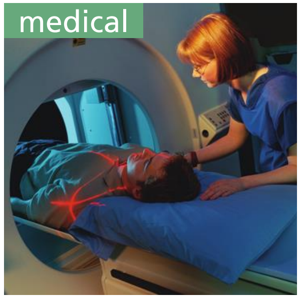
Making secure and reliable cars using Separation and Virtualization Technologies

Carmelo Loiacono - Field Application Engineer
carmelo@ghs.com



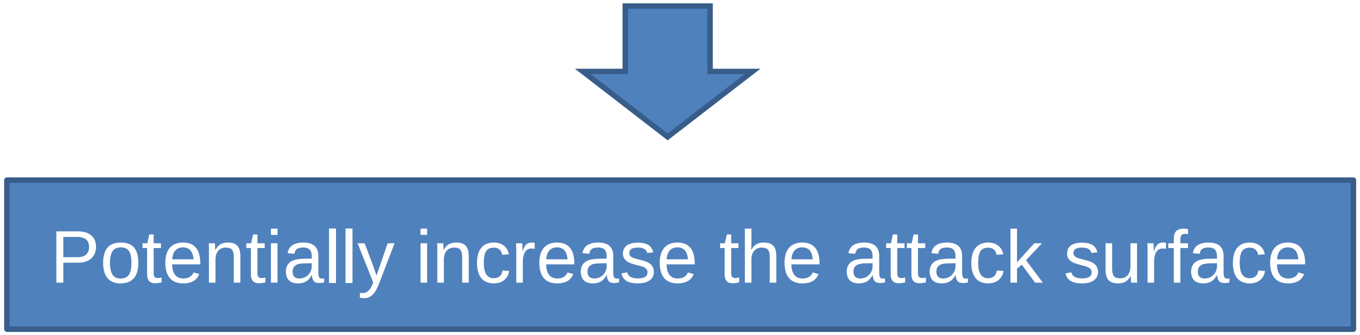
Agenda

- ❑ Motivations
- ❑ Separation
- ❑ Virtualization
- ❑ Advanced Applications
- ❑ Device Security Architectures

Motivations

❑ Automotive trends

- Bringing different electronic domains into single platform
- Increasing Vehicles Intelligence
- Vehicle internal networks are more and more connected to external devices

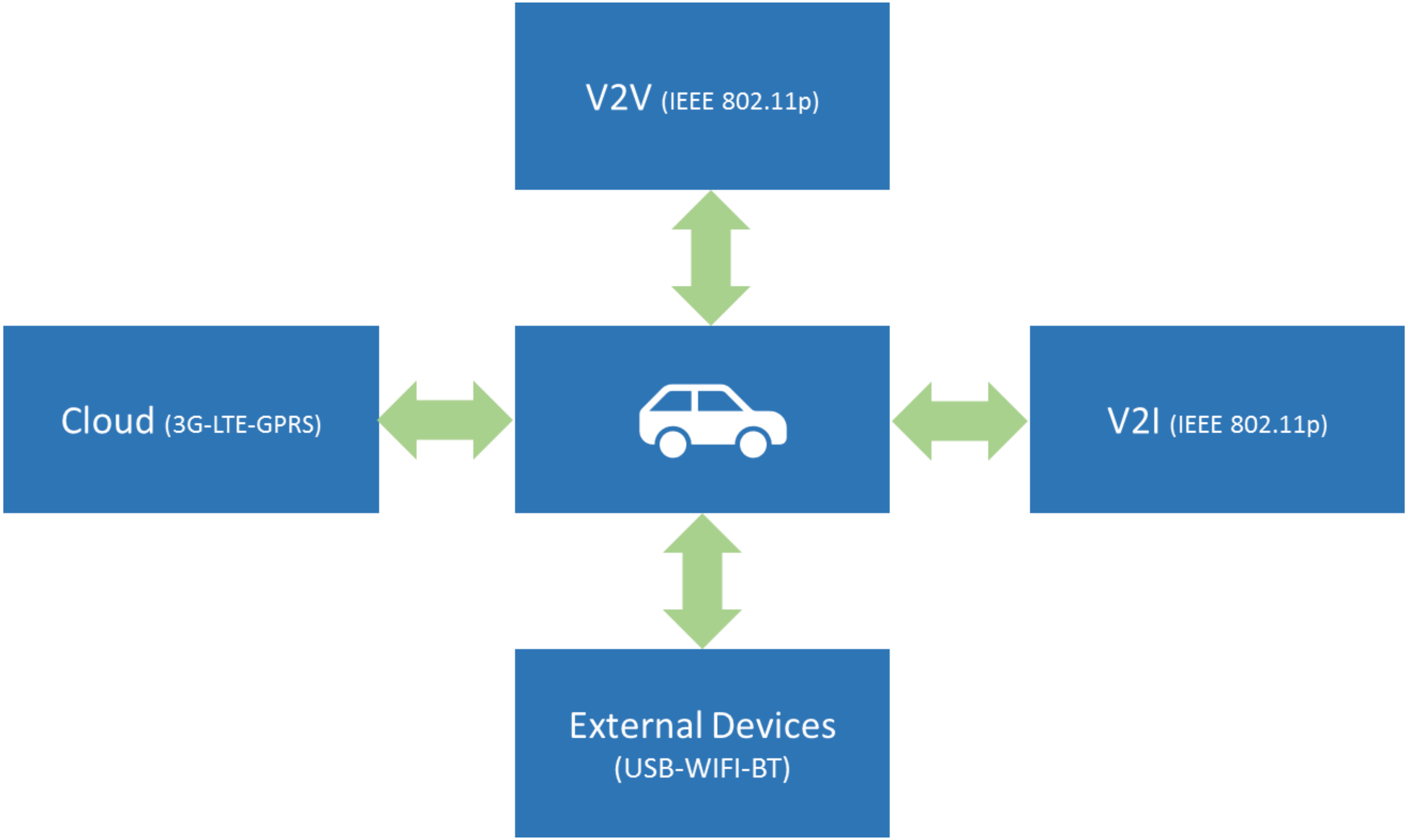


Potentially increase the attack surface

How Vulnerabilities Happen

- Architecture
  - Security not built-in from the ground up
  - Companies combine security-critical/non-security-critical applications and code
- Poor Coding
  - Programming errors (i.e. buffer overflows)
- Trade-offs
  - Cost (i.e. MMU vs. non-MMU processors)
  - Time-to-market
  - Features
  - Convenience

Automotive Connectivity



V2V (IEEE 802.11p)

Cloud (3G-LTE-GPRS)

V2I (IEEE 802.11p)

External Devices (USB-WIFI-BT)

Separation is Fundamental

- Security and Safety Architecture
  - Identify critical components in the system
  - Separate those components from untrusted code
  - Enforce strict access control

- Enables complex systems with high security and safety

Secure Separation

- Separation architecture for instrument clusters
  - Consolidation
  - Safely run HMI and safety-critical tasks on the same processor
  - Achieve real-time goals
  - Guarantee resources

Secure, Safe and Scalable Instrument Clusters

Separation Benefits

- No recompile needed for components not changed
  - Only re-link the changed parts to existing components
  - No API changes that effects application code
- Separation architecture yields independence between components
  - No need to rerun unit tests on unchanged components
  - Simply test changed/added functionality on relevant components prior to integration tests
  - Only need to rerun your integration tests, not the full test suite

INTEGRITY: a Secure and Safe RTOS

- Securely separate applications to allow mixed safety and security levels on the same processor
  - Including guest OS if needed -> **Virtualization**
- Isolate and protect sensitive data
- Secure the vehicle bus from interference from ‘outside’
- Be Ultra Reliable and deterministic
- Be designed from day 1 to be Safe, Secure and Deterministic

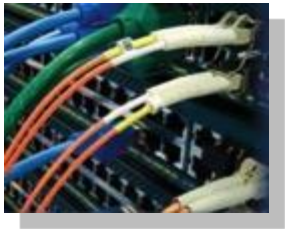
INTEGRITY Real-Time Operating System

- ❑ Unique real-time operating system architecture
  - ▪ Separation kernel architecture
  - ▪ Partition scheduling / resource guarantees
  - ▪ Advanced multicore/multiprocessor support
    - Single Core, AMP, SMP
  - ▪ Safely consolidate software on same processor

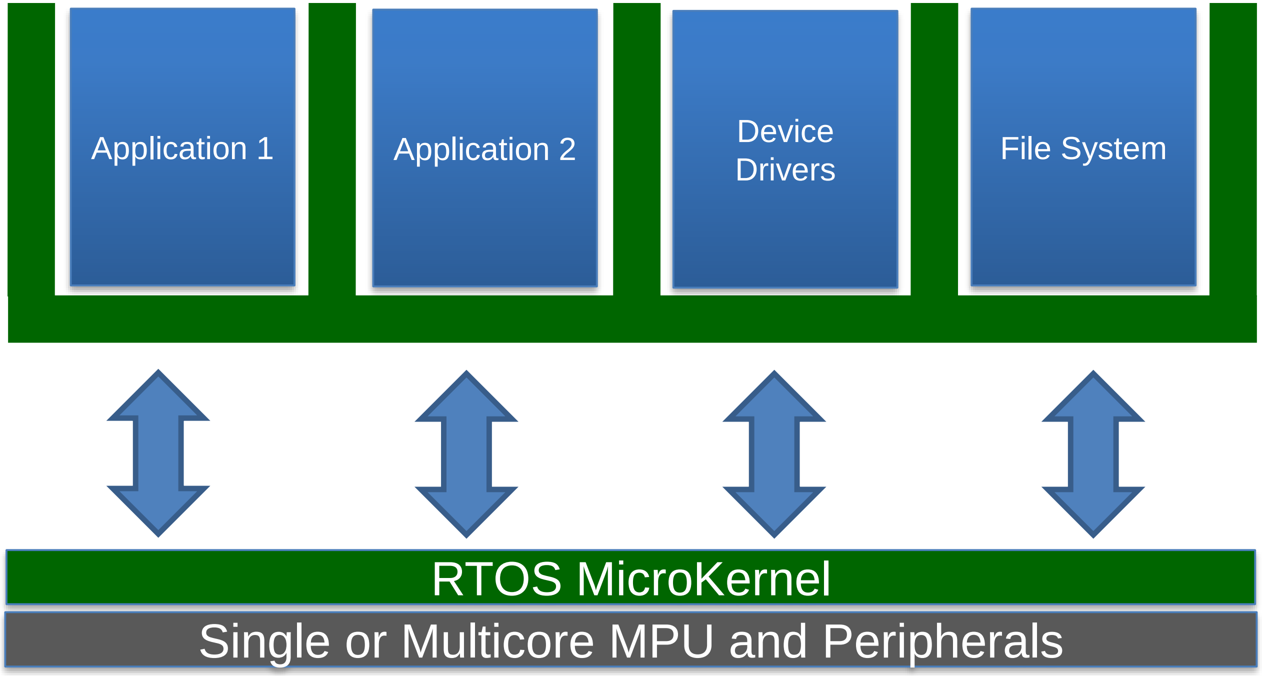
- ❑ The most highly certified RTOS in the embedded market segments
  - ▪ EAL 6+, highest software security certification in world
  - ▪ IEC 61508 SIL3 for industrial
  - ▪ CENELEC EN 50128 SW/SIL4 for railway
  - ▪ ISO 26262 ASIL for automotive
  - ▪ DO-178B Level A for avionics
  - ▪ FDA Class II, III approvals for medical

- ❑ Extensive middleware and ecosystem
  - ▪ Networking, routing, graphics and much more

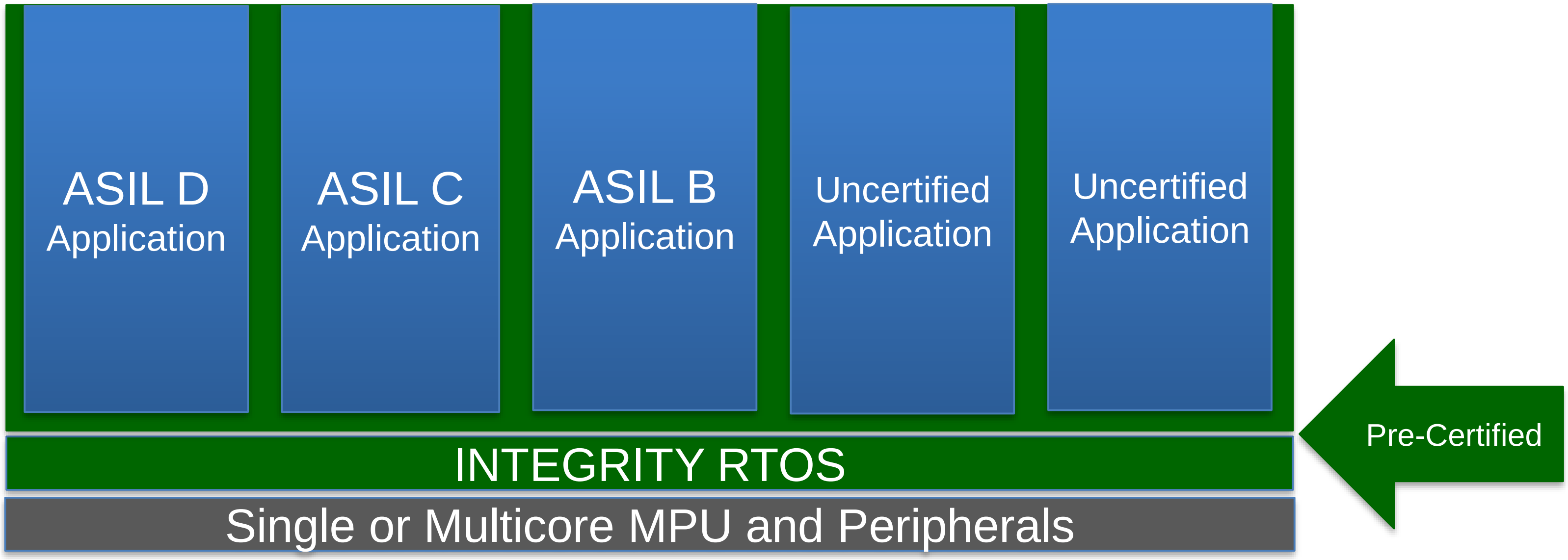
- ❑ Open platform support
  - ▪ POSIX, ARINC 653, OpenGLES, upgradeable and flexible



Separation Architecture



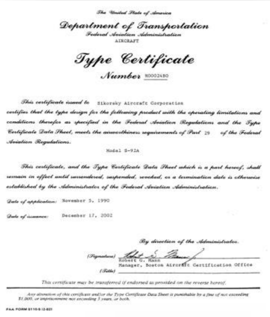
ECU Consolidation - Separation Architecture



Each Application Certified to its individual ASIL level
Reduced Development Costs
Reduced Certification Costs

Independent Expert Validation

Certifying Authority	Level Achived	Applicability	Industry
FAA/EASA (INTEGRITY-178B)	DO-178B Level A	Reliability, Safety	Avionics
NSA	EAL6+ High Robustness / Type 1	Security	Defense
NIST	FIPS 140-2, level 1	Security	All
DIA	TSABI PL-4	Security	Enterprise/IT
FDA	Class II, III	Reliability, Safety	Medical
TUV Nord, exida	IEC 61508:2010 SIL 4	Safety	Industrial Automation
TUV Nord, exida	EN 50128: 2011 SIL 4	Safety	Rail, Transportation
TUV Nord, exida	ISO 26262:2010 ASIL D	Safety	Automotive
Transdyne Corp.	SEI/CMMI Certified	Quality	All
IEEE and the Open Group	1003.1 IEEE POSIX Certified	Open, Interoperable	All



The United State of America

Department of Transportation

Federal Aviation Administration

AIRCRAFT

Type Certificate

Number H00024BO

This certificate issued to Sikorsky Aircraft Corporation certifies that the type design for the following product with the operating limitations and conditions therefor as specified in the Federal Aviation Regulations and the Type Certificate Data Sheet, meets the airworthiness requirements of Part 29 of the Federal Aviation Regulations.

Model S-92A

This certificate, and the Type Certificate Data Sheet which is a part hereof, shall remain in effect until surrendered, suspended, revoked, or a termination date is otherwise established by the Administrator of the Federal Aviation Administration.

Date of application: November 5, 1990

Date of issuance: December 17, 2002

By direction of the Administrator.

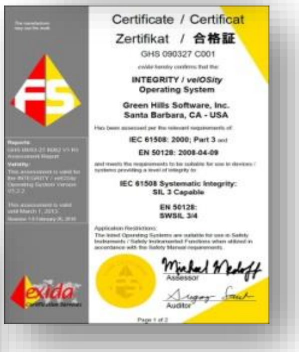
(Signature) Robert G. Mann

(Title) Manager, Boston Aircraft Certification Office

This certificate may be transferred if endorsed as provided on the reverse hereof.

Any alteration of this certificate and/or the Type Certificate Data Sheet is punishable by a fine of not exceeding $1,000, or imprisonment not exceeding 3 years, or both.

FAA FORM 8110-9 (2-82)



Certificate / Certificat

Zertifikat / 合格証

GHS 090327 C001

exida hereby confirms that the:

INTEGRITY / velOSity Operating System

Green Hills Software, Inc.
Santa Barbara, CA - USA

Has been assessed per the relevant requirements of:

IEC 61508: 2000; Part 3 and

EN 50128: 2008-04-09

and meets the requirements to be suitable for use in devices / systems providing a level of integrity to:

IEC 61508 Systematic Integrity: SIL 3 Capable

EN 50128: SWSIL 3/4

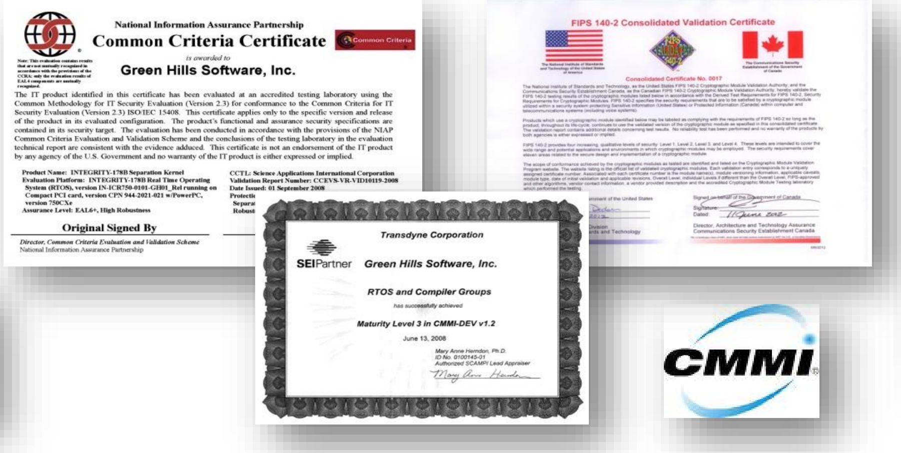
Application Restrictions:
The listed Operating Systems are suitable for use in Safety Instruments / Safety Instrumented Functions when utilized in accordance with the Safety Manual requirements.

Michael Medoff
Assessor

Auditor

Page 1 of 2

exida certification services



National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Green Hills Software, Inc.

Note: This evaluation contains results that are not mutually recognized in accordance with the provisions of the CCRA: only the evaluation results of EAL4 components are mutually recognized.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3) ISO/IEC 15408. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL6+, High Robustness

CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10119-2008
Date Issued: 01 September 2008
Protectio
Separat
Robust

Original Signed By

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0017

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

...rnment of the United States

Division
...rds and Technology

Signed on behalf of the Government of Canada
Signature:
Dated: 11 June 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

Transdyne Corporation

SEIPartner

Green Hills Software, Inc.

RTOS and Compiler Groups

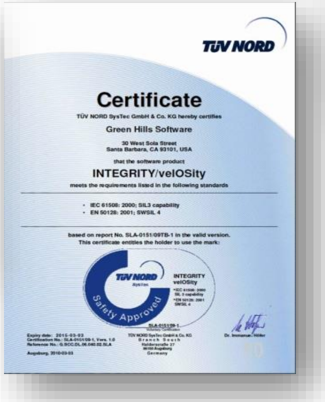
has successfully achieved

Maturity Level 3 in CMMI-DEV v1.2

June 13, 2008

Mary Anne Herndon, Ph.D.
ID No. 0100145-01
Authorized SCAMPI Lead Appraiser

Mary Ann Herndon



TÜV NORD

Certificate

TÜV NORD SysTec GmbH & Co. KG hereby certifies

Green Hills Software

30 West Sola Street
Santa Barbara, CA 93101, USA

that the software product

INTEGRITY/velOSity

meets the requirements listed in the following standards

- IEC 61508: 2000; SIL3 capability
- EN 50128: 2001; SWSIL 4

based on report No. SLA-0151/09TB-1 in the valid version.
This certificate entitles the holder to use the mark:

TÜV NORD SysTec Safety Approved

INTEGRITY
velOSity
•IEC 61508: 2000 SIL 3 capability
•EN 50128: 2001 SWSIL 4

SLA-0151/09-1
Voluntary Certification

Expiry date: 2015-03-02
Certification No.: SLA-0151/09-1, Vers. 1.0
Reference No.: G.SCC.DL.06.040.02.SLA

Augsburg, 2010-03-03

TÜV NORD SysTec GmbH & Co. KG
Branch South
Halderstraße 27
86150 Augsburg
Germany

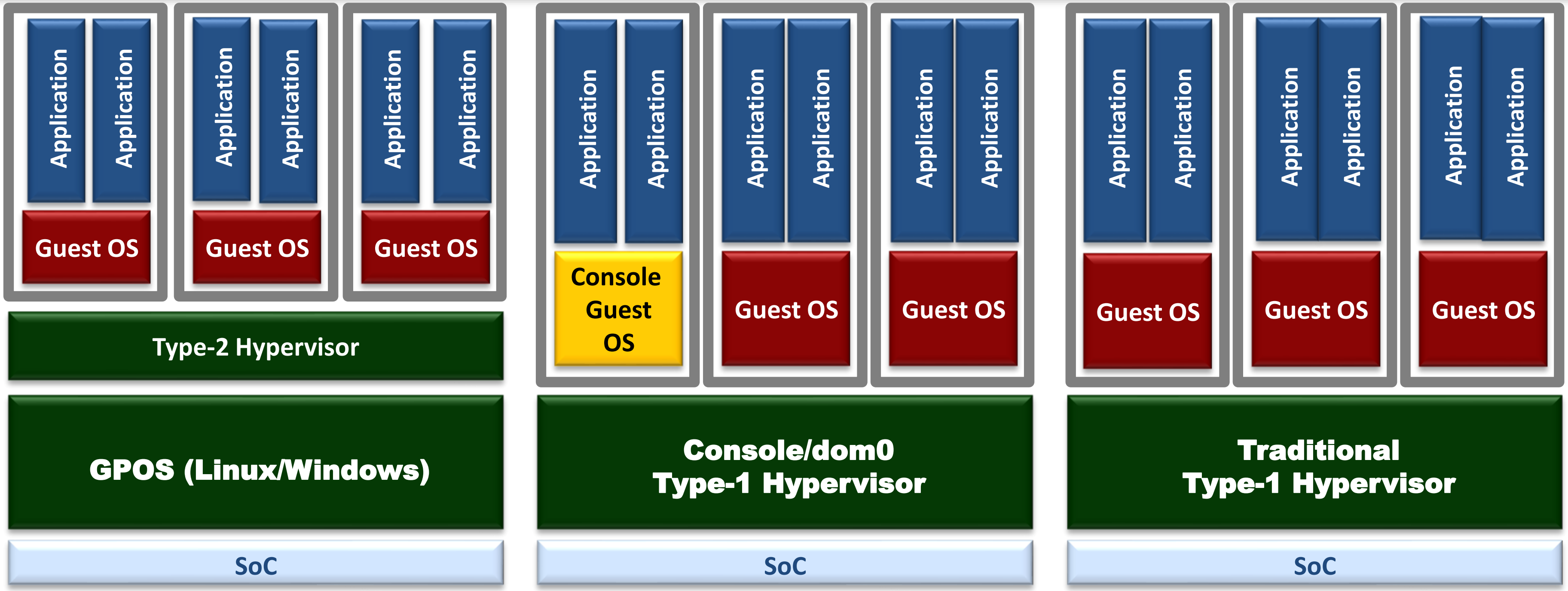
Dr. Immanuel Höfer

Virtualization

Commodity Operating Systems

- ❑ Embedded Linux OS (e.g. Yocto distribution)
  - ▪ provides an attractive set of ready-made software
  - ▪ consisting of millions of lines of code
  - ▪ will continue to contain security vulnerabilities and software bugs
- ❑ A powerful method for improving the security of a system having Linux as an Operating System
  - ▪ is to use an Hypervisor
    - to guarantee separation between the system software components

Architectural Comparison



- VMware Fusion/MVP
- Parallels
- Linux KVM
- ✓ GPOS limits security, performance, determinism

- Xen
- VLX-MH
- ✓ GPOS limits security, performance, determinism
- ✓ Large footprint

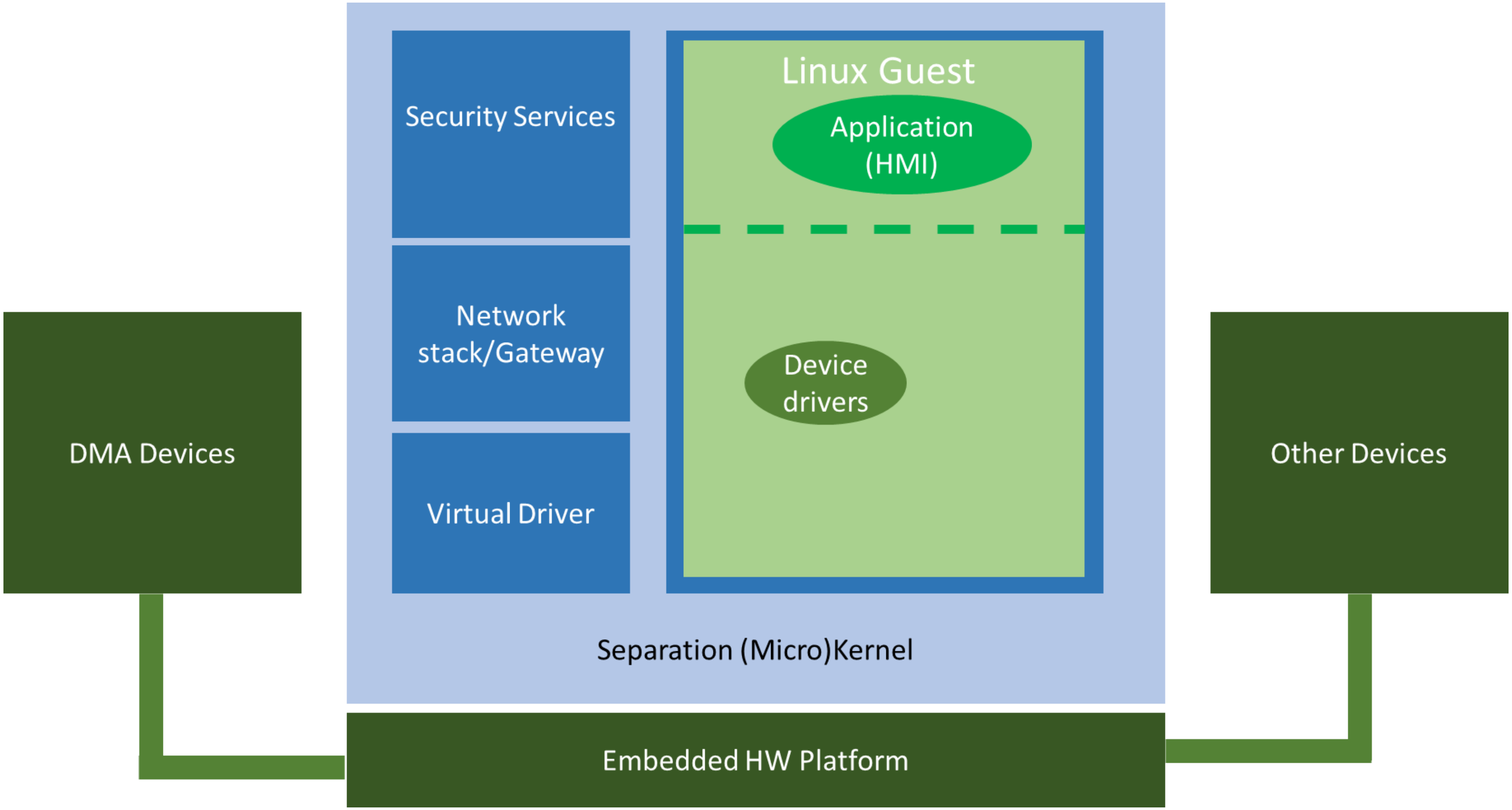
- VMware ESX
- OKL4
- ✓ Reinventing the wheel
- ✓ Lacks Real-time

INTEGRITY Multivisor
Microkernel Hosted Hypervisors

- What do hypervisors need to do?
  - Partition and protect memory resources
  - Secure access control for I/O and other system objects
  - Interprocess communication (IPC)
  - Schedule workloads securely and efficiently across cores
  - Power management
  - Device drivers
  - Handle disparate workloads – real-time and general purpose
  - Health monitoring / high availability

- This a subset of what a real-time microkernel already does extremely well
- Add System Virtualization as a *microkernel service*

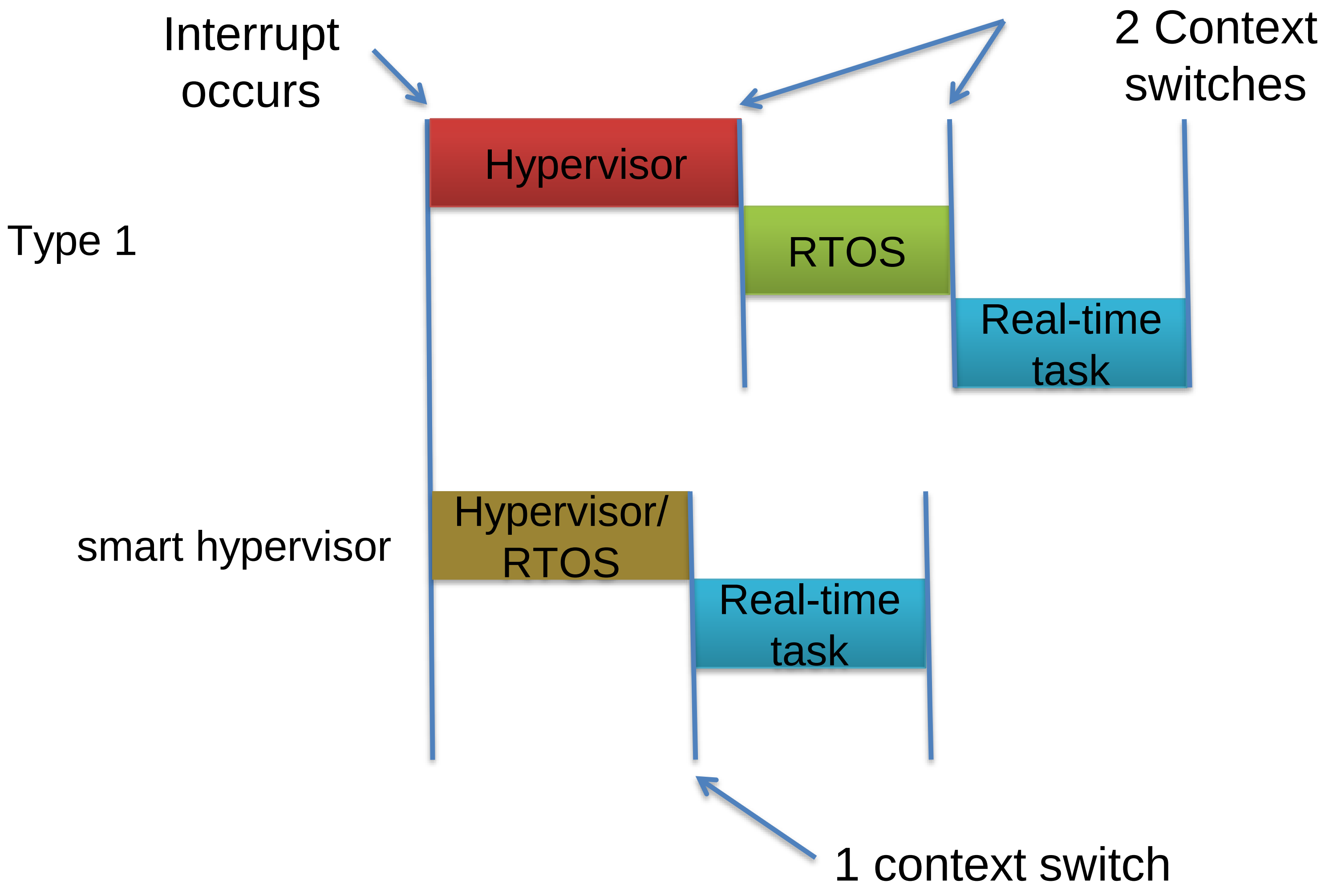
Microkernel Hosted Hypervisors - Architecture



I/O Device Security

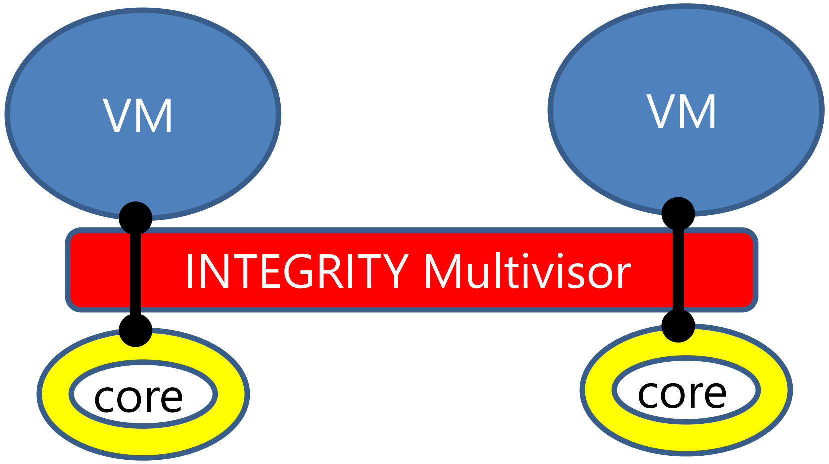
- ❑ Linux Guest connected device security
  - Especially for devices exploiting DMA
- ❑ I/O MMU (Second Stage MMU)
  - provides a programmatic interface to define which ranges of addresses the device can access
  - This allows device drivers to run purely in a Separation Kernel partition, or a Guest OS
  - taken as a compromise for the sake of either maintainability or time-to-market
- ❑ Virtual Drivers
  - devices managed by the Separation Kernel
  - flaw in a Guest OS device driver cannot
    - wrongfully program the DMA hardware
    - cause potentially fatal memory corruption

Hypervisor Type 1 vs smart hypervisor



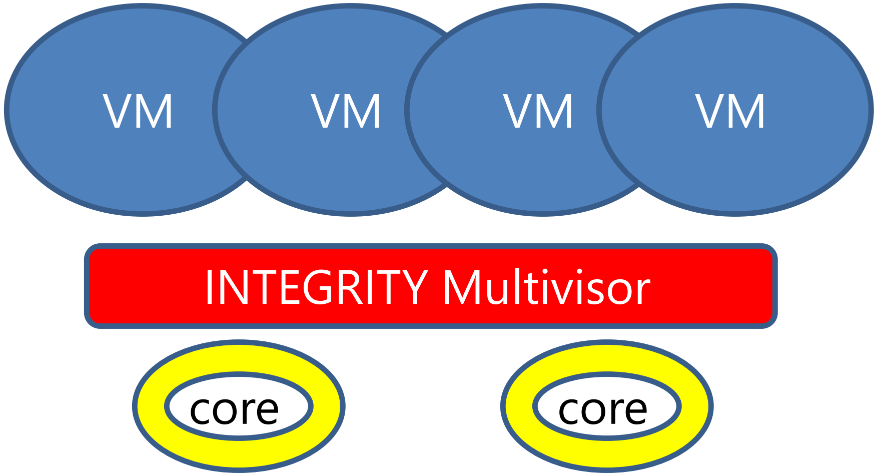
Multicore Approaches

- Static Partitioning
  - One VM per core
  - VMs are fixed to cores (no migration)
  - Simplest – no scheduling
  - Least flexible use of cores
  - Basically this is Asymmetric Multi Processing with memory protection



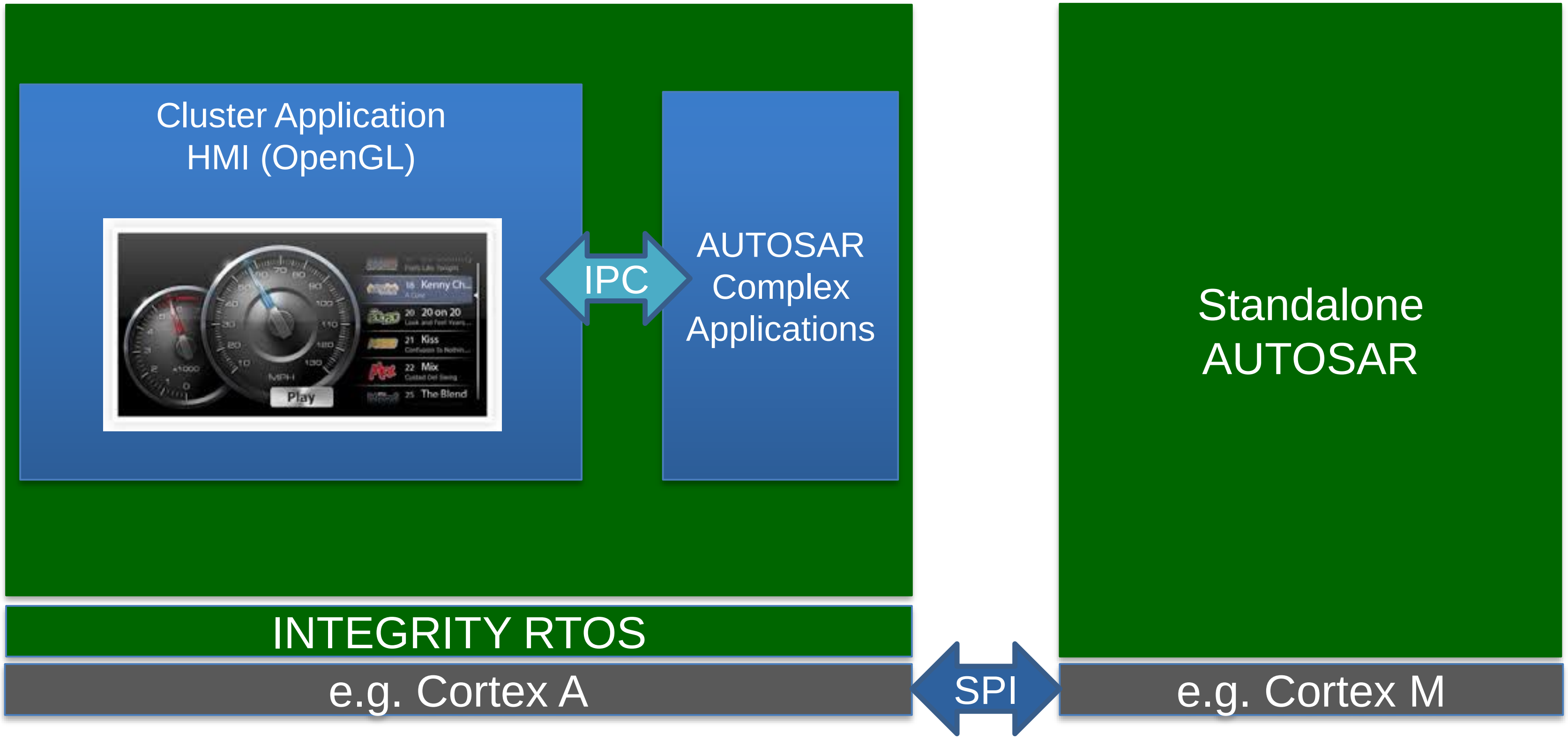
Multicore Approaches

- Dynamic Partitioning
  - Fully scheduled VMs (one or more VMs per core)
  - Power efficiency
    - Example: dual core, 2 VMs, each 50% loaded
      - Optimal: run both VMs on one core and turn the other core off
  - Well-suited to microkernel architecture
    - VMs and/or native processes are schedulable and migratable



Advanced Applications

Digital Cluster



Cluster Application
HMI (OpenGL)

IPC

AUTOSAR
Complex
Applications

Standalone
AUTOSAR

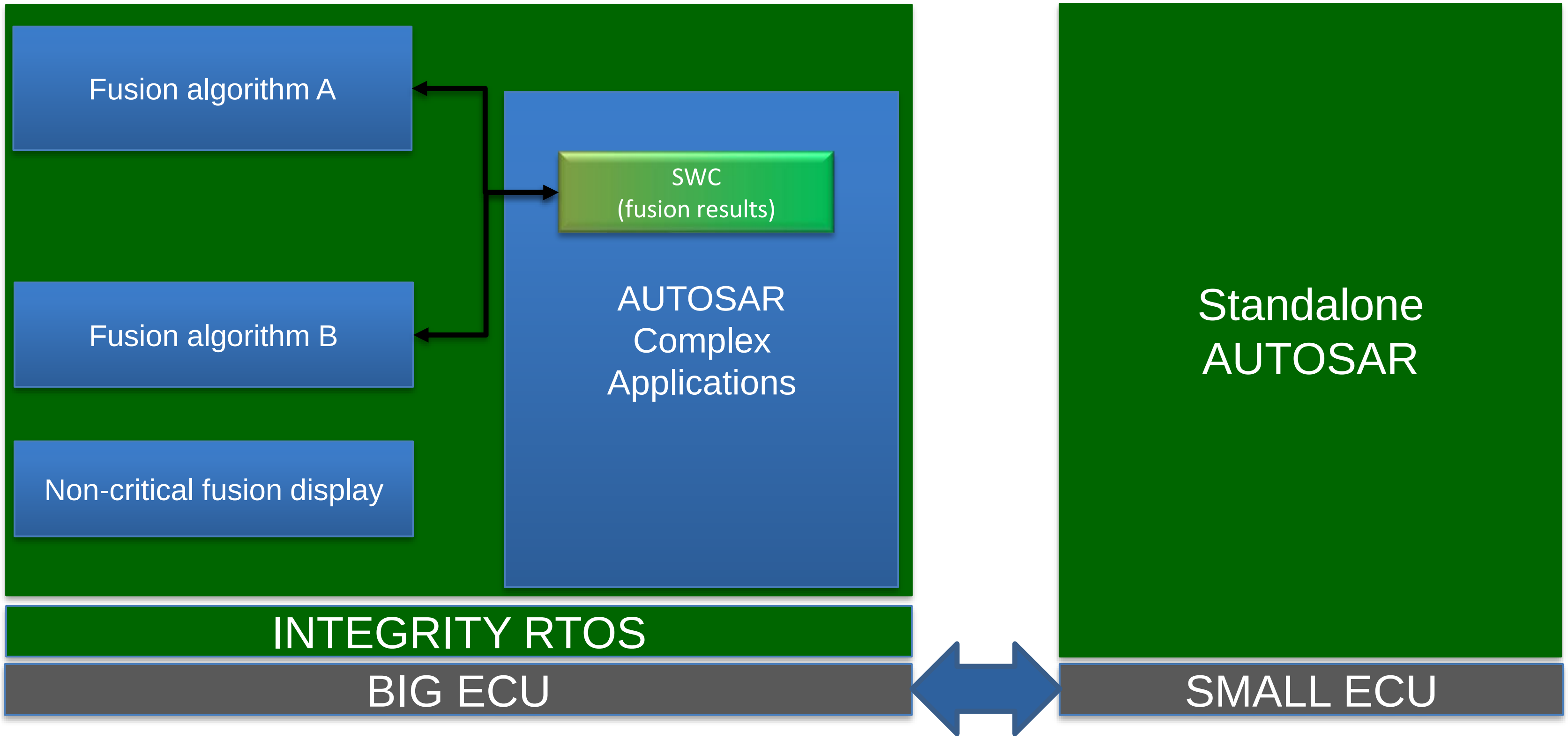
INTEGRITY RTOS

e.g. Cortex A

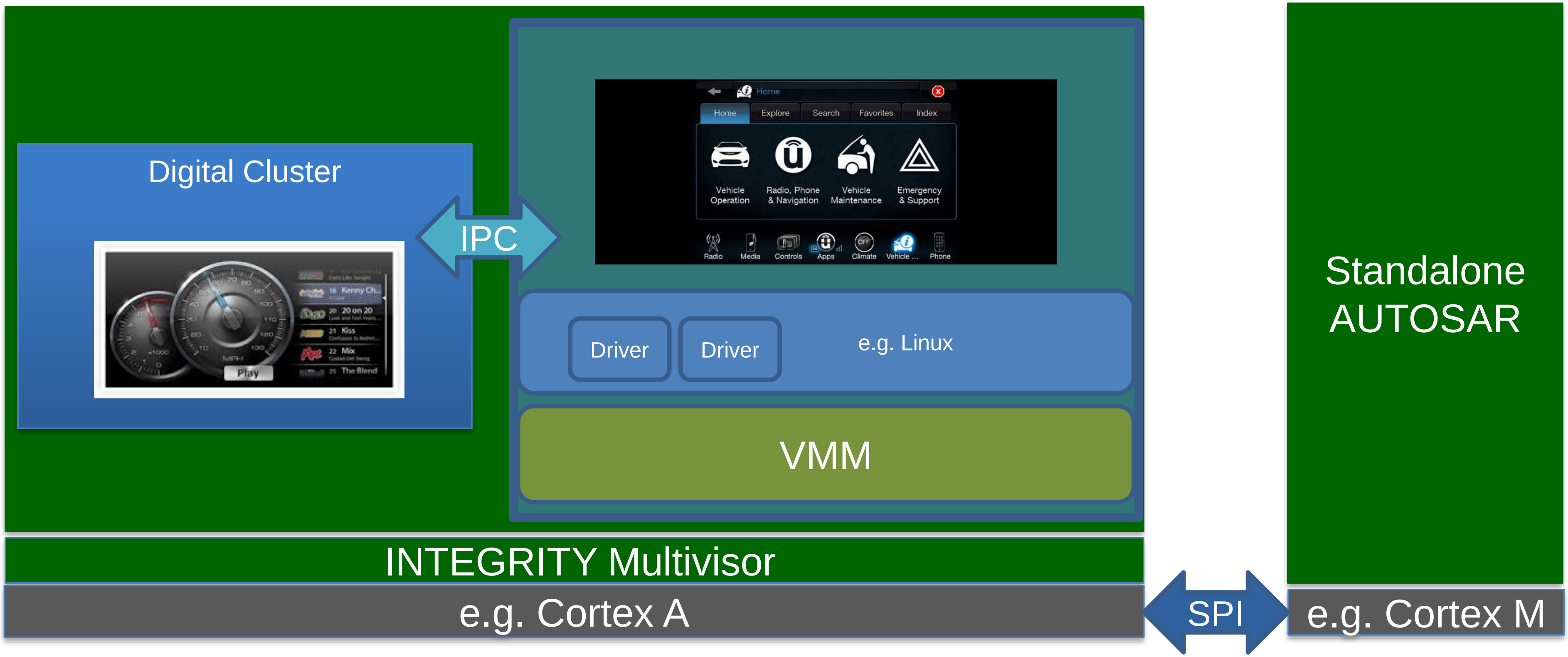
SPI

e.g. Cortex M

ADAS - Data Fusion



Digital Cluster + IVI



Digital Cluster

IPC

Driver

Driver

e.g. Linux

VMM

Standalone AUTOSAR

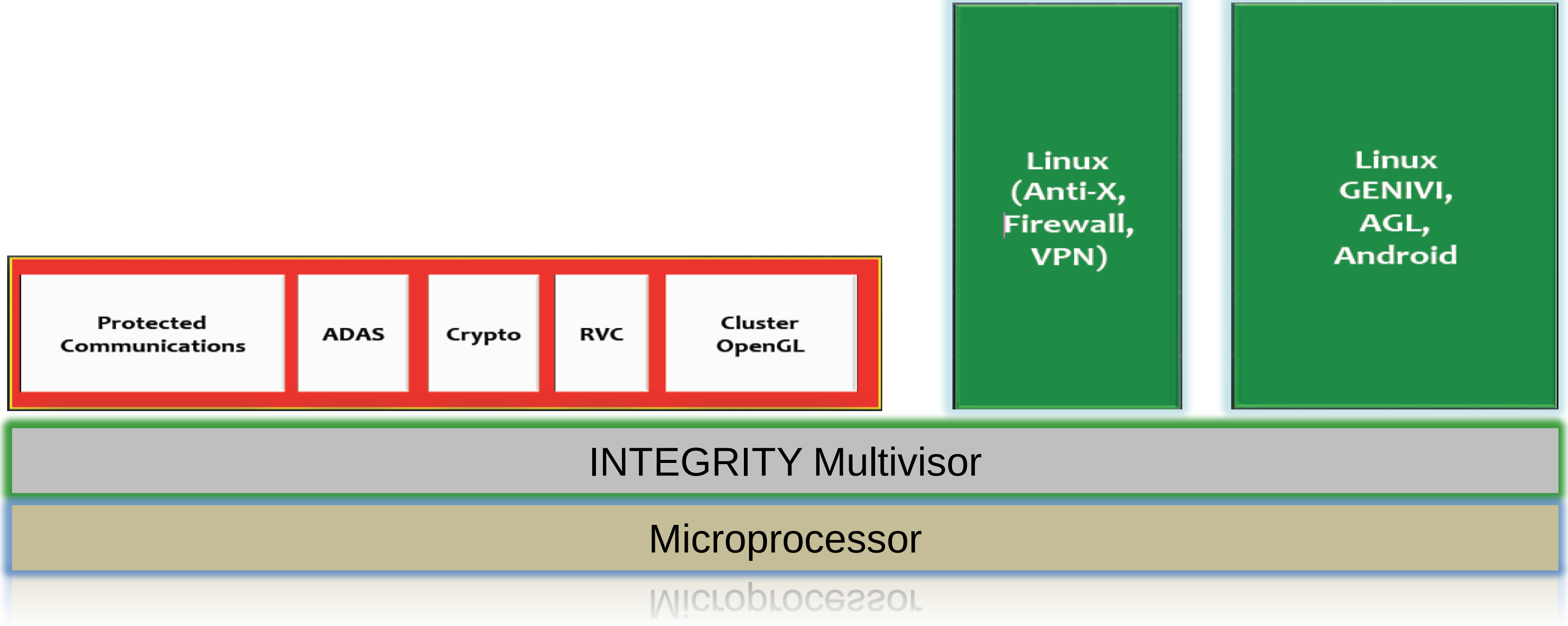
INTEGRITY Multivisor

e.g. Cortex A

SPI

e.g. Cortex M

Platform for ADAS
Advanced Driver Assistance Systems



Device Security Architecture

ISO 26262: Safety vs Security

Using ISO 26262 ≠ Security in your design

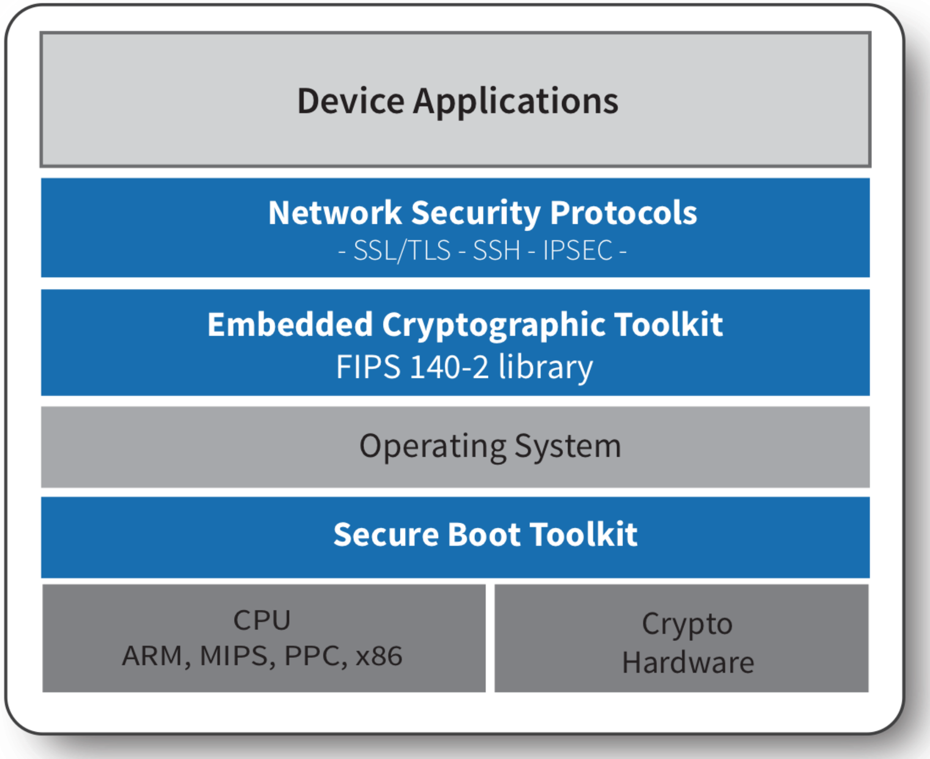
- If you design to ISO 26262, other considerations ***must*** be taken to achieve levels of system security
  - Secure Boot
  - Device Authentication
  - Software Authentication
  - FIPS 140-2 Cryptography
  - Use of products that adhere to and are certified to high Evaluation Assurance Levels (EAL) by BSI and/or Common Criteria
  - And more….

Purpose of Embedded Security Design

1. Protect data from unauthorized viewing
   - Data In Transit
   - Data In Storage
2. Protect operational reliability
   - Network Attacks
   - Physical Attacks
   - External Threats
   - Internal Threats

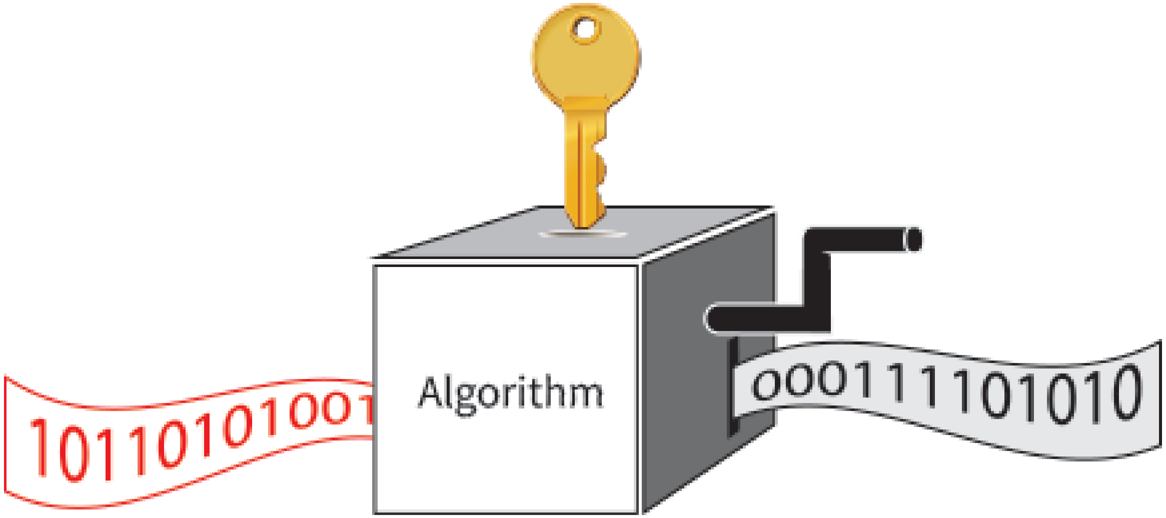
Device Security Architecture

- ❑ Secure Data
- ❑ Verify software has not been tampered
- ❑ Authenticate Remote Systems and Users



Kerckhoff's Principle

A cryptographic system should be secure even if everything about the system, except the private key, is public knowledge.

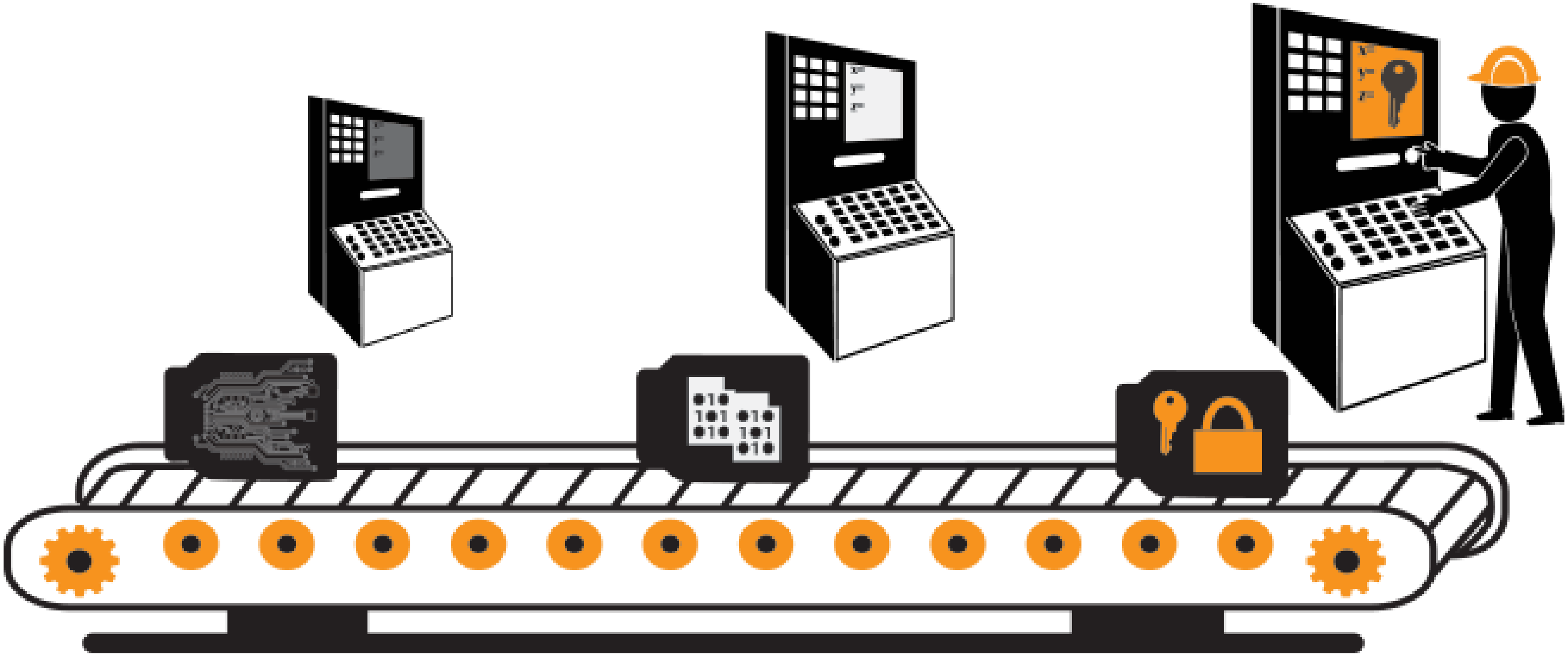


Typical Manufacturing Flow

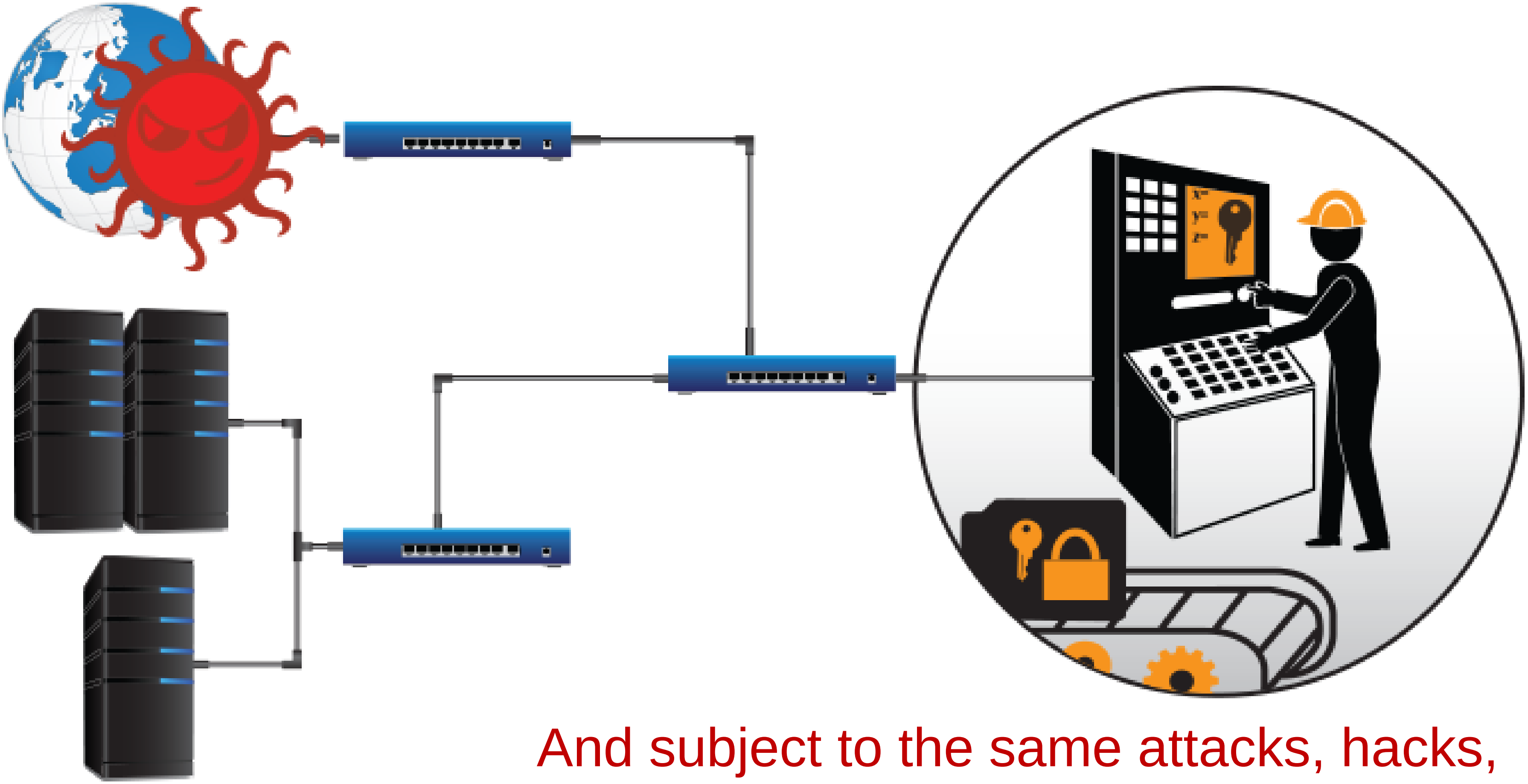
- 1-
Integrated Circuit Test

- 2-
Software Load & Functional Test

- 3-
Key Injection & Final Test



Networked for Monitoring and Updates



And subject to the same attacks, hacks, and breaches as the corporate network!

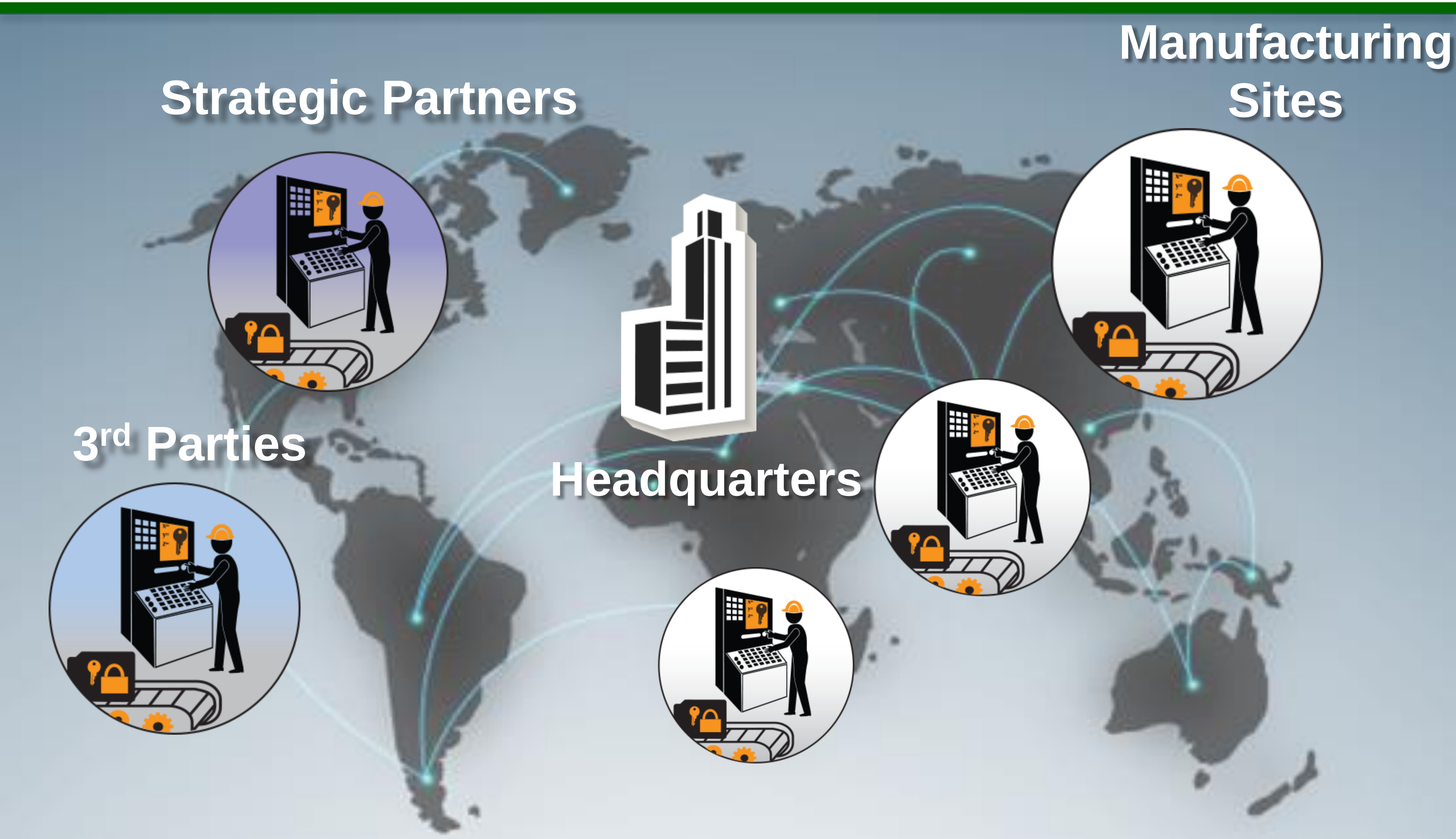
But This Isn’t Just Any Data!

- ❑ Network Attacks
- ❑ Disgruntled Employee
- ❑ Accident

Compromised Keys

= All Devices at Risk!

Supply Chain Complexity Makes it Harder

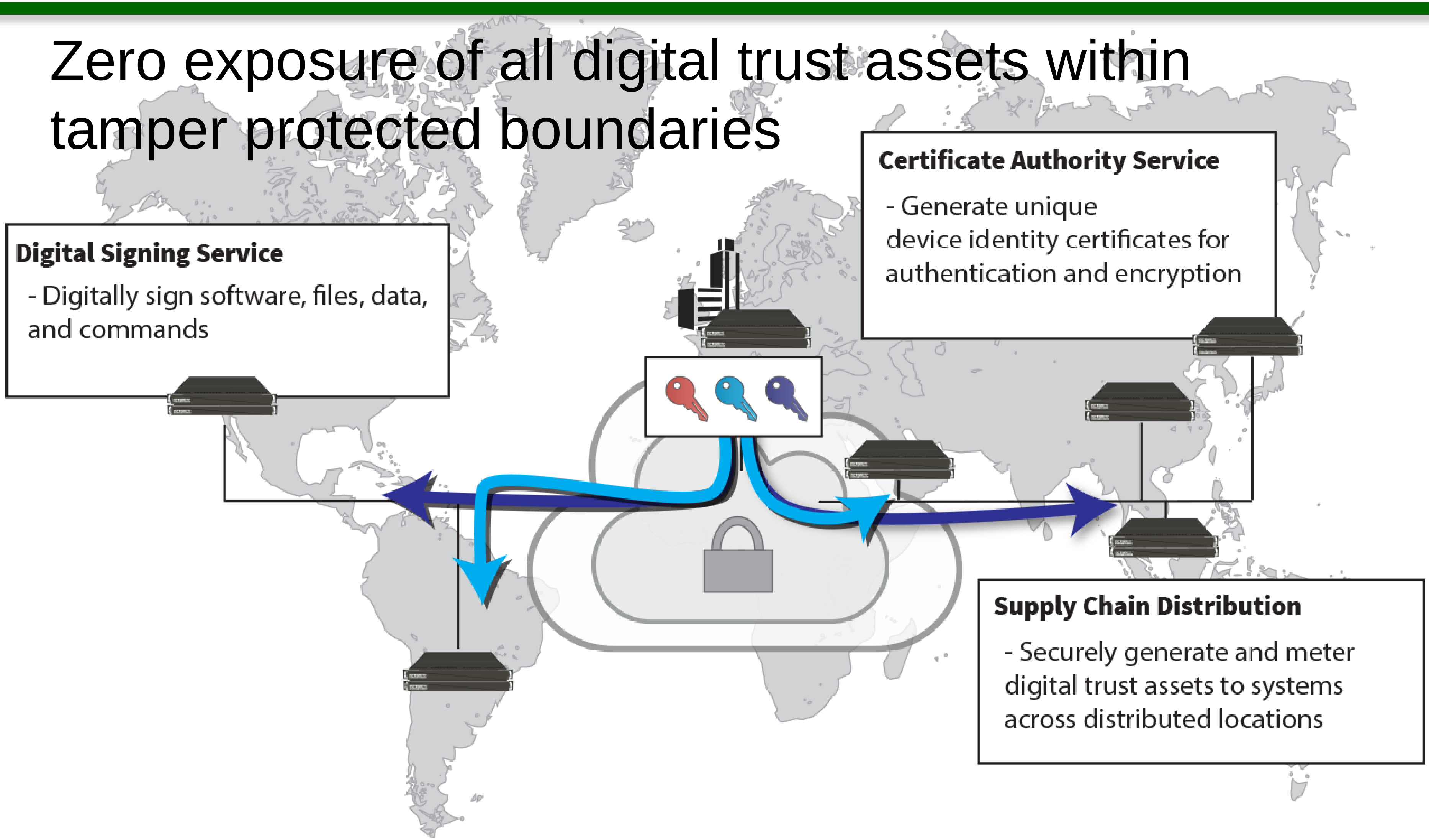


The Purpose of a Security Infrastructure

- Protect digital trust assets from unauthorized access across ALL endpoints
- Digitally sign software & data
- Generate keys & certificates
- Distribute assets to devices

Security Infrastructure

Zero exposure of all digital trust assets within tamper protected boundaries



Digital Signing Service

- Digitally sign software, files, data, and commands

Certificate Authority Service

- Generate unique device identity certificates for authentication and encryption

Supply Chain Distribution

- Securely generate and meter digital trust assets to systems across distributed locations

Green Hills SOFTWARE

Thanks for your attention!

Q & A