Industrial Internet Consortium

Reference Architecture

Dynamic Composition and Automated Interoperability Challenge

David Beberman
aicas GmbH

Challenge: IIC-RA Chapter 16

Chapter 16 Dynamic Composition and Automated Interoperability

Section 16.3 Functional Components

- Dynamic Composition
- Integration Contract Management

IIC-RA Viewpoint

Chapter 7 Implementation Viewpoint

- Relevant for all architectures described
- Edge and Device software dynamic composition
- CPU and OS agnostic
- Hardware configuration aware
  - part of integration contract

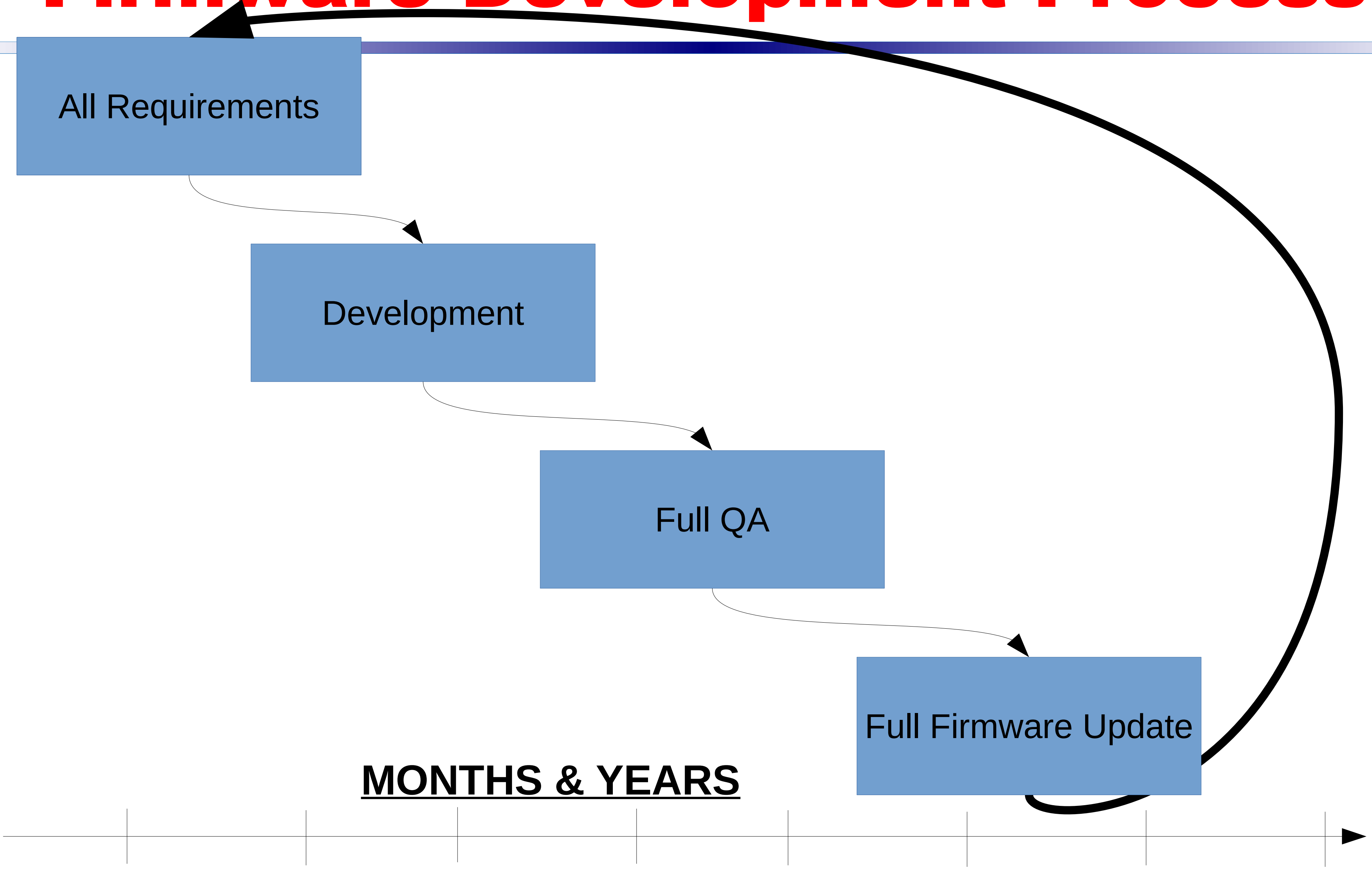
“Hidden” Challenge

Vendor Quality Assurance Department

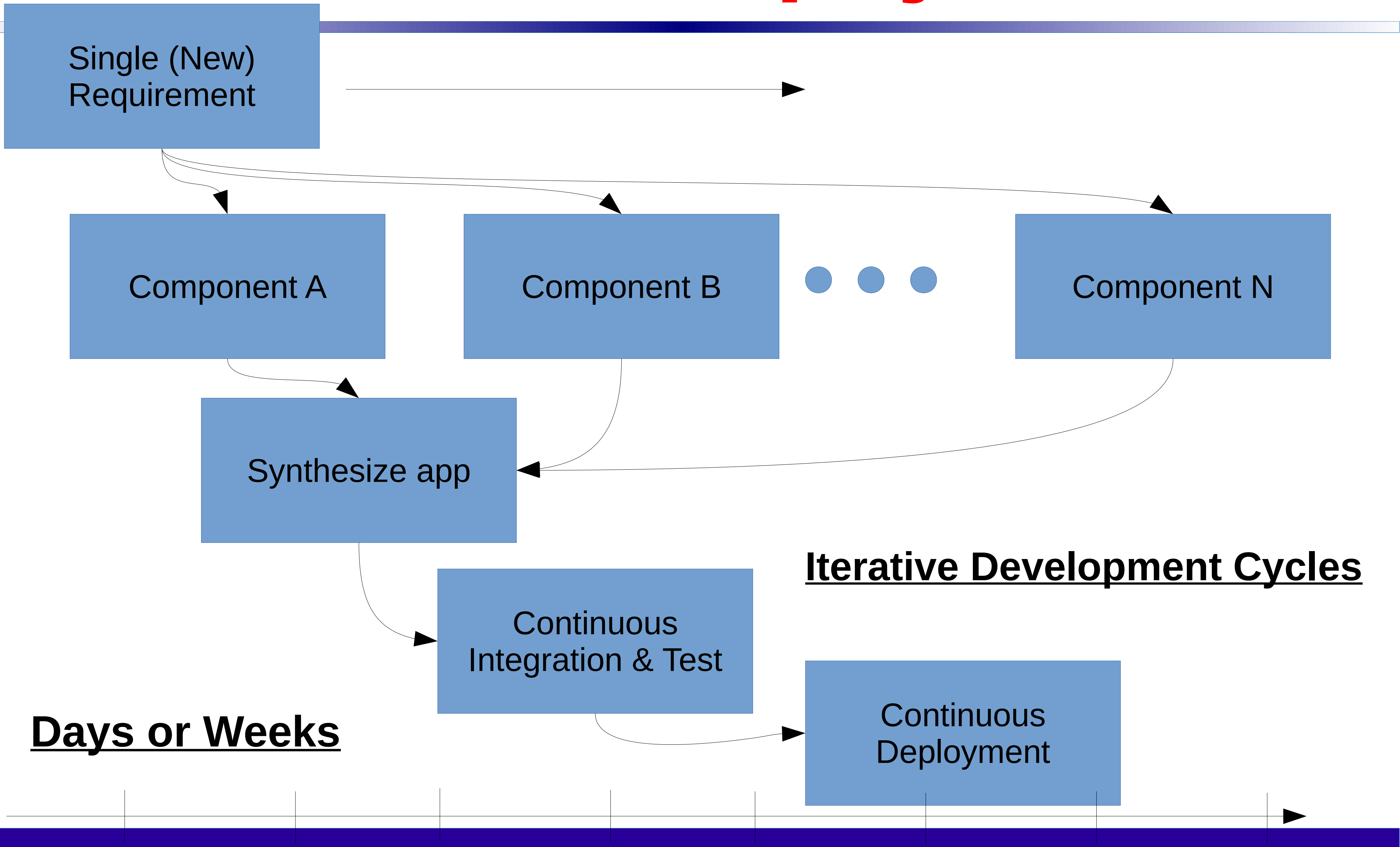
potential chokepoint

- Technical Challenge
  - Proof of dynamic composition and integration automation
- Process Challenge
  - Transition from “big bang” QA to continuous integration, verification and delivery (Agile concept)
- Mindset Challenge
  - History is against us
  - But, Michael Barr's Trial Testimony - Blackbox Testing Insufficient

Firmware Development Process



Continuous Deployment



Iterative Development Cycles

Days or Weeks

Software Dynamic Composition Critical Features

Verifiable Component Isolation Enables

- Component Dependency Resolution
- Component Verification - Automated Tools (e.g. SA)
- Component Automated Unit, System, Regression Test

Component Resource Requirements

- Core Integration Contract Data
- Output From Development and Verification

Objective: Isolation Independence

Show Stability of Software Dynamic Composition

- Transient Composition - Reacting to Events
- Persistent Composition - General Componet Updates
- Online “Live” Composition - No Reset/Restart
- Offline Composition
  - May Require Operation Mode Change

Security Concerns!!!

Automotive Hacks!

- Fiat Chrysler Jeep Hack

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

- GM ONStar

http://analysis.tu-auto.com/telematics/weekly-brief-100-gadget-hacks-gm-cars-build-defcon-hacker-conference?utm_campaign=TUA%2003AUG15%20Newsletter.htm&utm_medium=email&utm_source=Eloqua&elq=4091a7b3978a4049217ebe887202e08&elqCampaignId=2953&elqaid=7083&elqat=1&elqTrackId=55347cd6af6941a988002bc6552eb6fc

https://threatpost.com/holes-in-progressive-dongle-could-lead-to-car-hacks/110511

Security Level for Embedded Systems

- VxWorks

https://community.rapid7.com/community/metasploit/blog/2010/08/02/shiny-old-vxworks-vulnerabilities

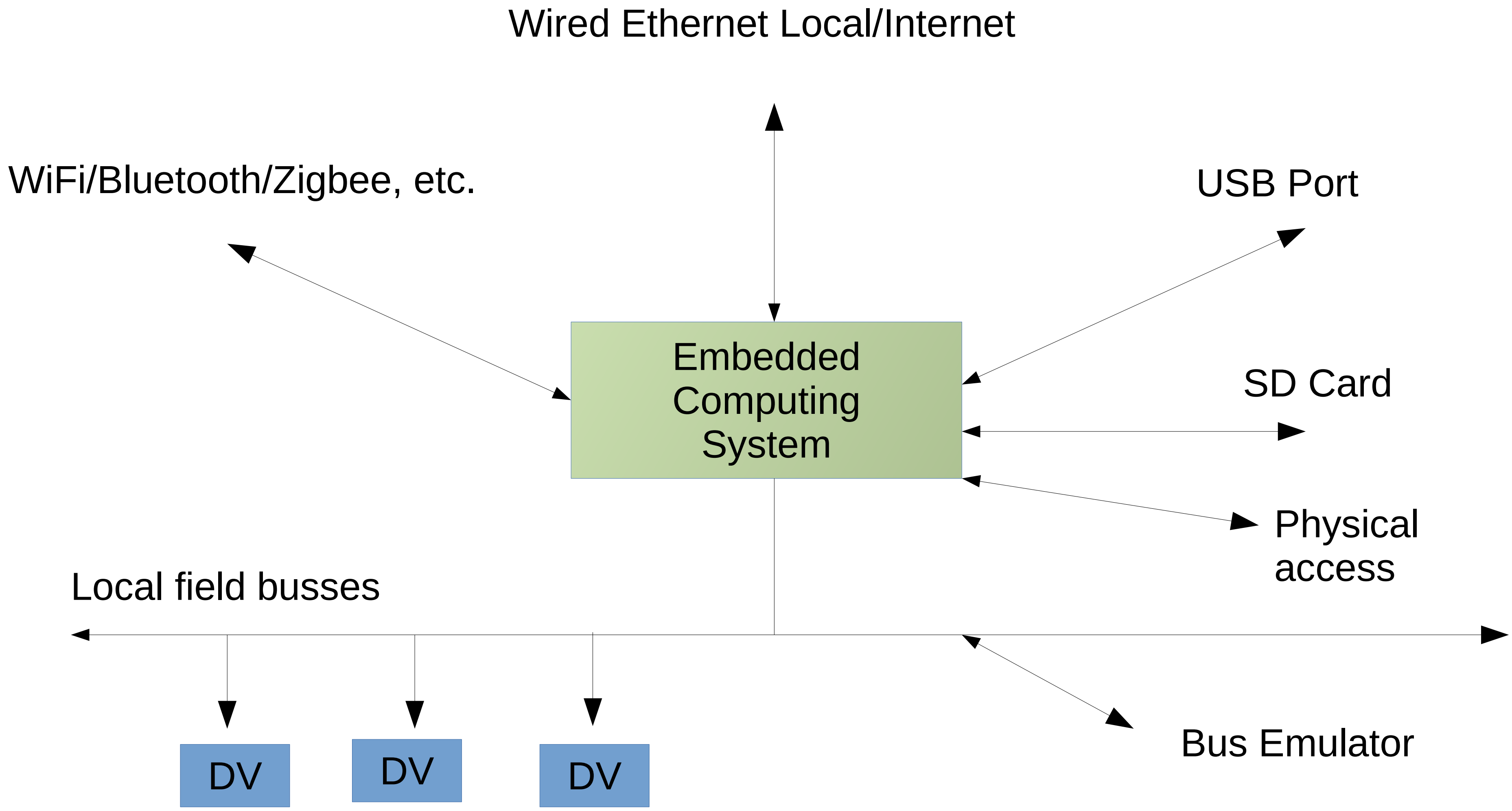
- QNX

https://www.fishnetsecurity.com/6labs/blog/pentesting-qnx-neutrino-rtos

https://ics-cert.us-cert.gov/advisories/ICSA-13-189-01

- Debugger port common practice
  - pdebug, qconn, netcat, qnet
  - similar for other OS's

Attack Vectors


Wired Ethernet Local/Internet
WiFi/Bluetooth/Zigbee, etc.
USB Port
Embedded Computing System
SD Card
Physical access
Local field busses
Bus Emulator
DV
DV
DV

Examples of Attacks

- Fieldbus (CAN, MOD, Etc.) emulator
  - rogue packet insertion
  - reprogramming
  - jamming
- Wired Ethernet
  - snooping of data
  - insertion of bogus data
- USB Port/SD Card
  - system reprogramming
- Peripheral Device Compromise
  - local control
  - rogue packets, etc.
- Wifi/Bluetooth/Zigbee
  - dictionary attack
  - opaque traffic analysis

Cyber Threats

- Denial of Service
- Hijacked Bot Attack
- Dictionary Attack
- Remote commanding of physical systems
- Falsified Sensor and Control Data – impacting local and distributed systems
- Breach of data privacy

Security Reference Material

- Senator Markey's Spycar Act
  - reference
- Industrial Internet Security Framework
  - Under development
- Trusted Computing Group Trusted Platform Module
  - TCG TPM
- ARM Trustzone
- Intel Trusted Execution Technology (TXT)

Core Security Concepts

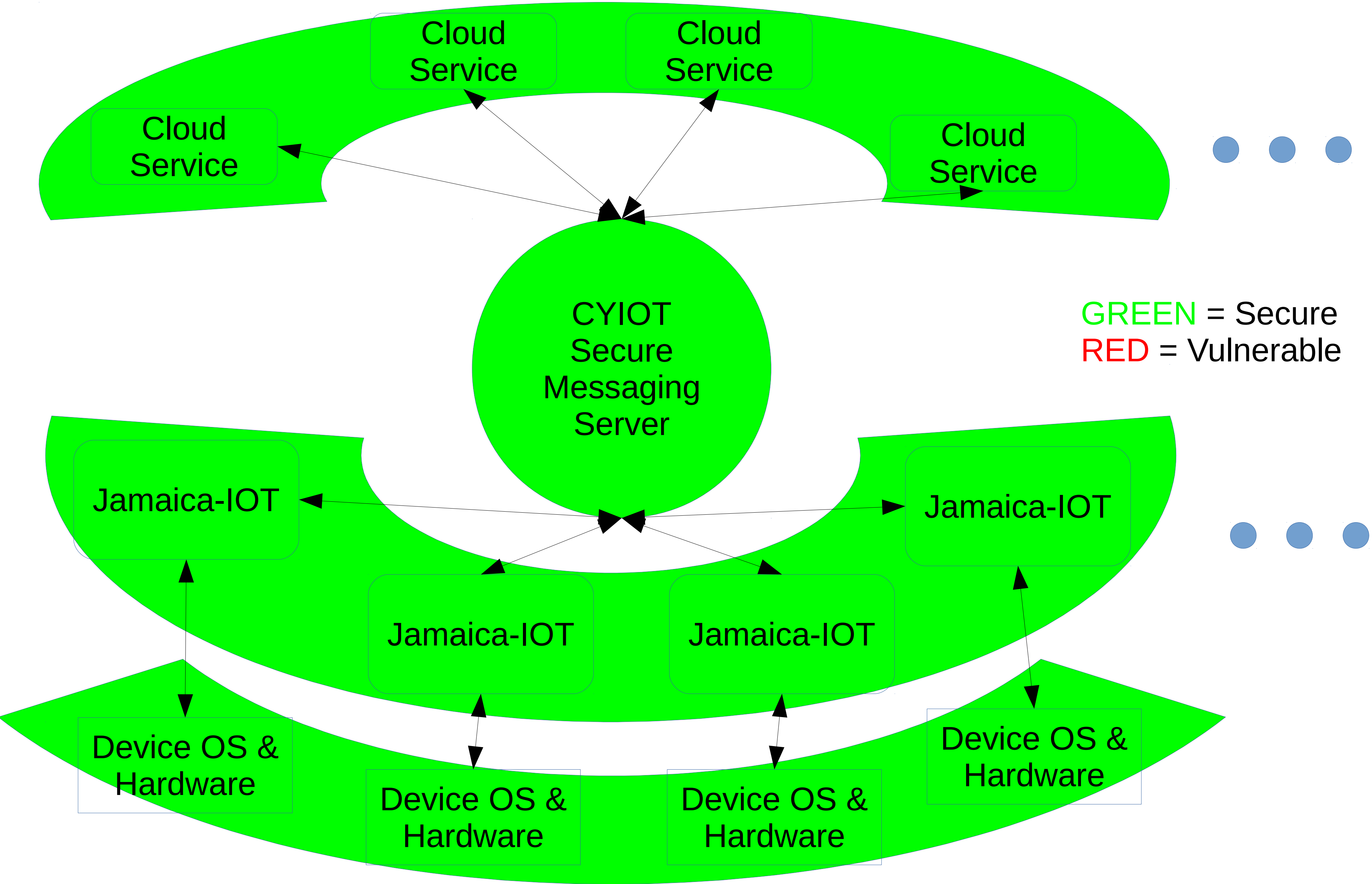
- Secure Hash Algorithm
  - (SHA 256)
- Symmetric Key Encryption/Decryption
  - (AES 256)
- Assymmetric Key Encryption/Decryption
  - RSA
  - ECC
- “Shielded Locations”
  - one-time programmable bits

Cyber Threat Prevention

- Dictionary Retry Delays
- Secure Outbound Connect-only Messaging
  - end-to-end client verification
- Secure Applet Sandbox
- Whitelisting
- Local bus intrustion detection

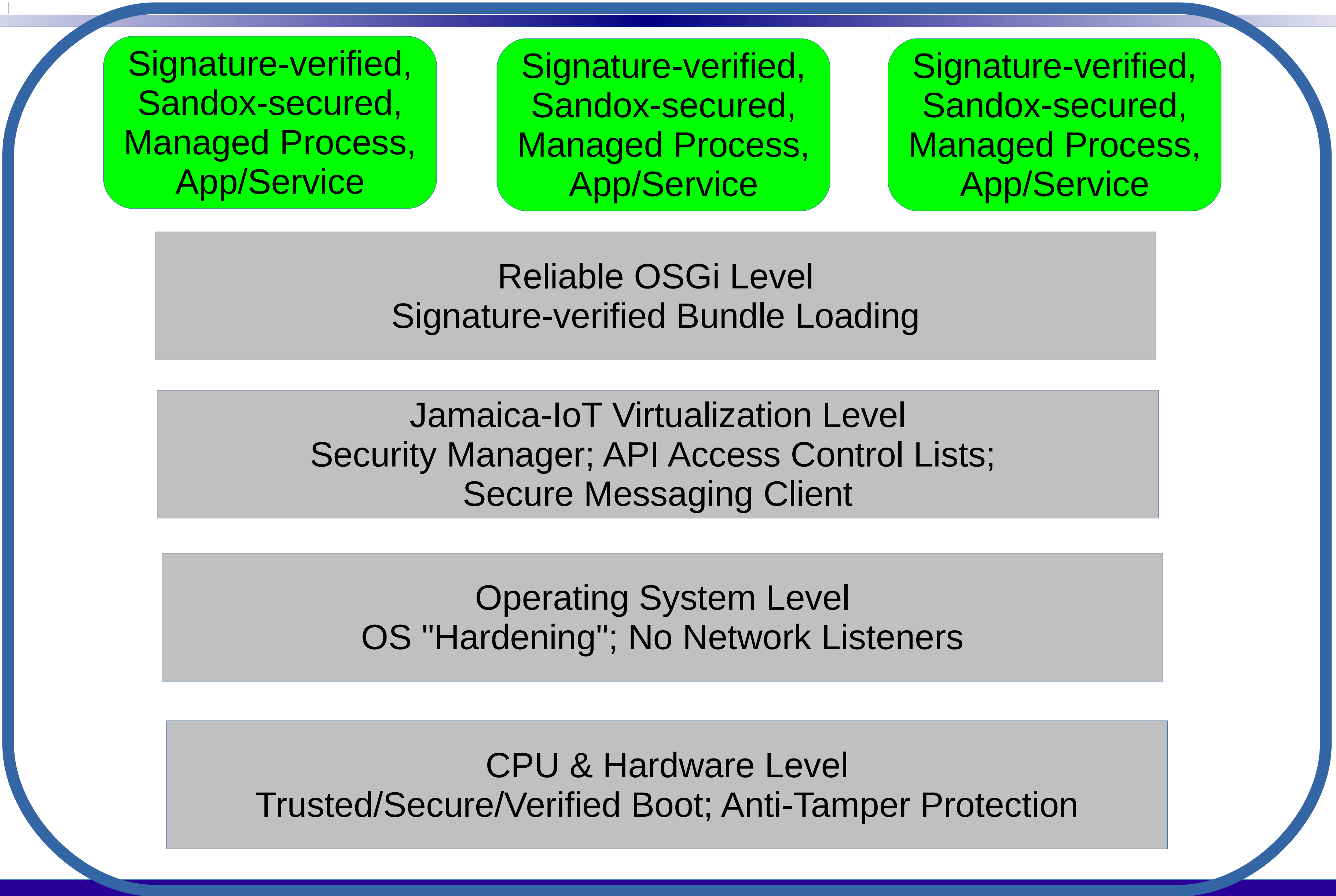
Security Concepts for JamaicaCAR & Jamaica-IoT

Combined Jamaica-IoT, Messaging & Cloud Security Domain with hardened Device operating system and hardware



GREEN = Secure
RED = Vulnerable

JamaicaVM-IoT Security Stack



Signature-verified, Sandox-secured, Managed Process, App/Service

Signature-verified, Sandox-secured, Managed Process, App/Service

Signature-verified, Sandox-secured, Managed Process, App/Service

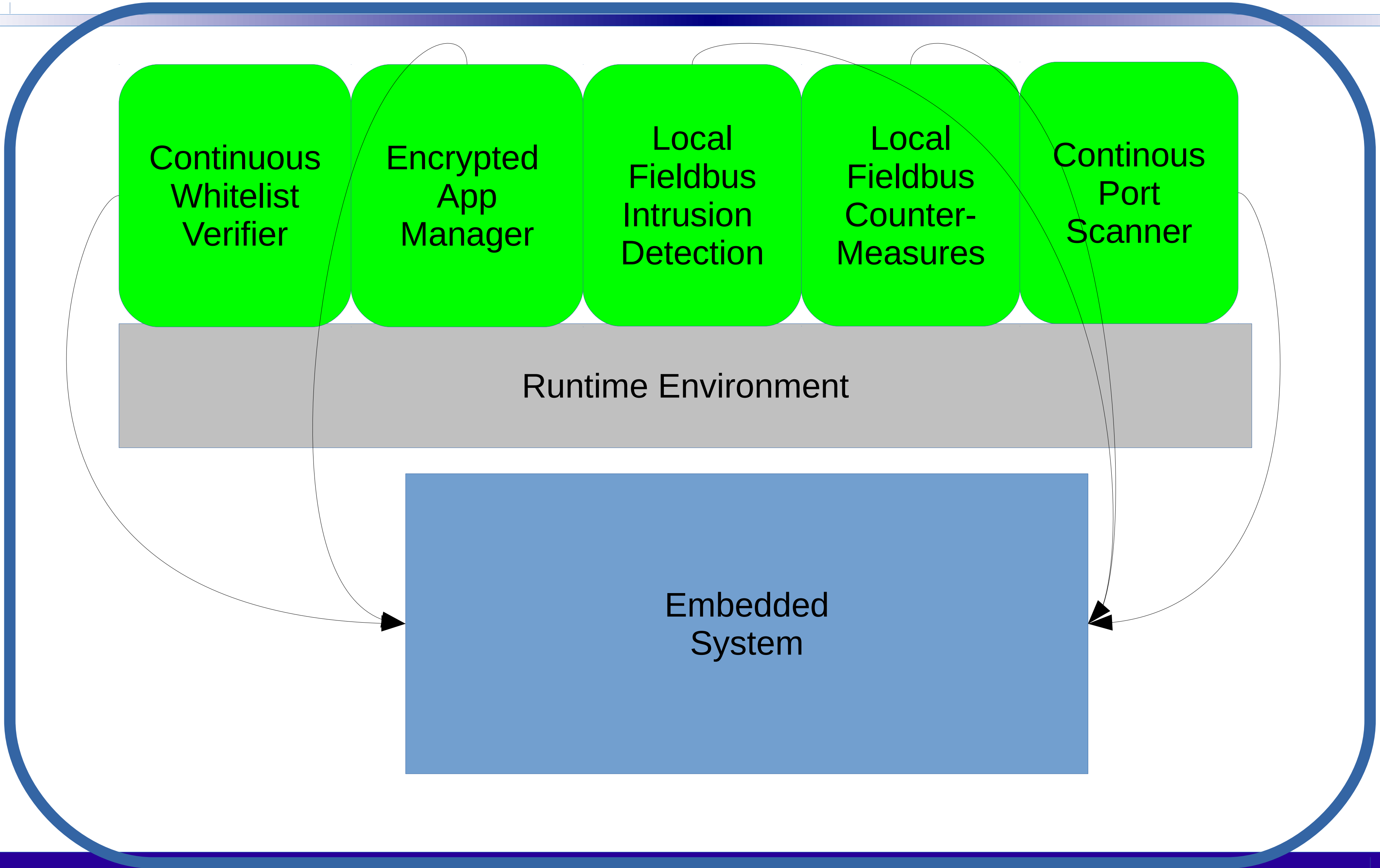
Reliable OSGi Level
Signature-verified Bundle Loading

Jamaica-IoT Virtualization Level
Security Manager; API Access Control Lists;
Secure Messaging Client

Operating System Level
OS "Hardening"; No Network Listeners

CPU & Hardware Level
Trusted/Secure/Verified Boot; Anti-Tamper Protection

JamaicaVM-IoT Security Direction


Continuous Whitelist Verifier
Encrypted App Manager
Local Fieldbus Intrusion Detection
Local Fieldbus Counter-Measures
Continous Port Scanner
Runtime Environment
Embedded System

Security Direction

- Continous Whitelist Verifier
  - .JAR,.EXE,.SO Signature Verifier
  - Running process monitoring
- Encrypted App Manager
  - Symmetric Decryption with protected key
  - Obfuscation guard technology
- Fieldbus Intrusion Detection
  - Learned Patterns Based
  - Transparent

- Fieldbus Countermeasures
  - Intentional Jamming
  - Mode protection
  - Command countering
  - Warnings/Emergency Shutdown
  - Global notification
- Continuous Port Scanning
  - Close unauthorized ports
  - Identify rogue software

Software Supplychain Security

Supplychain Components

- Verification Stage Requirements
  - Toolchain
  - Code Verification
  - Supplier
  - Deployment
  - Installation
  - Runtime
  - API Permissioning

Supplychain Signatures

- Tool chain signature – Aicas Certificate
- Code verification – Supplier Certificate
- Supplier – OEM Certificate
- Deployment – OEM Certificate
- Installation – OEM/Supplier/Toolchain verification
- Runtime – Local Signature Verification
- API Permissions – OEM/Supplier signatures

Device-as-a-Service (DaaS) Concept

DaaS

Ubiquitous Software Platform

- Available on Gateways, Sensors, Actuators, Monitors, Controllers, etc.

Modular Architecture

- Applications, Components, Subcomponents

Hardware, OS Independence

- Leverages available hardware and OS
- Future Proof, heterogeneous environments

“Component Store”

DaaS Software Requirements

Secure OTA Dynamic Lifecycle

- Download, Install, Load, Run, Pause, Stop, Deinstall

Continuous Deployment

DaaS Admission Control Policy

- Managed Resource Limits

Standard APIs, Formally Defined Language and Programming Model

- Worldwide software community acceptance

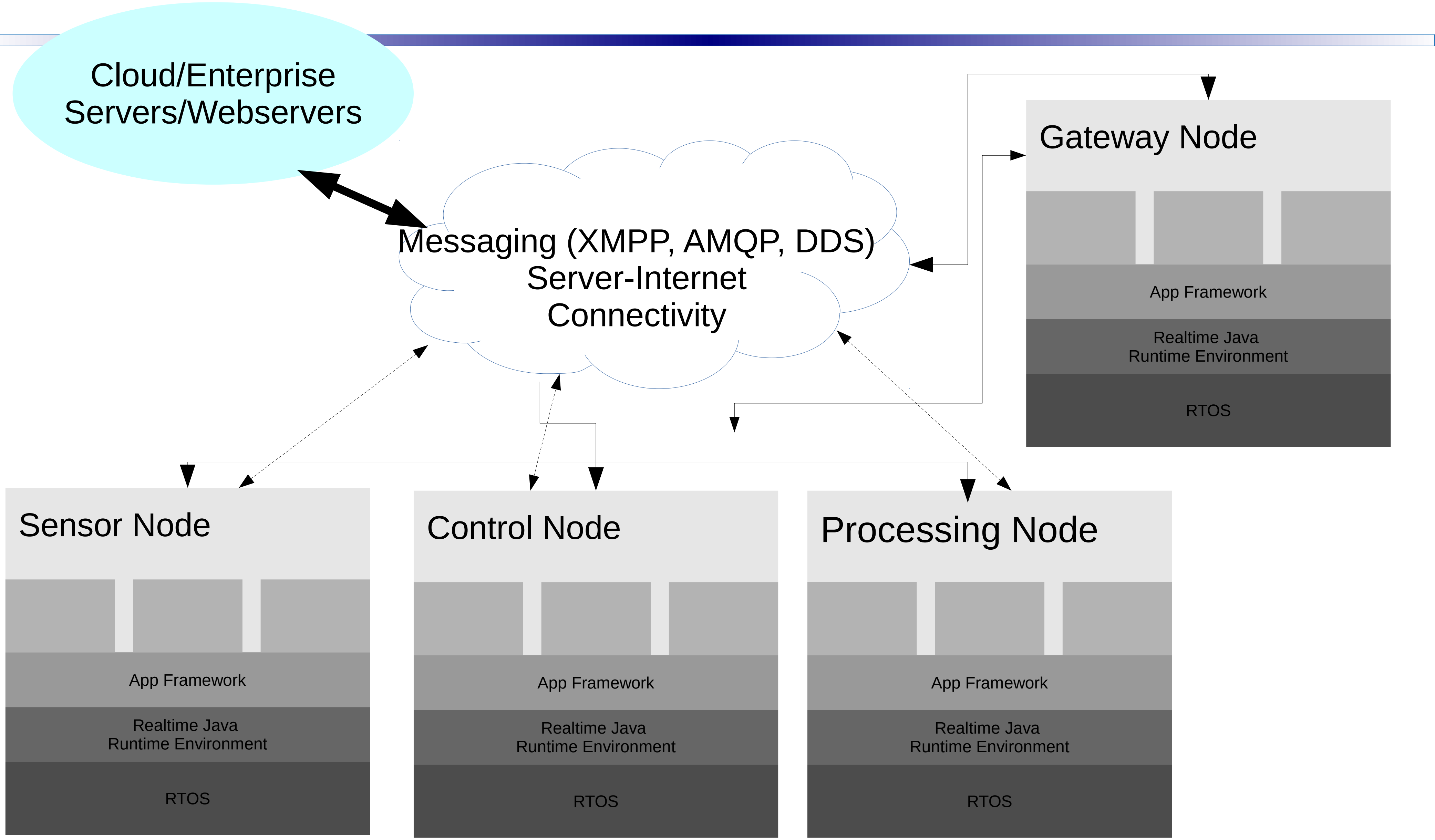
Support Control Systems, PLCs, etc.

- Periodic Tasks, Event-driven Tasks
- Realtime/Determinism
- Device I/O
- Industry-specific Protocols

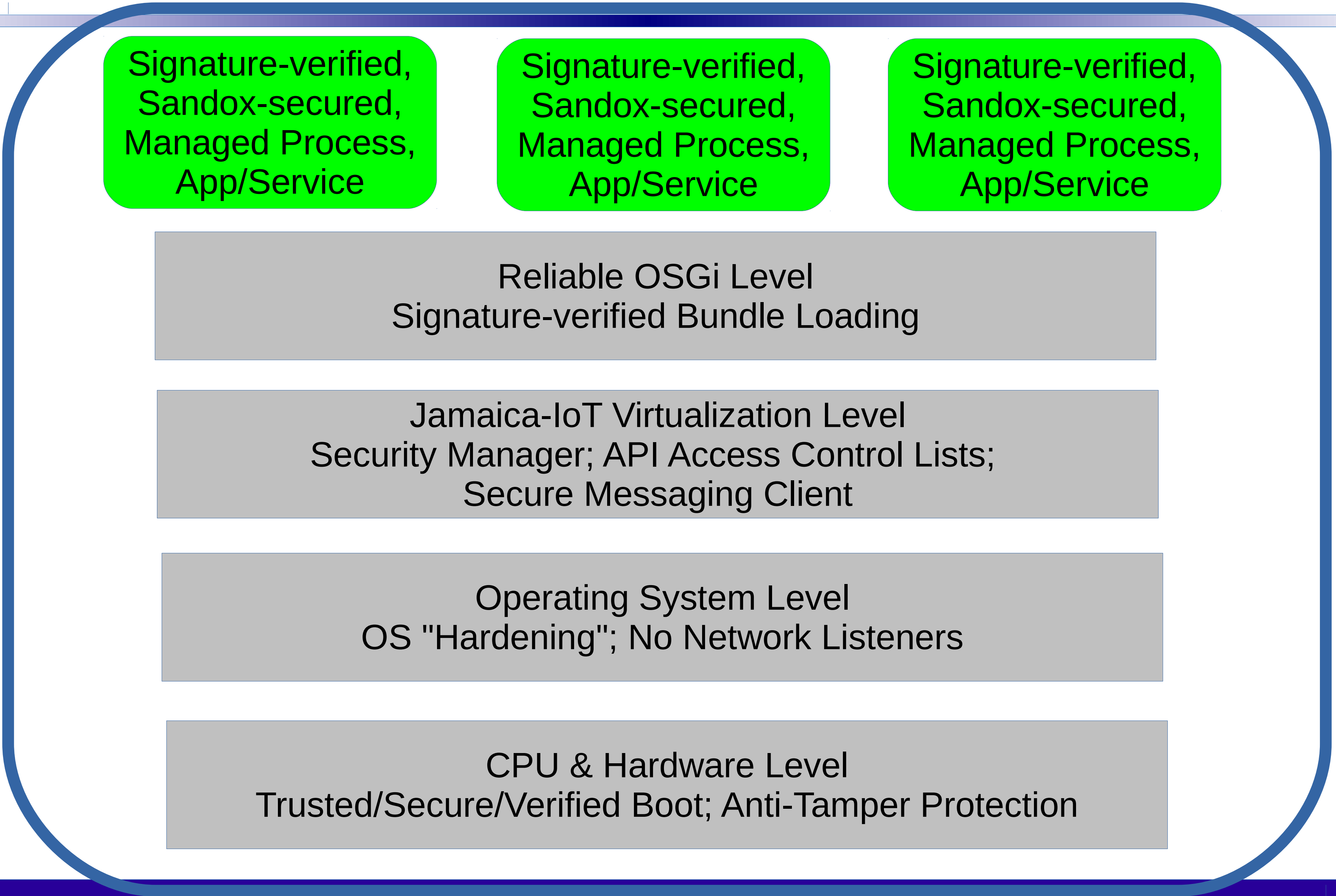
General Resource Efficiency

- Scalable with resource availability

IIoT DaaS


Cloud/Enterprise Servers/Webservers
Messaging (XMPP, AMQP, DDS) Server-Internet Connectivity
Gateway Node
App Framework
Realtime Java Runtime Environment
RTOS
Sensor Node
App Framework
Realtime Java Runtime Environment
RTOS
Control Node
App Framework
Realtime Java Runtime Environment
RTOS
Processing Node
App Framework
Realtime Java Runtime Environment
RTOS

JamaicaVM-IoT Security Stack



Signature-verified, Sandox-secured, Managed Process, App/Service

Signature-verified, Sandox-secured, Managed Process, App/Service

Signature-verified, Sandox-secured, Managed Process, App/Service

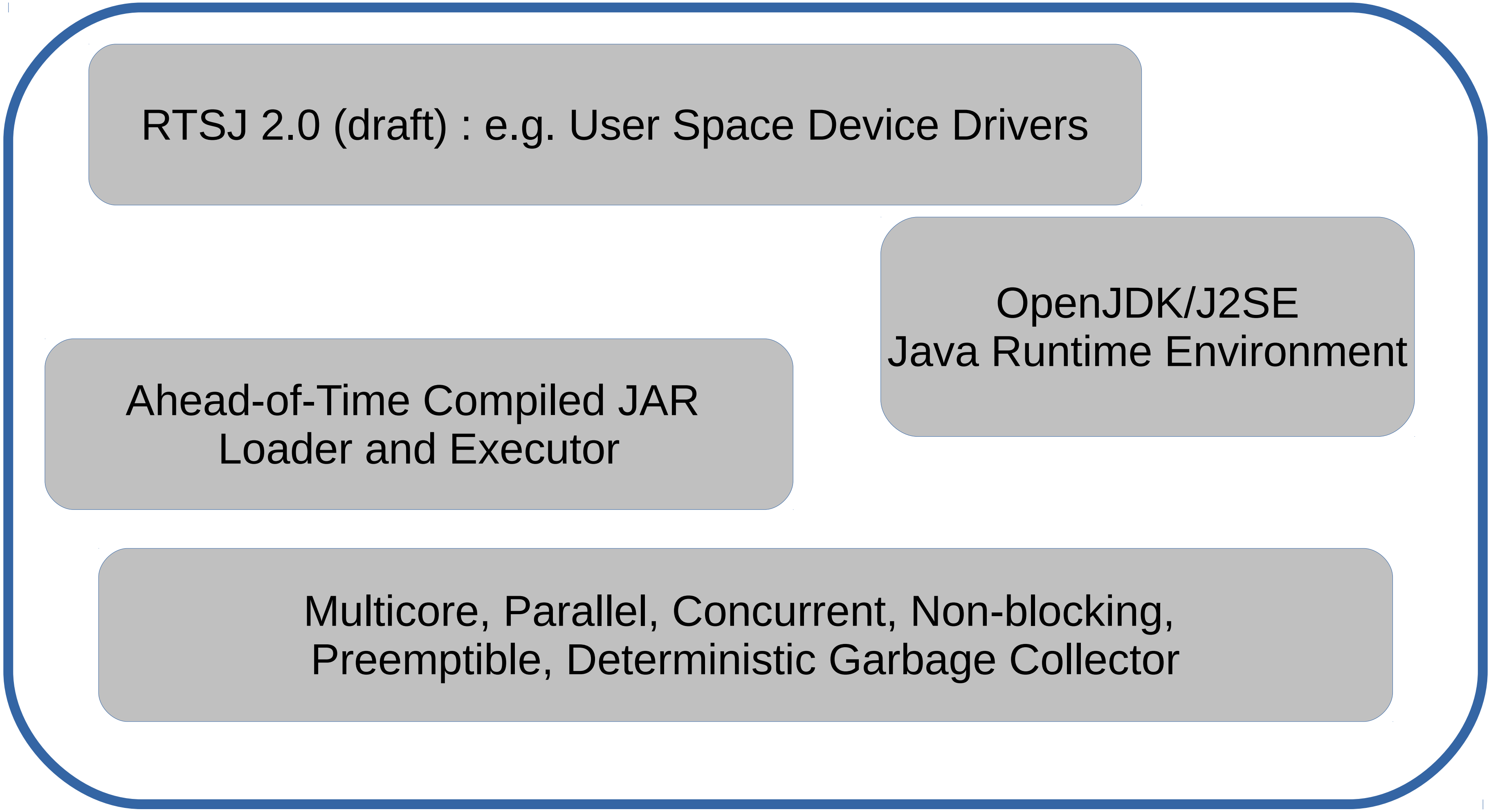
Reliable OSGi Level
Signature-verified Bundle Loading

Jamaica-IoT Virtualization Level
Security Manager; API Access Control Lists;
Secure Messaging Client

Operating System Level
OS "Hardening"; No Network Listeners

CPU & Hardware Level
Trusted/Secure/Verified Boot; Anti-Tamper Protection

JamaicaVM Runtime & Realtime Specification for Java



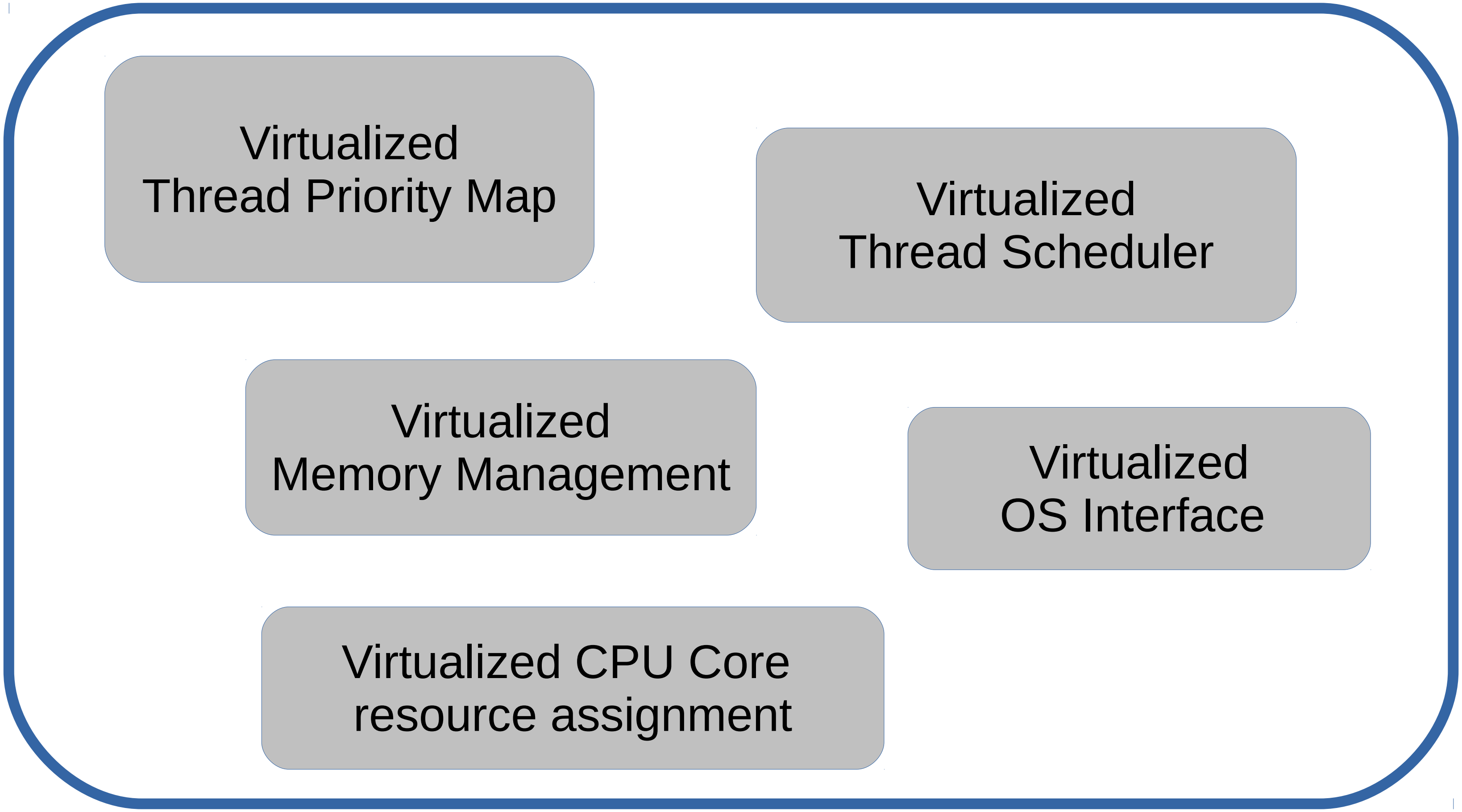
RTSJ 2.0 (draft) : e.g. User Space Device Drivers

OpenJDK/J2SE
Java Runtime Environment

Ahead-of-Time Compiled JAR
Loader and Executor

Multicore, Parallel, Concurrent, Non-blocking,
Preemptible, Deterministic Garbage Collector

Jamaica Process Level Virtualization



Virtualized Thread Priority Map

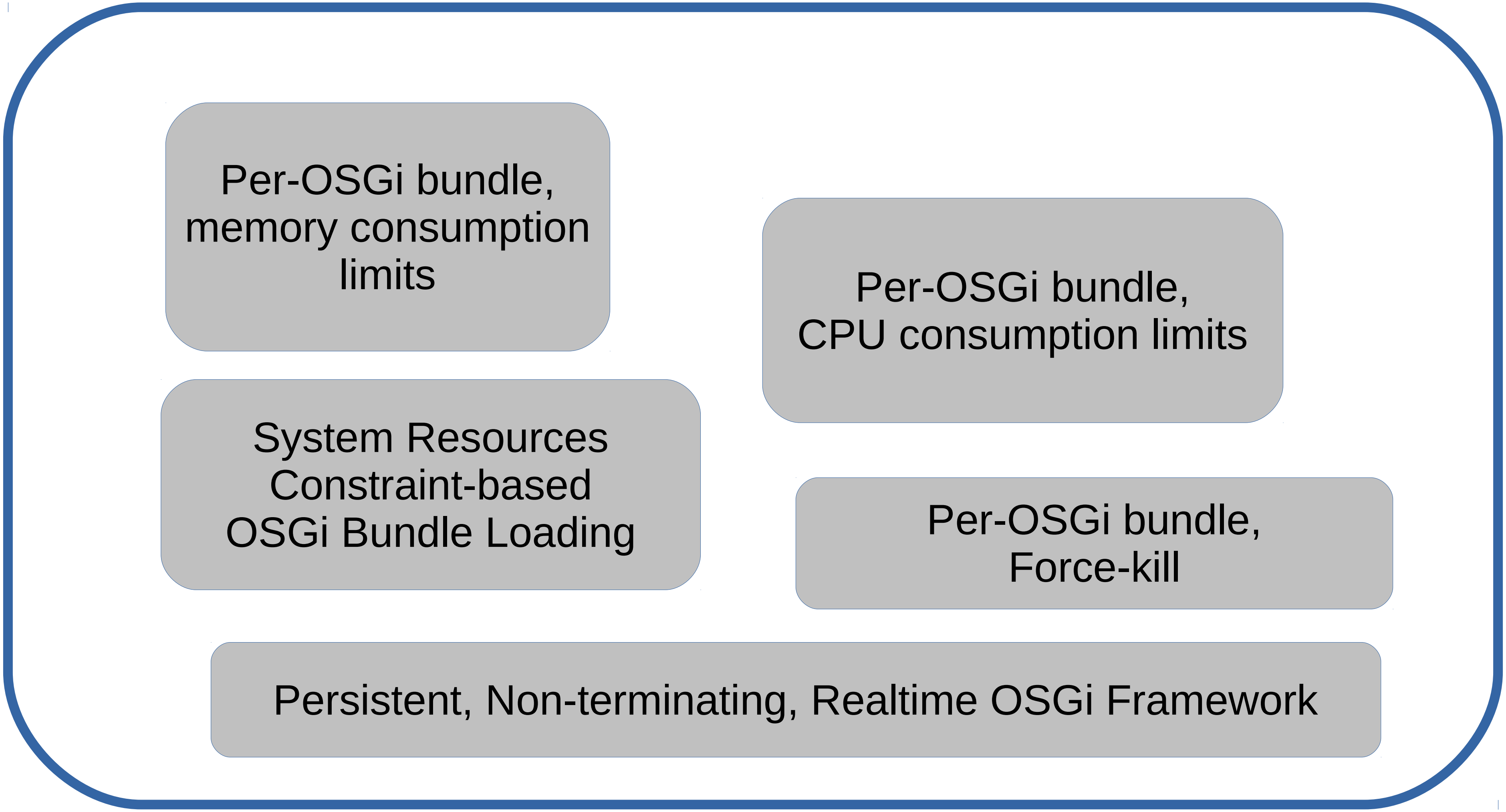
Virtualized Thread Scheduler

Virtualized Memory Management

Virtualized OS Interface

Virtualized CPU Core resource assignment

Jamaica Reliable OSGi



Per-OSGi bundle, memory consumption limits

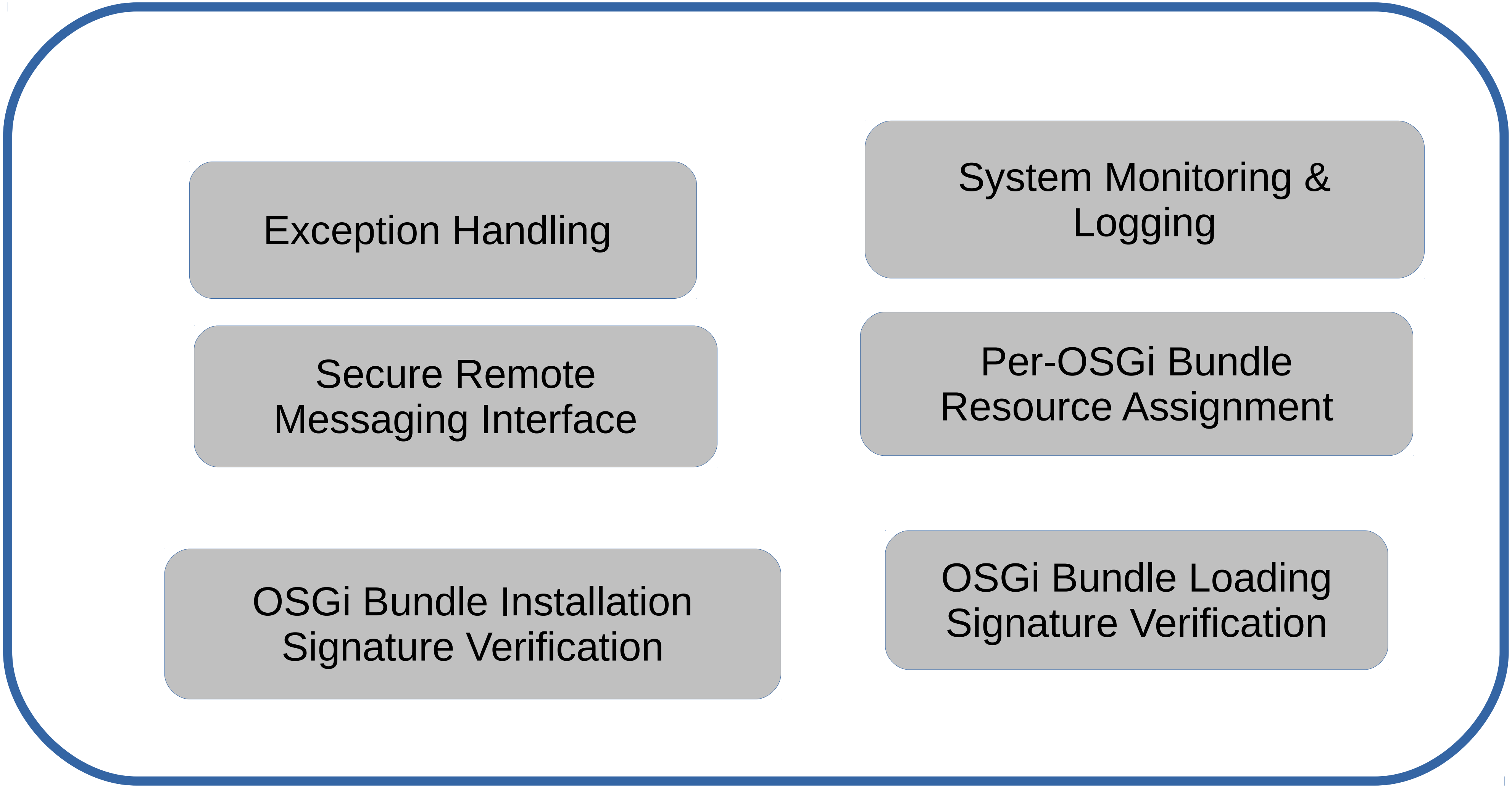
Per-OSGi bundle, CPU consumption limits

System Resources Constraint-based OSGi Bundle Loading

Per-OSGi bundle, Force-kill

Persistent, Non-terminating, Realtime OSGi Framework

OSGi Bundle Management Services



Exception Handling

System Monitoring & Logging

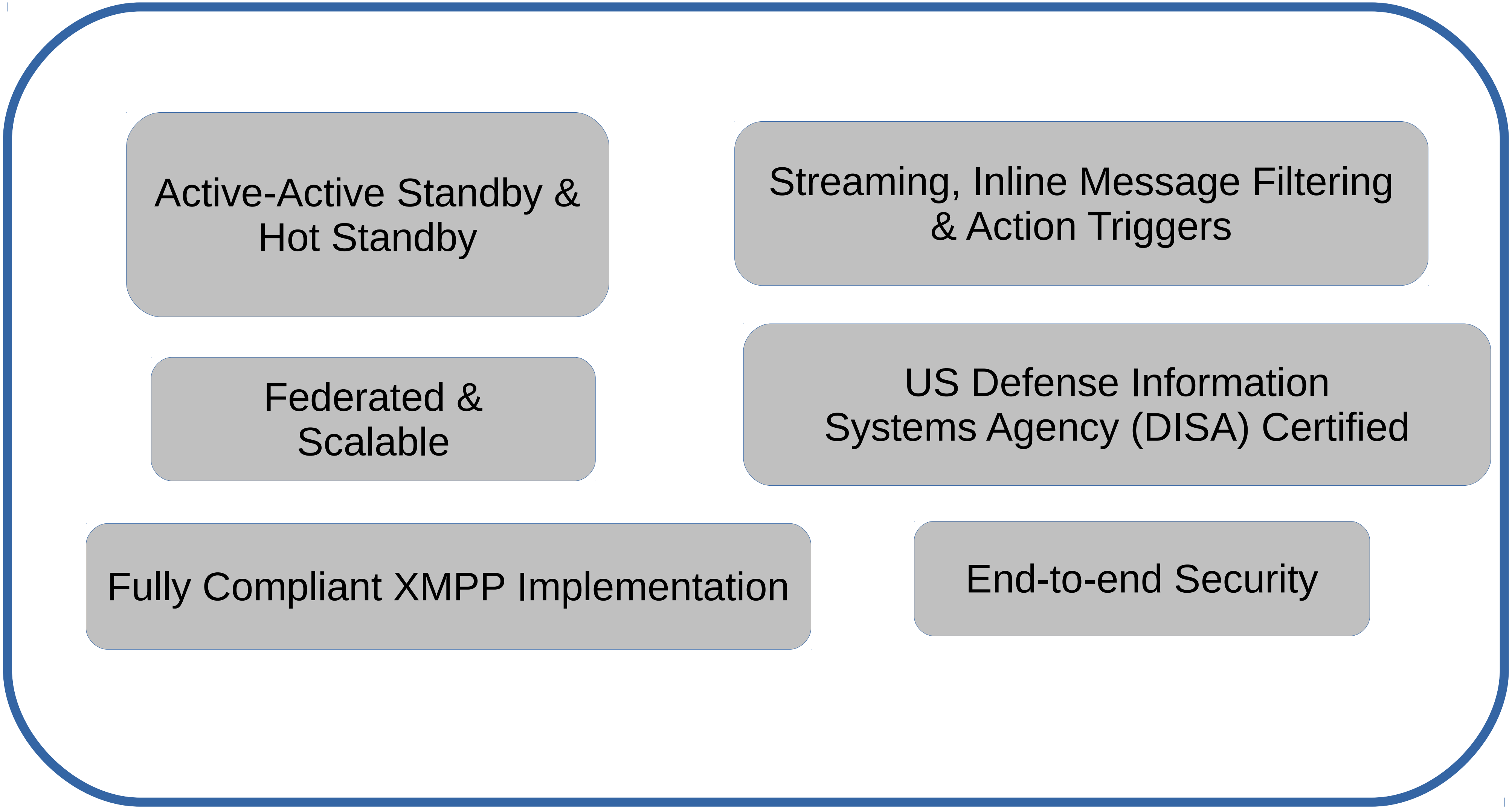
Secure Remote Messaging Interface

Per-OSGi Bundle Resource Assignment

OSGi Bundle Installation Signature Verification

OSGi Bundle Loading Signature Verification

Jamaica-IoT Service Bus



Active-Active Standby & Hot Standby

Streaming, Inline Message Filtering & Action Triggers

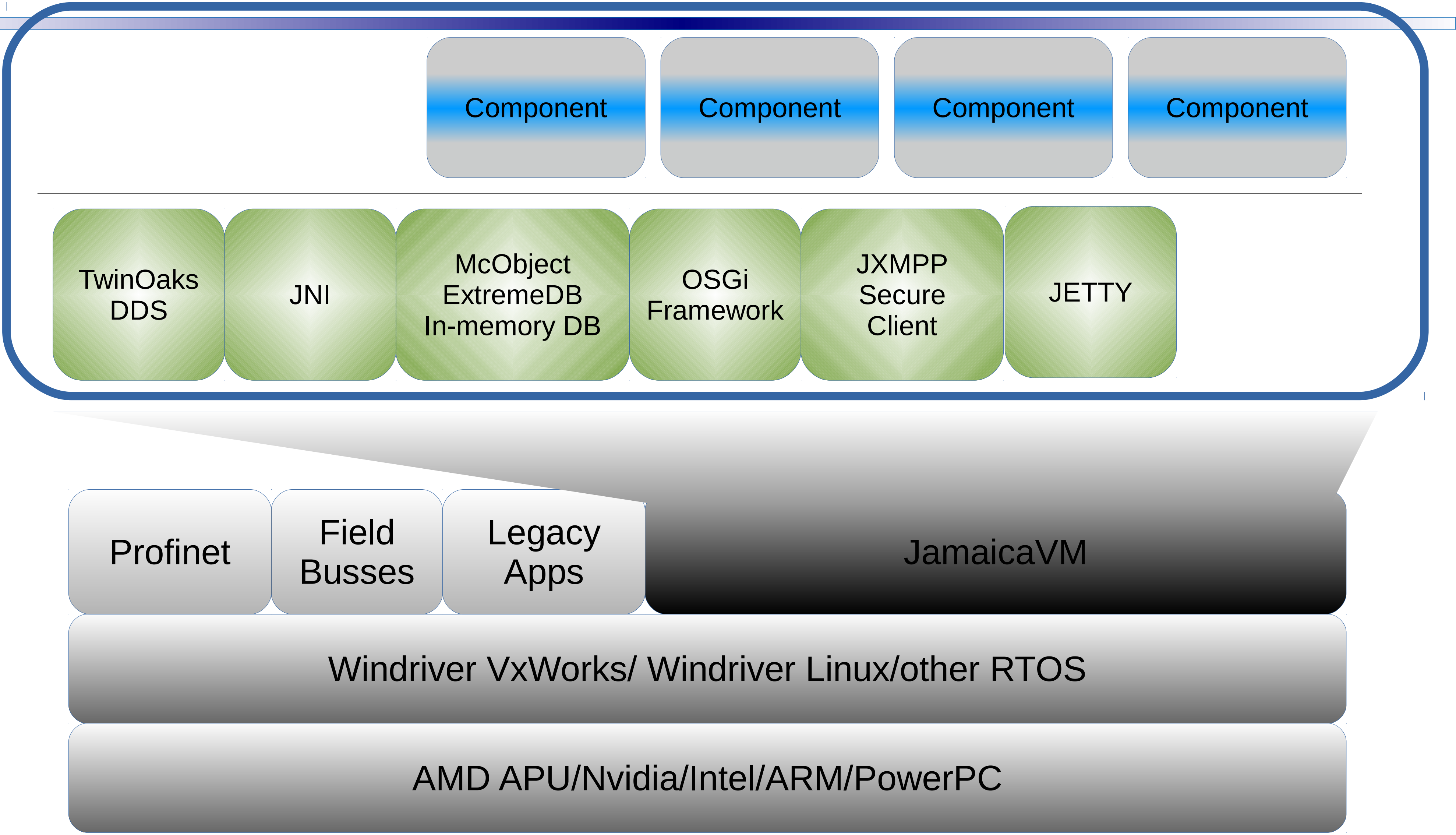
Federated & Scalable

US Defense Information Systems Agency (DISA) Certified

Fully Compliant XMPP Implementation

End-to-end Security

Typical IIoT DaaS Node Example



Component

Component

Component

Component

TwinOaks DDS

JNI

McObject ExtremeDB In-memory DB

OSGi Framework

JXMPP Secure Client

JETTY

Profinet

Field Busses

Legacy Apps

JamaicaVM

Windriver VxWorks/ Windriver Linux/other RTOS

AMD APU/Nvidia/Intel/ARM/PowerPC

Industrial Internet Consortium

Reference Architecture

Dynamic Composition and Automated Interoperability Challenge

David Beberman

aicas GmbH