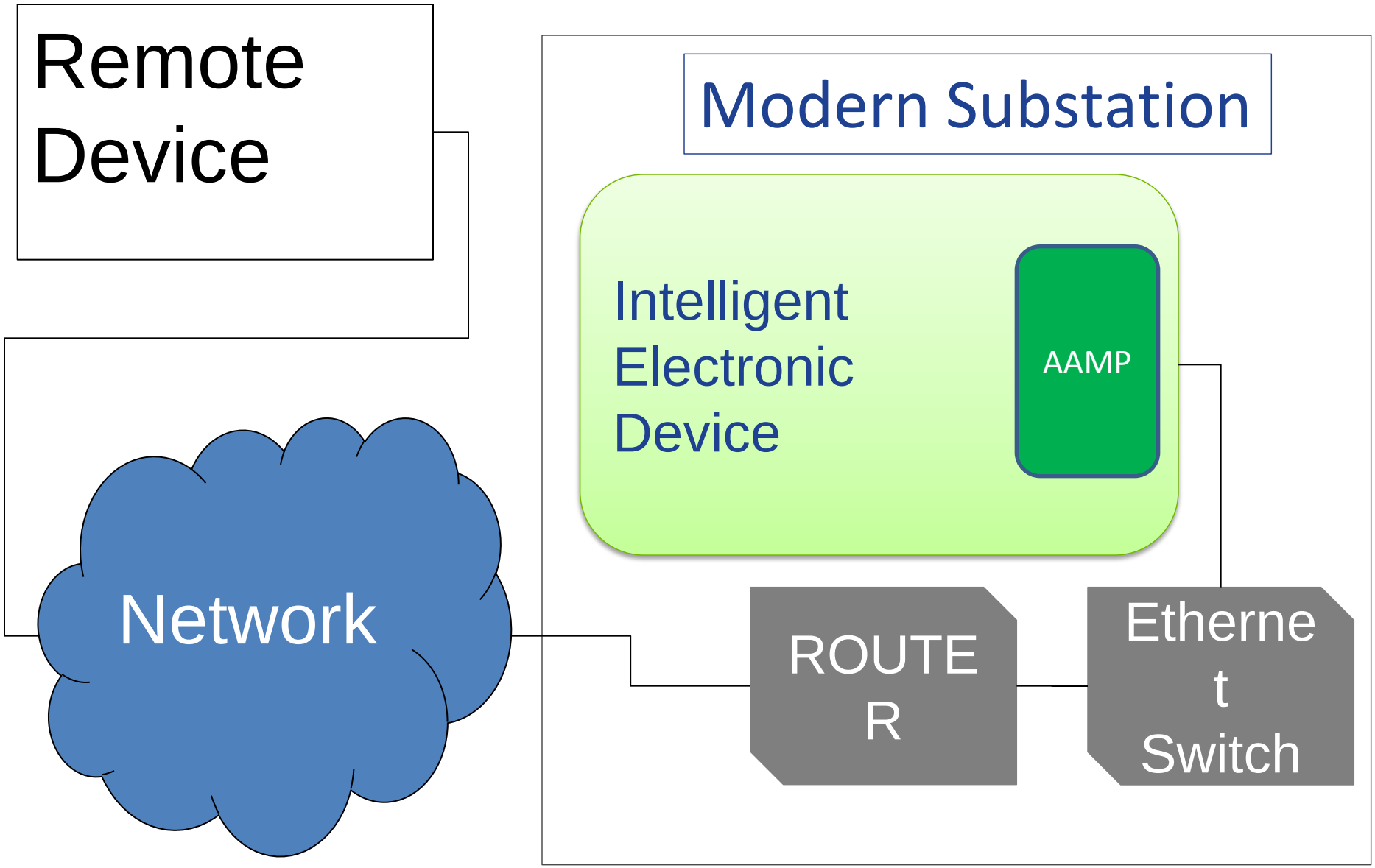


IED

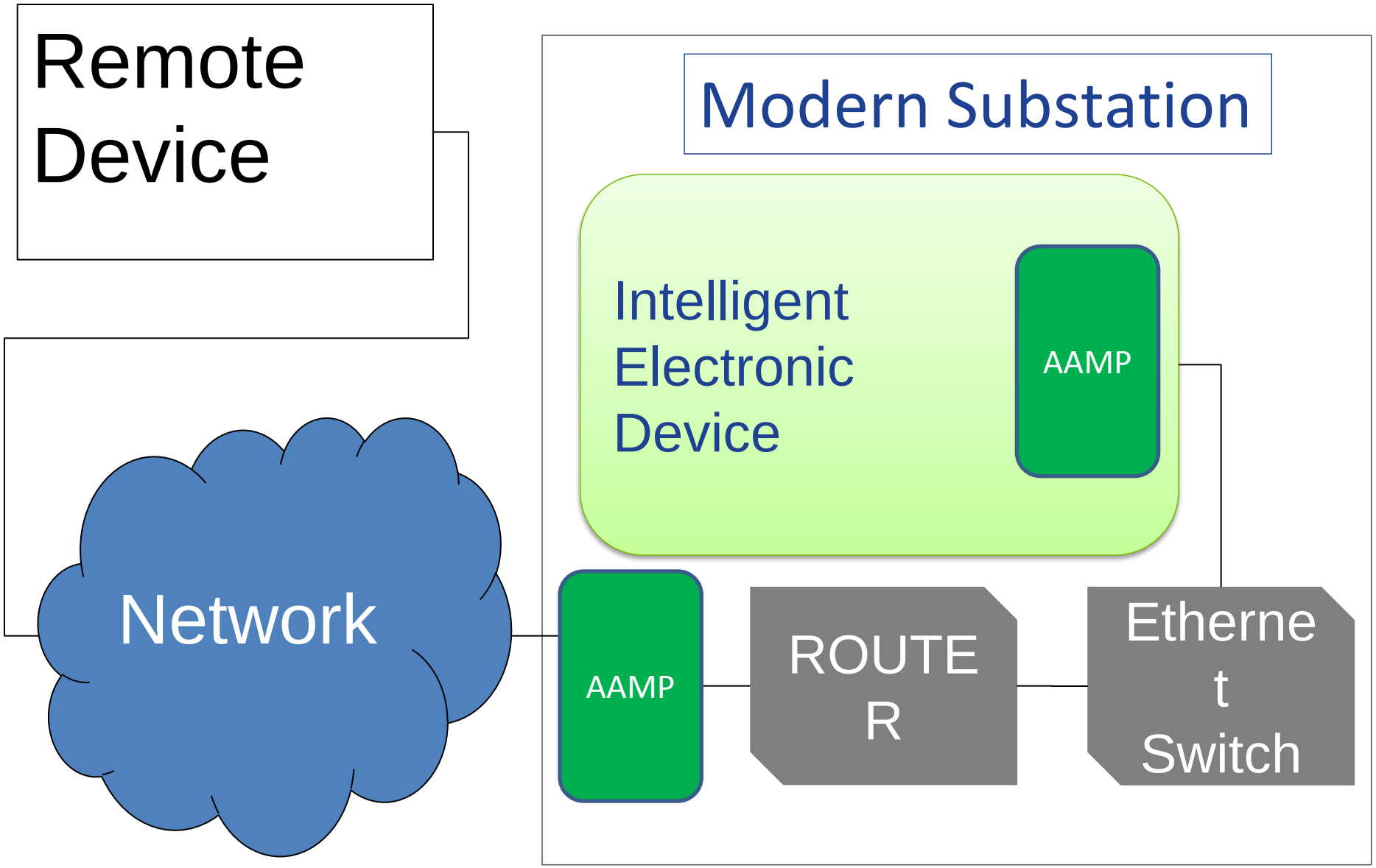
Simple Architecture



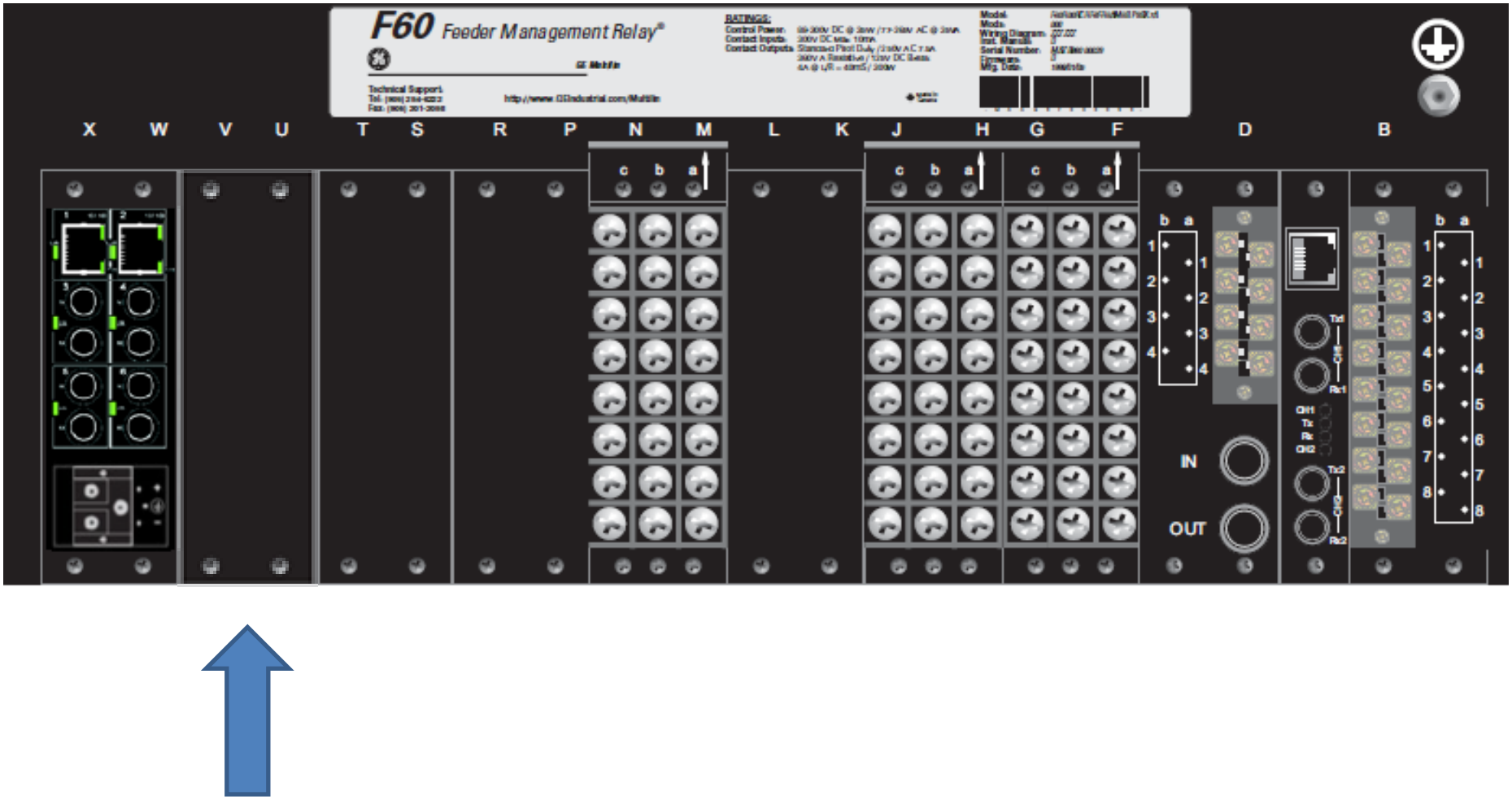
Simple Architecture



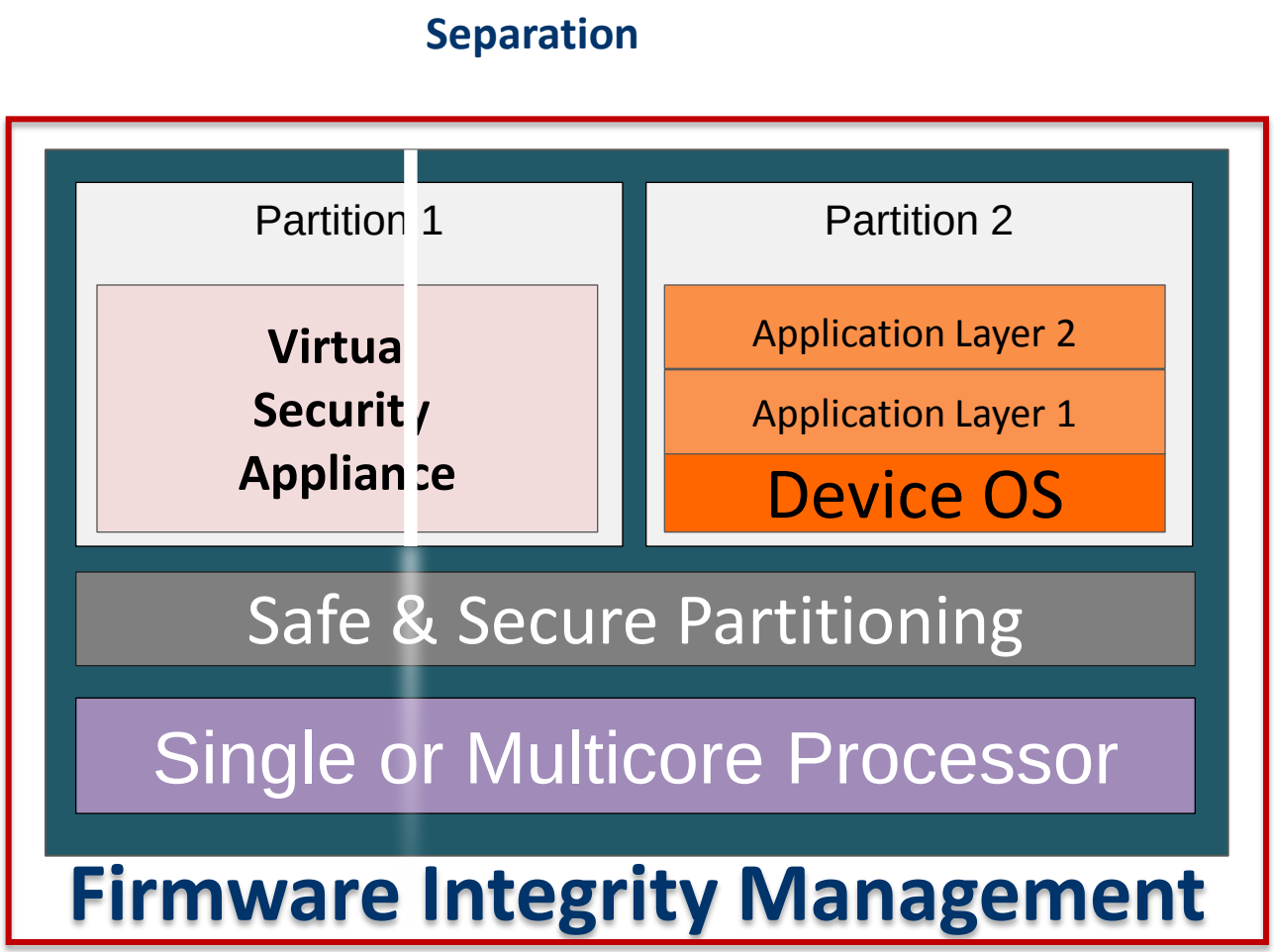
Simple Architecture



AAMP Module

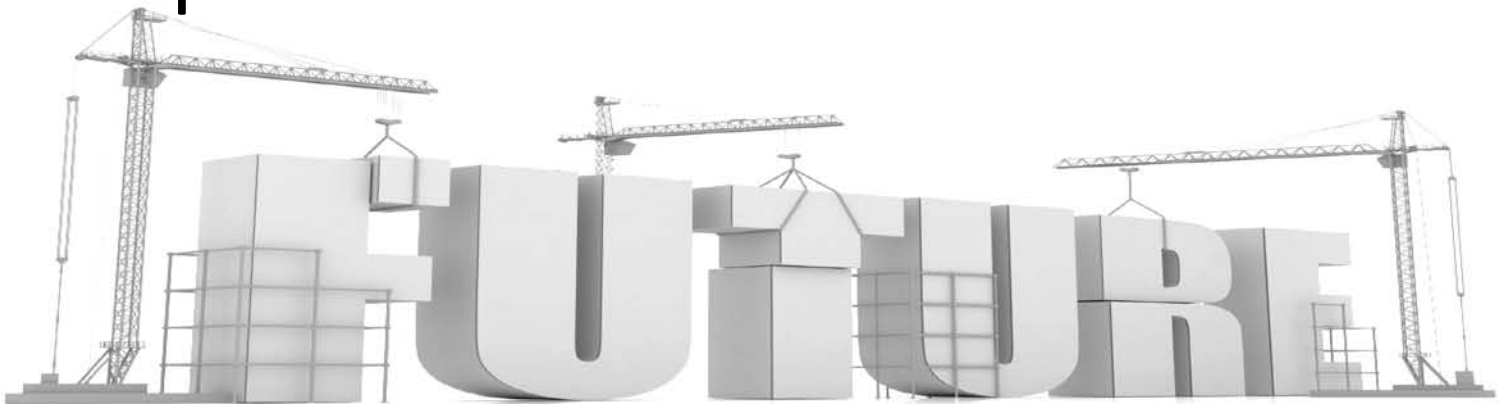

F60 Feeder Management Relay®
X W V U T S R P N M L K J H G F D B
c b a
IN
OUT

Drive Down Costs: Embedded Firmware AAMP



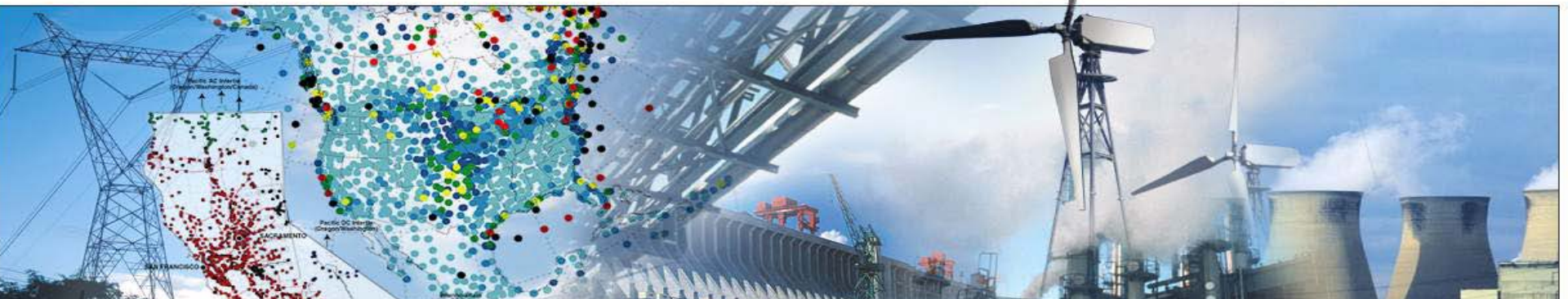
Adaptive Anti-Malware Protection (AAMP)

- Adds a layer of protection to industrial protocols and applications
- Utilizes Vulnerability Signatures (not exploit based!)
- Implements the Critical Pass Filter
- Performs Deep packet inspection
- Adapts to YOUR Devices



How does AAMP meet the need?

- Provides Security to chosen devices
- Can be updated in rapid response to new threats (zero day vulnerabilities)
- Does not change the real time operating system
- Does not change the configuration of commissioned devices
- Operates in time critical environments without adverse performance
- Can be maintained remotely and simply



Summary

- Cyber Security Enables Progress
- Traditional Methods for managing the dynamic world of cyber security do not fit utility requirements
- Adaptive Anti-Malware Protection technology solves the key requirements for security solutions

Thank You!

Eric MacDonald, GE Digital Energy, eric.macdonald@ge.com
Mike Ahmadi, Wurldtech, mahmadi@wurldtech.com
Nate Kube, Wurldtech, nkube@wurldtech.com
Alexander Damish, Wind River, alexander.damisch@windriver.com
Daniel Thanos, GE Digital Energy, daniel.thanos@ge.com

imagination at work

wurldtech

WIND RIVER