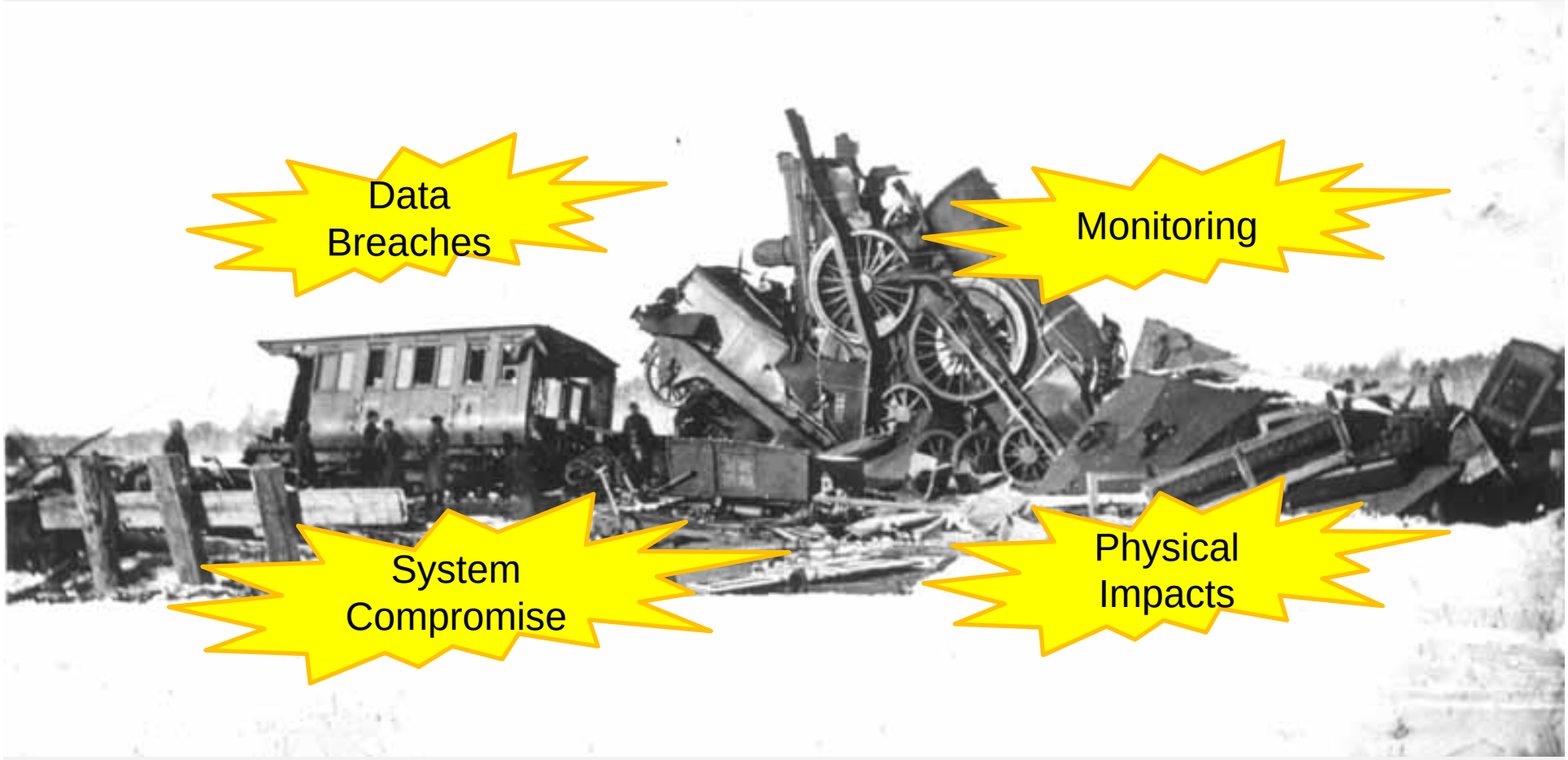
Trusted Computing Group: Where Trust Begins

Today's Agenda

1:30 – 2:00	Welcome and Introduction to Trusted Computing Group	Steve Hanna Infineon Technologies
2:00 – 2:25	Trust in the Cloud	Michael Donovan Hewlett-Packard
2:25 – 2:55	Break: Demonstration Showcase	
2:55 – 3:20	Trusted Network Connect (TNC) and Security Automation	Lisa Lorenzin Juniper Networks
3:20 – 3:45	Industrial Control Systems Security	Ludwin Fuchs Asguard Networks
3:45 – 4:10	Trusted Platform Modules (TPMs) as Virtual Smart Cards	John Fitzgerald Wave Systems
4:10 – 4:30	Closing Remarks: Demonstration Showcase	

Today's Cybersecurity Train Wreck



Source: Historical photograph, Lagerlunda Railway Accident, 1875.

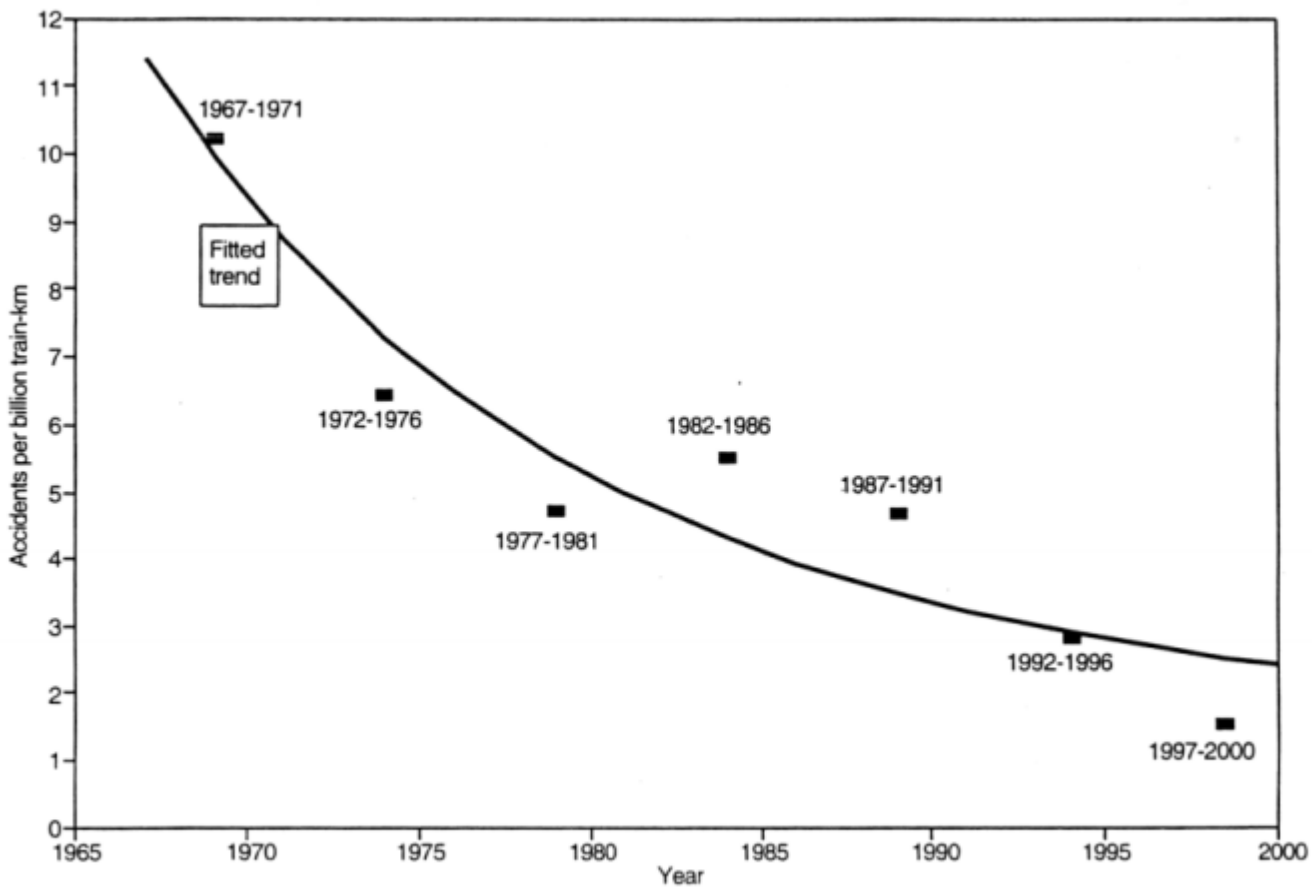
Untrusted Systems

Source: S E C Railway Narrow Gauge Museum of Nagpur

Trusted Systems

Source: Bruce Fingerhood
License: CC BY 2.0
Link: http://www.flickr.com/photos/springfieldhomer

Benefits of Trusted Systems



Source: Evans, A. W. (2003), Estimating Transport Fatality Risk from Past Accident Data, Accident Analysis and Prevention, Vol. 35, Issue 4.

What is Trust?

Source: pixabay.com
License: CC0 Public Domain
Link: http://www.pixabay.com

Trust is…

the belief that a person or system will behave predictably, even under stress

based on experience and/or evidence

based on fundamental properties (identity, integrity)

easy to lose and hard to regain

What is a Trusted System?

A trusted system is…

predictable, even under stress

trusted based on experience and/or evidence

based on fundamental properties (identity, integrity)

Building Trusted Systems

1. **Build a Hardware Root of Trust into each device**

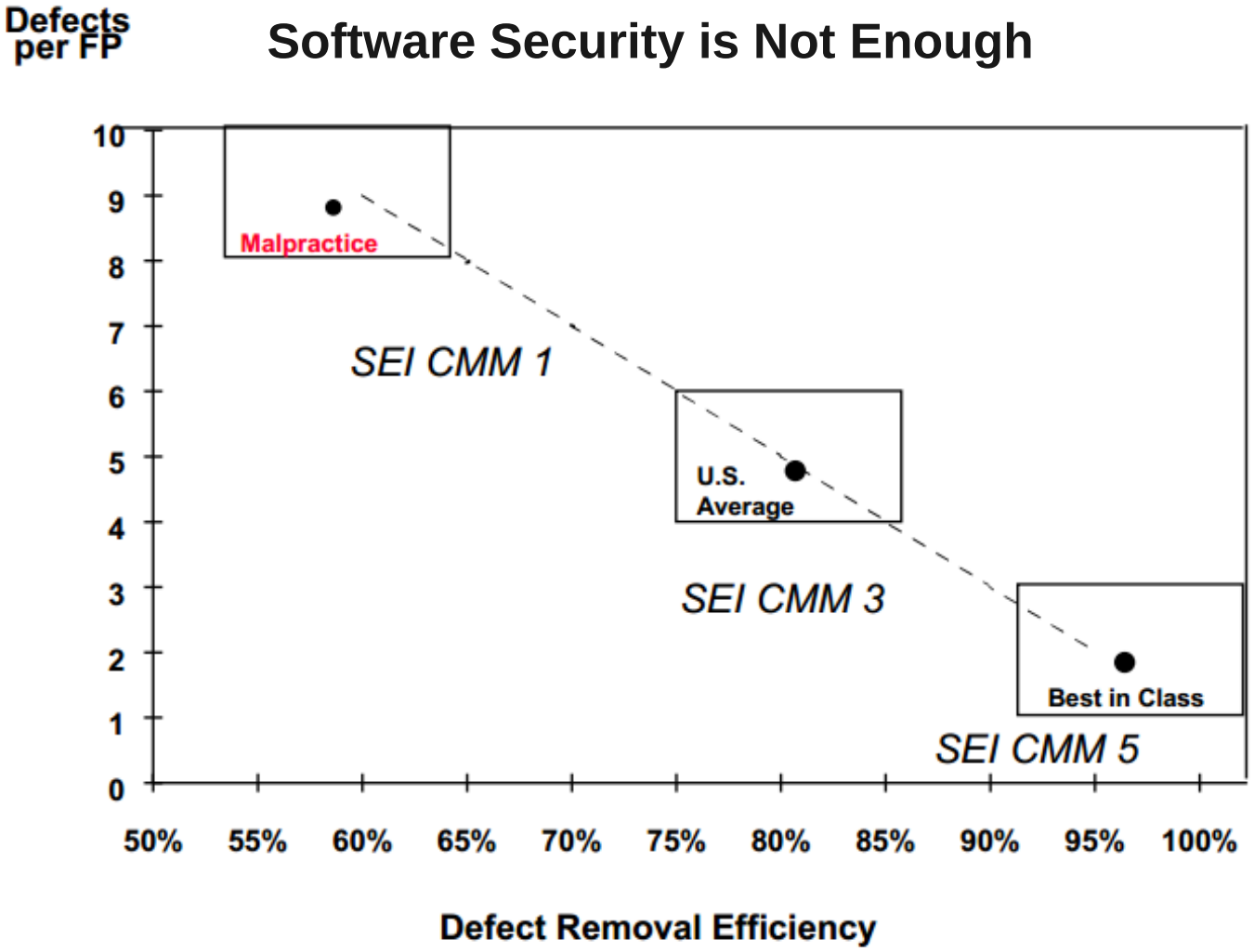
What is a Hardware Root of Trust?

- **Hardware Security**
  - Trusted Platform Module (TPM)
- **Provides**
  - Foundation for Secure Software
- **Features**
  - Authentication
  - Encryption
  - Attestation

Identity

Integrity

Why Hardware?



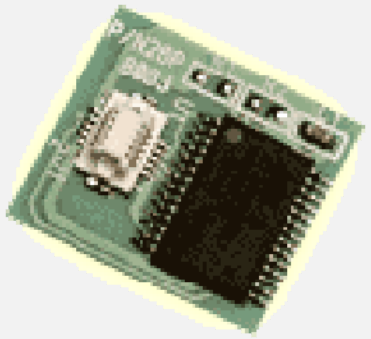
Graph used with permission of Capers Jones.

Building Trusted Systems

1. **Build a Hardware Root of Trust into each device**

2. **Employ Hardware Storage Encryption**

Hardware Storage Encryption



- **Hardware Security**
  - Self-Encrypting Drive (SED)
- **Provides**
  - Protection against Physical Attacks
  - Protection against Loss and Theft
  - Cryptographic Wipe
- **Features**
  - Encryption

Building Trusted Systems

1. **Build a Hardware Root of Trust into each device**
2. **Employ Hardware Storage Encryption**
3. **Add Security Automation**

Security Automation

- **Security Coordination Standards**
  - Connect Existing Systems
  - Enable New Capabilities
- **Provide**
  - Automation for All Phases of Cyber
    - Preparation
    - Detection
    - Analysis
    - Response

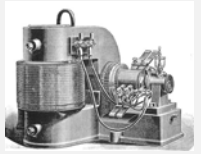
Building Trusted Systems

1. **Build a Hardware Root of Trust into each device**

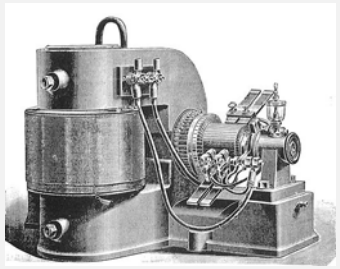
2. **Employ Hardware Storage Encryption**

3. **Add Security Automation**

4. **Protect Legacy Systems**



Protect Legacy Systems



- **Legacy Systems**
  - ICS/SCADA or Old Systems
  - Vulnerable to Disruption or Infection
  - Need Protection
- **Protection**
  - Place into Enclaves
  - Overlay Secure Communications
  - Restrict to Authorized Parties

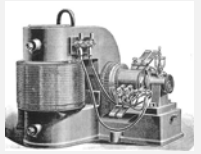
Building Trusted Systems

1. **Build a Hardware Root of Trust into each device**

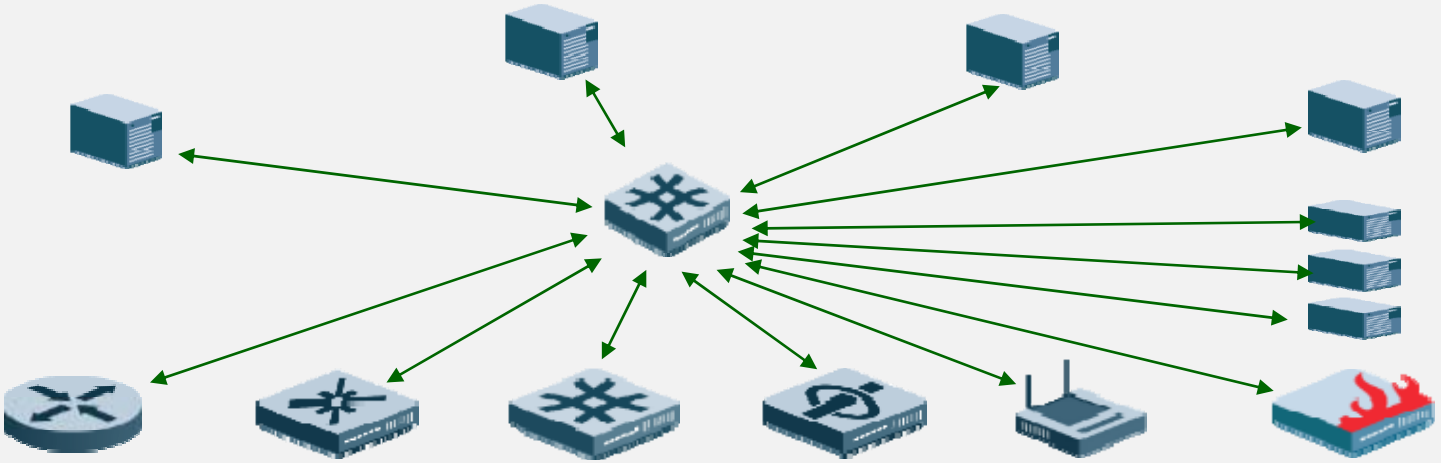
2. **Employ Hardware Storage Encryption**

3. **Add Security Automation**

4. **Protect Legacy Systems**



Why Open Standards?



Interoperability	Vendor Neutrality
Security	Certification
Lower Costs	Ubiquity

TCG = Open Standards for Trusted Computing

- **TCG is the only group focused on trusted computing standards**
- **TPM specification implemented in more than a billion devices**
  - Chips, PCs, servers, printers, kiosks, industrial systems, and many embedded systems
- **Trusted Computing is more than TPM**
  - Secure Storage
  - Security Automation
  - Secure Cloud
  - Secure Mobile Devices
  - Secure Legacy Devices

What Can I Do Now?

1. See What You Already Have

- Enterprise PCs and servers with TPMs
- Microsoft Windows with built-in TPM support
- Red Hat Enterprise Linux with built-in TPM support
- Self-Encrypting Drives widely available for little to no cost differential
- Network equipment supports TNC standards
- ICS/SCADA gateways support TCG's ICS standards

What Can I Do Now?

1. **See What You Already Have**
2. **Deploy It**
   - TPM as virtual smart card or for disk encryption
     - Huge cost savings, easier management, and better security
   - SEDs
     - Strong data protection, quick and secure drive re-use
     - Strict but easy compliance, “safe harbor” from data breach regulations
   - TNC
     - Secure wireless and wired networks
     - Ensure only healthy and approved devices are connecting
     - Also include security automation features

What Can I Do Now?

1. **See What You Already Have**
2. **Deploy It**
3. **Demand More**
   - Ask vendors for Trusted Computing support
   - Mention TCG standards in acquisition documents (RFPs, etc.)
   - Look for TCG certification

Questions?

Today's Agenda

1:30 – 2:00	Welcome and Introduction to Trusted Computing Group	Steve Hanna, Infineon Technologies
2:00 – 2:25	Trust in the Cloud	Michael Donovan, Hewlett-Packard
2:25 – 2:55	Break: Demonstration Showcase	
2:55 – 3:20	Trusted Network Connect (TNC) and Security Automation	Lisa Lorenzin, Juniper Networks
3:20 – 3:45	Industrial Control Systems Security	Ludwin Fuchs, Asguard Networks
3:45 – 4:10	Trusted Platform Modules (TPMs) as Virtual Smart Cards	John Fitzgerald, Wave Systems
4:10 – 4:30	Closing Remarks: Demonstration Showcase	