Turnstile: A High-Assurance Cross Domain Platform

Mark Bortz, David Greve, David Hardin, James Marek, Raymond Richards, and Matthew Wilding

NSA High Confidence Systems and Software (HCSS)

May 2007

Rockwell Collins Proprietary Information

Unclassified/FOUO

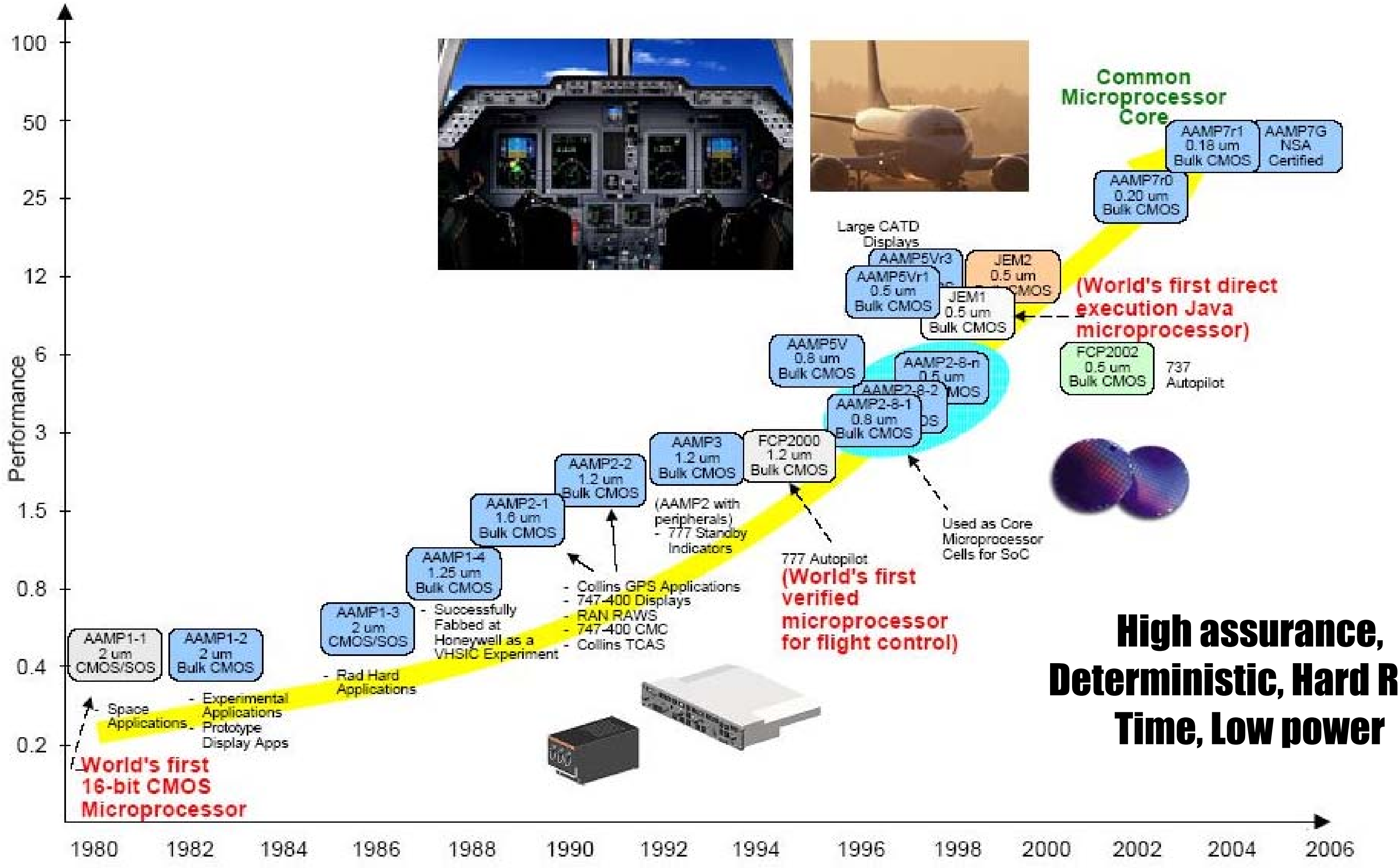
Turnstile

- A High-Assurance Cross Domain platform based on the NSA MILS-certified AAMP7G microprocessor that is accreditable to PL-5 and is also compact, affordable, fast, and flexible.

Assurance Approach

- Utilize the Rockwell Collins AAMP7G microprocessor as the core engine
  - The AAMP7G MILS certification from NSA enables RCI to restrict the highest level of analysis to the “guard kernel”
  - Additional tools developed in conjunction with NSA allows RCI to prove information flow of AAMP7G critical code
- I/O processing (network protocol stack, JMS, etc.) relegated to Offload Engines (OE’s) that do not have to be as highly trusted
  - System integrator can add value to OE’s in the form of custom protocol handlers, etc. without fear of compromising the integrity of the kernel

RCI Microprocessor Technology

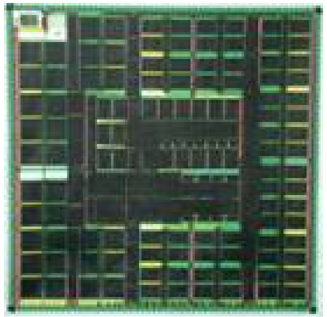


High assurance, Deterministic, Hard Real Time, Low power

MILS Through Hardware Partitioning

AAMP7G Certified Microprocessor

- High Code Density (2:1 Over CISC, 4:1 Over RISC)
- Low Power Consumption
- Long life cycle relative to other commercial uproc.
- Screened for full military temp range (-55 C to +125 C)
- Supports legacy software applications
- Design artifacts owned by RCI
- Implements *intrinsic partitioning*
    - Separation kernel in hardware



AAMP7G certification

- AAMP7G to be used in applications that require separation of data at different classification levels.
- Requirements similar to Common Criteria EAL-7, which entails an evaluation based in part on the use of formal methods.

National Security Agency

Information Assurance Directorate
Approval Certificate

[illegible]

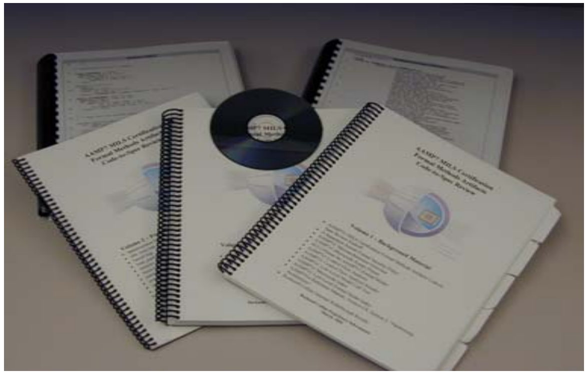
[redacted]

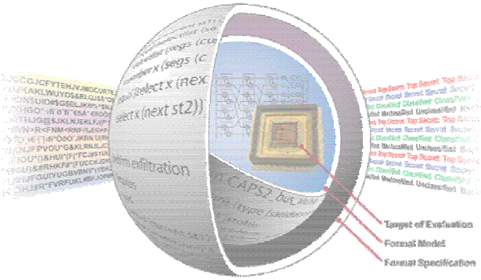
Capable of simultaneously processing unclassified through Top Secret Codeword information

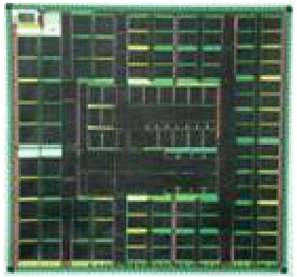
AAMP7G Certified Microprocessor

- Developed formal description of separation for uniprocessor, multipartition system
- Modeled trusted AAMP7G microcode
- Constructed machine-checked proof that separation holds of AAMP7G model
- Model subject of intensive code-to-spec review with AAMP7G microcode
- Satisfied formal methods requirements for NSA AAMP7G certification awarded in May 2005

"… capable of simultaneously processing unclassified through Top Secret Codeword information"



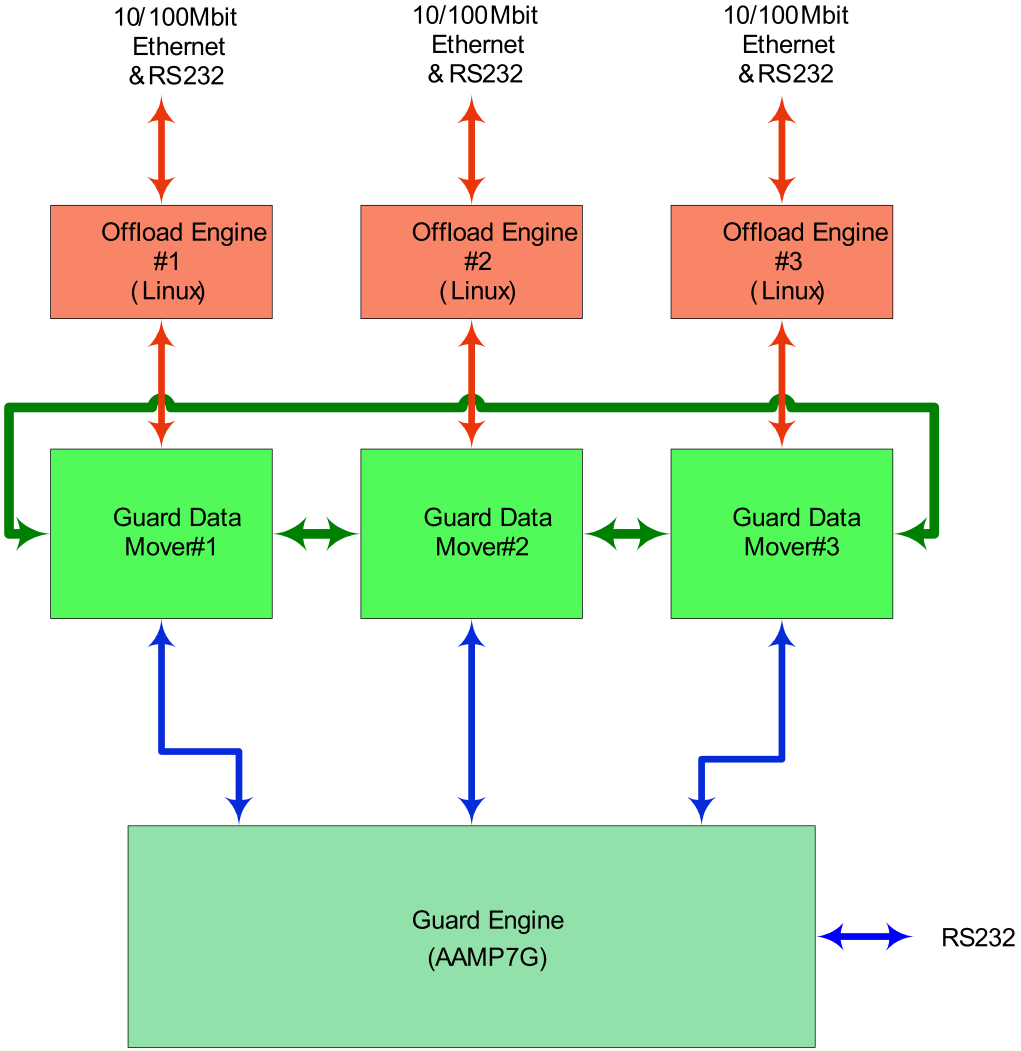




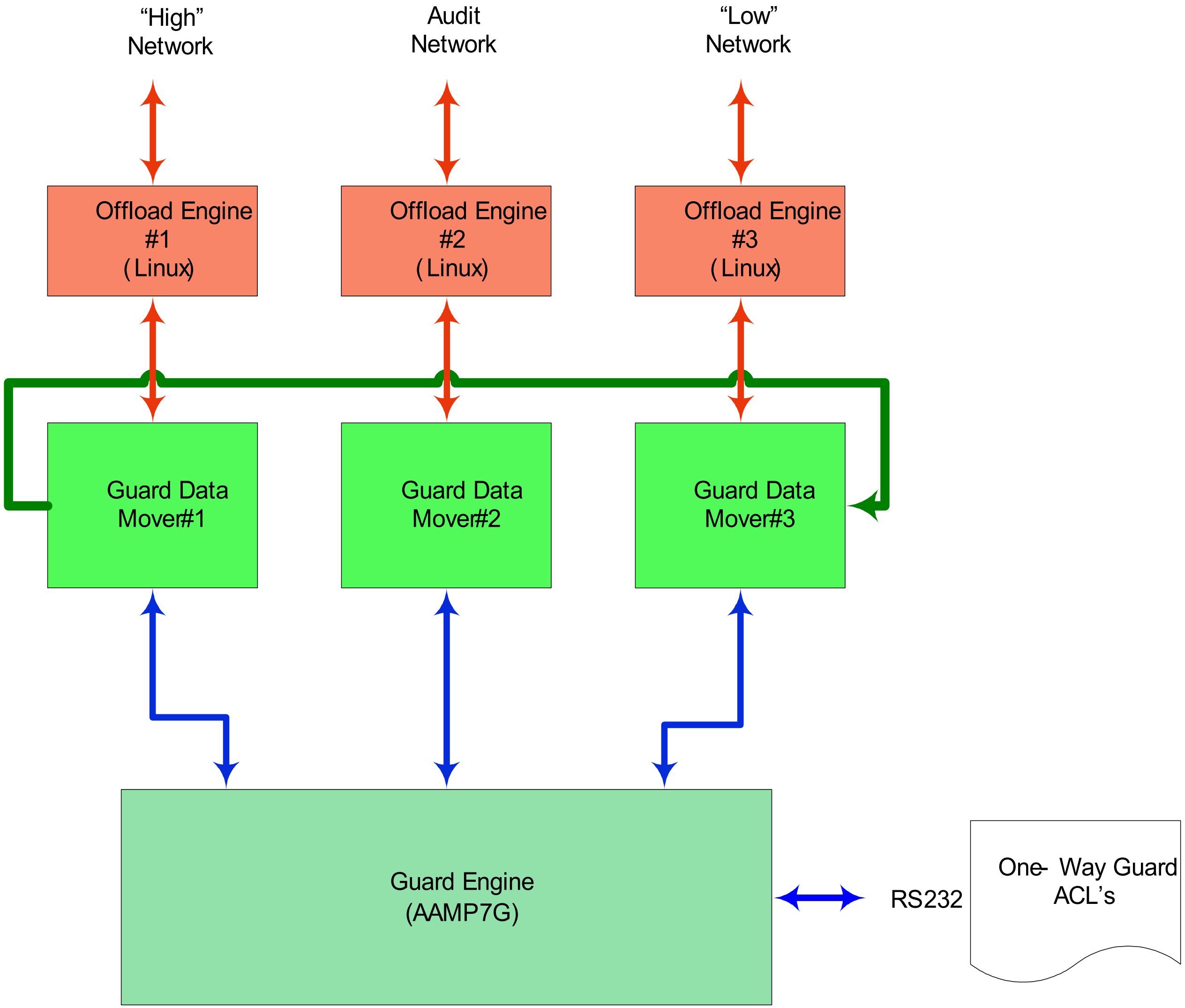
Turnstile Functional Components

- Guard Engine
  - Performs guard function
  - Configures system
  - Performs audit function
  - Performs health monitoring
- Offload Engines
  - Perform network I/O
  - Support user-defined functionality (e.g., JMS clients)
  - Performs (self) health monitoring
- Guard Data Movers
  - Perform high-speed I/O under control of Guard Engine
  - No autonomous behavior

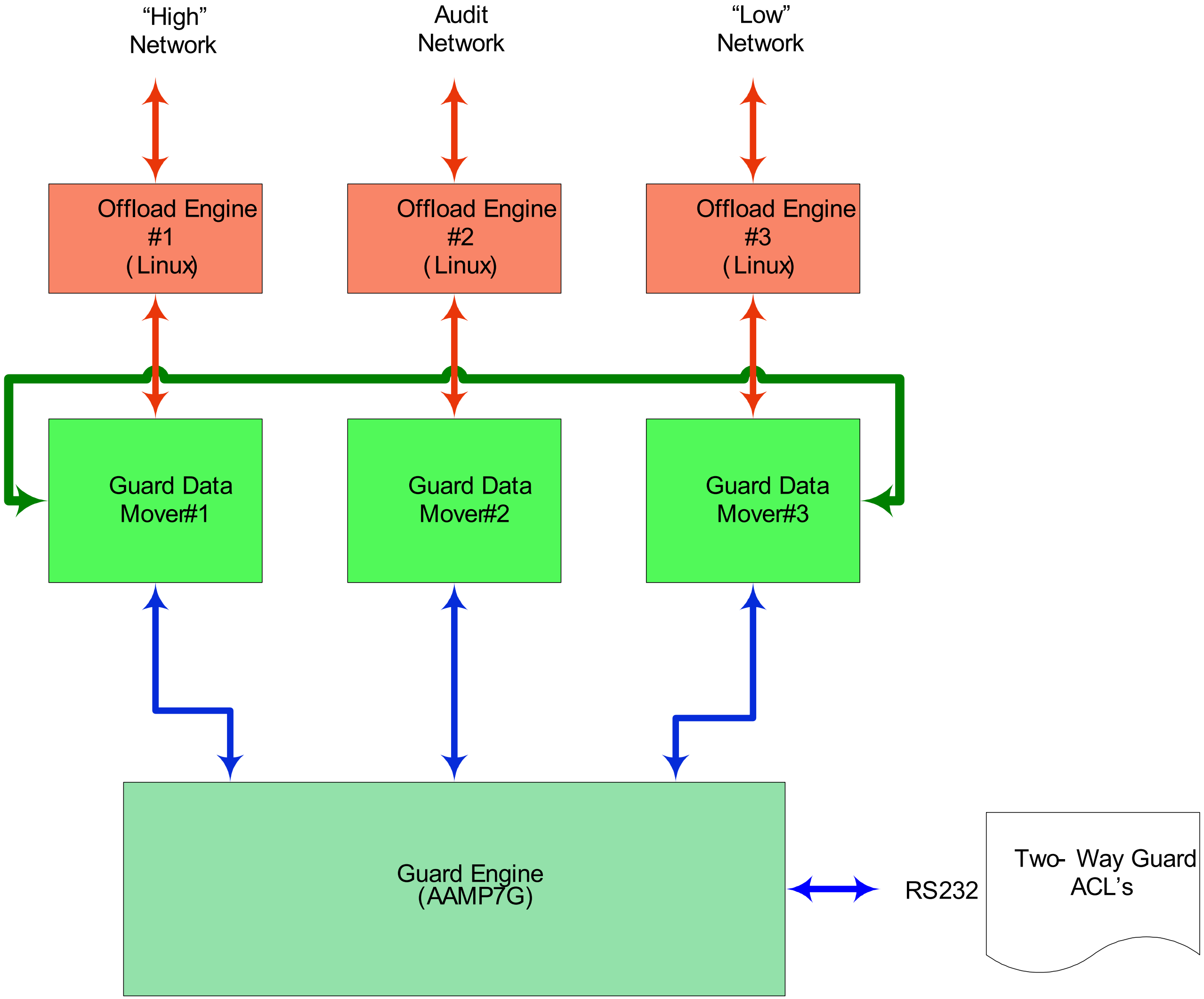
Turnstile Functional Block Diagram


10/100Mbit Ethernet & RS232
10/100Mbit Ethernet & RS232
10/100Mbit Ethernet & RS232
Offload Engine #1 (Linux)
Offload Engine #2 (Linux)
Offload Engine #3 (Linux)
Guard Data Mover#1
Guard Data Mover#2
Guard Data Mover#3
Guard Engine (AAMP7G)
RS232

One-Way Guard Use Case



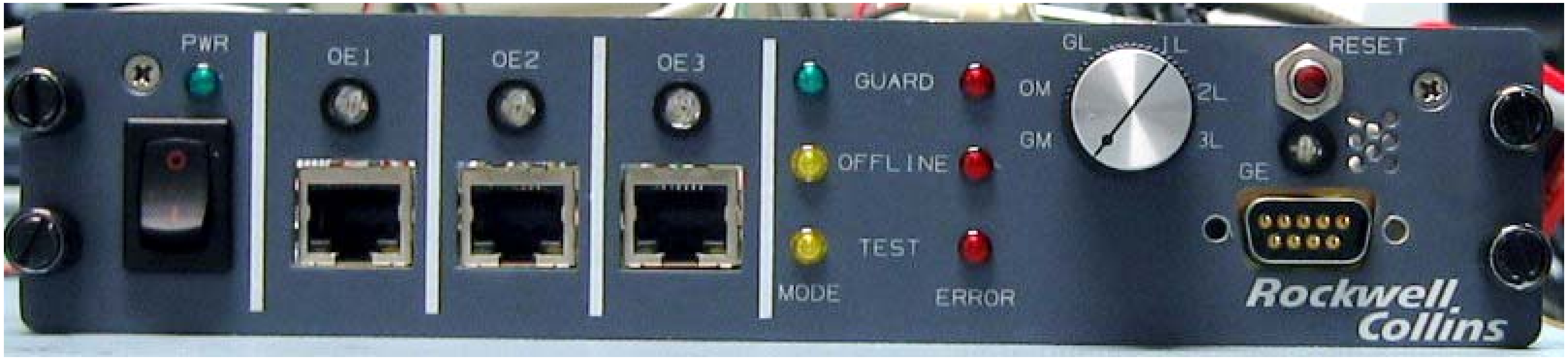
Two-Way Guard Use Case



Turnstile Top Level Design Requirements

- DCID 6/3
  - Protection Level 5
  - Availability: Medium
  - Integrity: High
- High/Low data interfaces are 10/100BaseT Ethernet (RJ45)
- Audit/Control port is 10/100BaseT Ethernet (RJ45)
- Enclosure will be ½U rack mount
- Enclosure will operate from 110/240V 50/60Hz AC
- User programmable (Offload Engines)
- Configurable Guard Engine Access Control Lists (ACL’s)
- Operation in a benign, ground environment

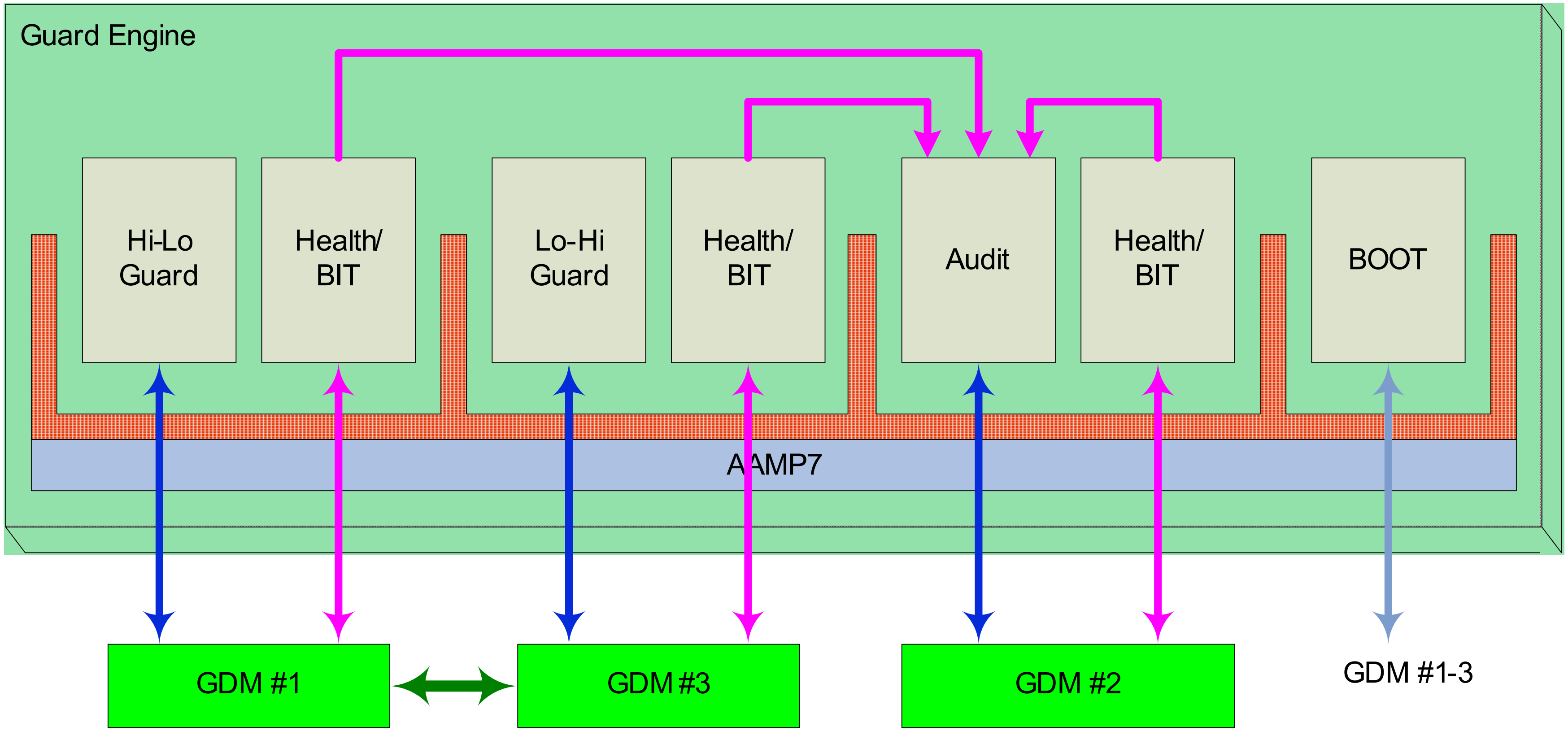
Turnstile Front Panel



Guard Engine

- The Turnstile guard engine provides the following functionality:
  - Nonvolatile storage (program and configuration data storage)
  - Volatile storage
  - Real Time Clock
  - GDM interfaces
  - RS-232 interface (for loading ACL’s)

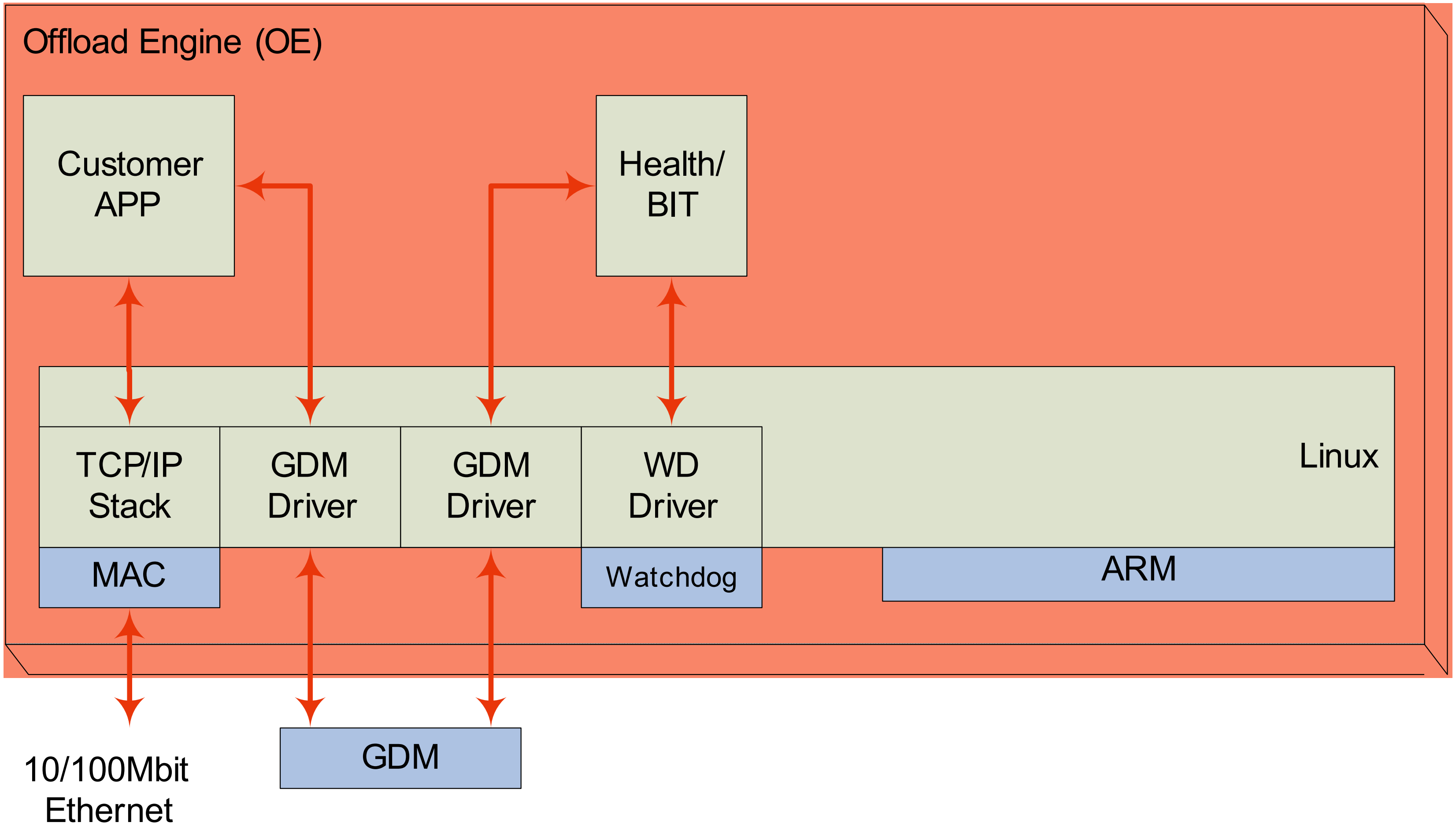
Turnstile Guard Engine Software and Hardware Interaction



Offload Engines (OE’s)

- Each Turnstile offload engine provides the following functionality:
  - Nonvolatile storage (program and configuration data storage)
  - Volatile storage
  - 10/100BASE-T Ethernet channel
  - RS-232 interface
  - Linux Operating System

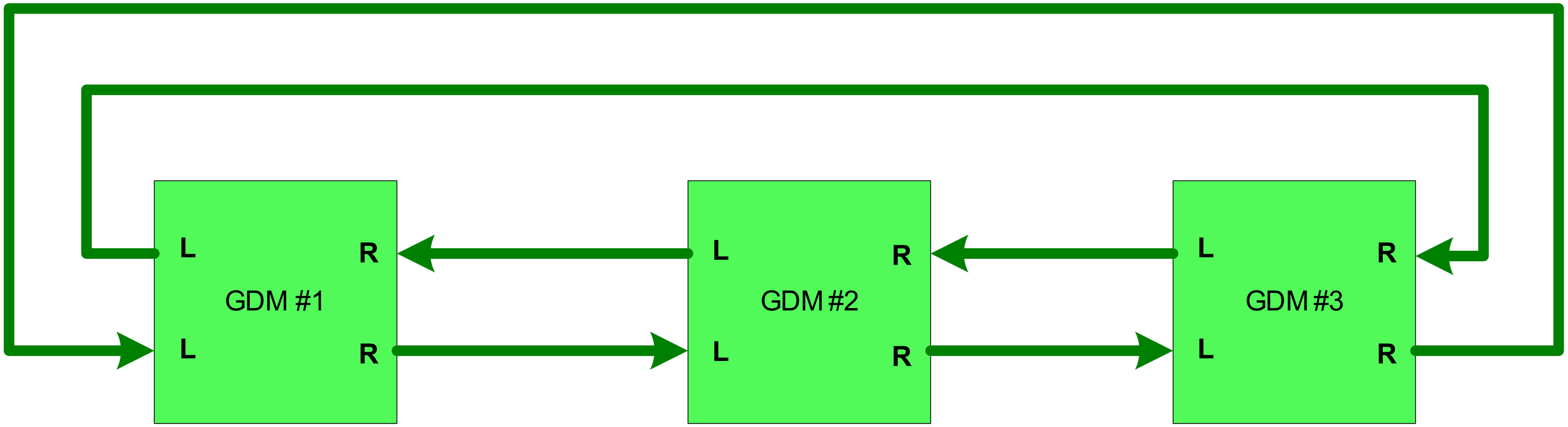
Turnstile Offload Engine Software and Hardware Interaction



Guard Data Movers (GDM's)

- Turnstile provides three independent GDMs.
- Each GDM provides the following OE interfaces:
  - Transmit Data (Data flow from offload engine to the GDM)
  - Receive Data (Data flow from GDM to offload engine)
  - Control (Data flow from GDM to offload engine)
  - Health/Status (Data flow from offload engine to GDM)
  - Audit (Data flow from GDM to offload engine)
- Each GDM provides the following independent Guard Engine interfaces:
  - Configuration
    - Only AAMP7G Guard Engine can configure the three GDM's, at boot time
  - Transmit Data & Control (Transmit Data buffer is read/write by the guard engine)
  - Control (Data flow from guard engine to GDM)
  - Health/Status (Data flow from GDM to guard engine)
  - Audit (Data flow from guard engine to GDM)

Guard Data Mover Interconnect



Audit Interface

- Audit
  - Turnstile audit utilizes the SYSLOG protocol.
  - Turnstile produces periodic “health” audit messages, at five minute intervals.
  - The “health” audit messages include a timestamp, BIT results from each subsystem, and network cable status (attached/unattached).
  - The Turnstile produces “dropped” audit messages for dropped data messages.
  - The “dropped” audit messages include a timestamp, message ID, message source address, message destination address, and reason for not passing.
  - The audit interface does **not** provide an information channel from the low-to-high network.
- Control
  - Growth capability to allow coprocessors for special purposes, e.g. virus scanning, high-speed XML checking, etc.

Health Monitoring

- Power-On Built-In Test (PBIT)
  - Performed during system reset
  - Goes into Fail mode if failed
- Continuous BIT (CBIT)
  - Performed periodically during normal operation without disruption to normal operation
  - Goes into Fail mode if failed
- Initiated BIT (IBIT)
  - Performed when in a diagnostic mode and an IBIT command has been received

- Watchdog timers on GE, OE's must be periodically strobed
  - If any not strobed in time, system reset will occur

Two Initial Turnstile Use-Cases

- One-Way Guard
- Two-Way Guard

One-Way Guard (OWG) Characteristics

- The Turnstile OWG is capable of associating classification semantics with message headers, in accordance with the CISS-ISM classification metadata standard.
- The Turnstile OWG applies a Mandatory Access Control based on interface classification and message classification markings.
- The Turnstile OWG supports labeling each interface with at least a classification level and a national releasability set.
- The Turnstile OWG will process at least the following IC-ISM attributes: *classification*, *releasableTo*, and *disseminationControls*.
- The high network OE supports a JMS consumer.
- The connection protocol is handled by customer supplied software.
- **Low to High Guard**
  - Turnstile passes messages from the Low network to the High network only.
- **High to Low Guard**
  - Turnstile passes messages from the High network to the Low network only.
  - Turnstile sends an informational message to the high OE for each dropped OWG message.
  - The dropped message informational message contains the following information: Data message ID, time stamp, reason for failure.

OWG Characteristics (cont'd.)

- **OWG Performance**
  - Turnstile is able to accept, process and send data messages that are 1KB or less in size with a maximum latency of 40ms, not including processing time for any system integrator provided applications executing on the OEs.
  - Turnstile is able to accept, process and send data messages that are 20KB or less in size with a maximum latency of 80ms, not including processing time for any system integrator provided applications executing on the OEs.

Turnstile ACL’s

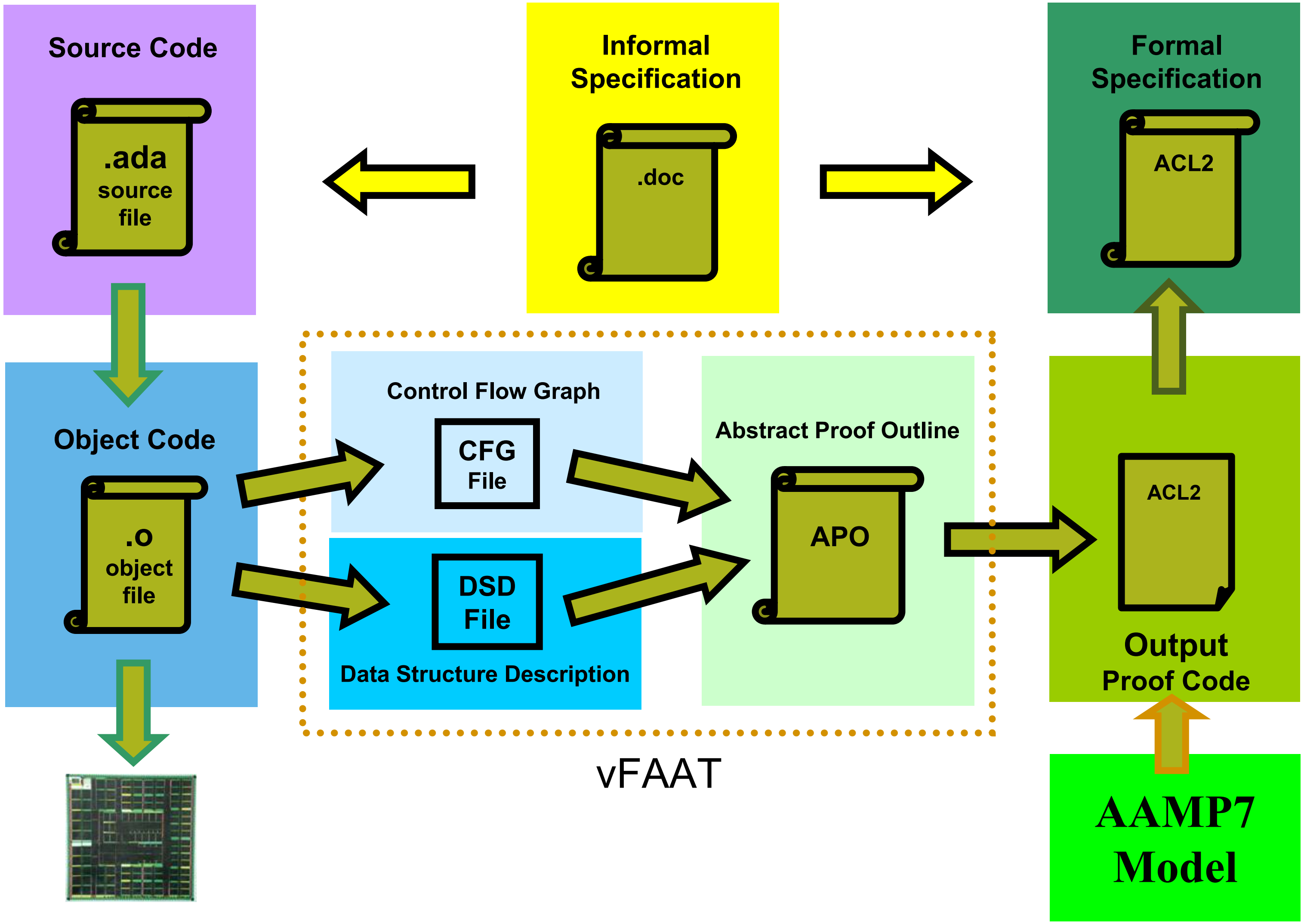
- Conform to the Common Information Sharing Standard for Information Security Marking (CISS-ISM)
  - Turnstile processes ACL’s based on at least the following CISS-ISM tags: classification, disseminationControls, and releasableTo
- A Turnstile ACL consists of a destination specifier, and a matching rule for messages for that destination
- Turnstile matching rules are comprised of the following operators on tag values: AND, OR, NOT, EQUAL, CONTAINS
- Example: Top Secret messages releasable to Australia

```
AND
  EQUAL classification TS
  AND
    CONTAINS disseminationControls REL
    CONTAINS releasableTo AUS
```

Two-Way Guard (TWG) Characteristics

- The guard engine supports two distinct sets of ACLs: one for low-to-high messages and the other for high-to-low messages.
- The high and low OEs each support a JMS consumer and producer.
- Turnstile sends an informational message to the high OE for every dropped TWG data message being transmitted from high to low.
- The dropped message informational message contains the following information: Data message ID, time stamp, reason for failure.
- TWG Performance
  - Turnstile is able to accept, process and send 1 KB data messages with a maximum latency of 40 msec, in both directions, not including processing time for any system integrator provided applications executing on the OEs.

Guard Verification: vFaat Formal Code Proofs



Source Code

.ada source file

Informal Specification

.doc

Formal Specification

ACL2

Object Code

.o object file

Control Flow Graph

CFG File

DSD File

Data Structure Description

Abstract Proof Outline

APO

ACL2

Output Proof Code

vFAAT

AAMP7 Model

Formal Specification

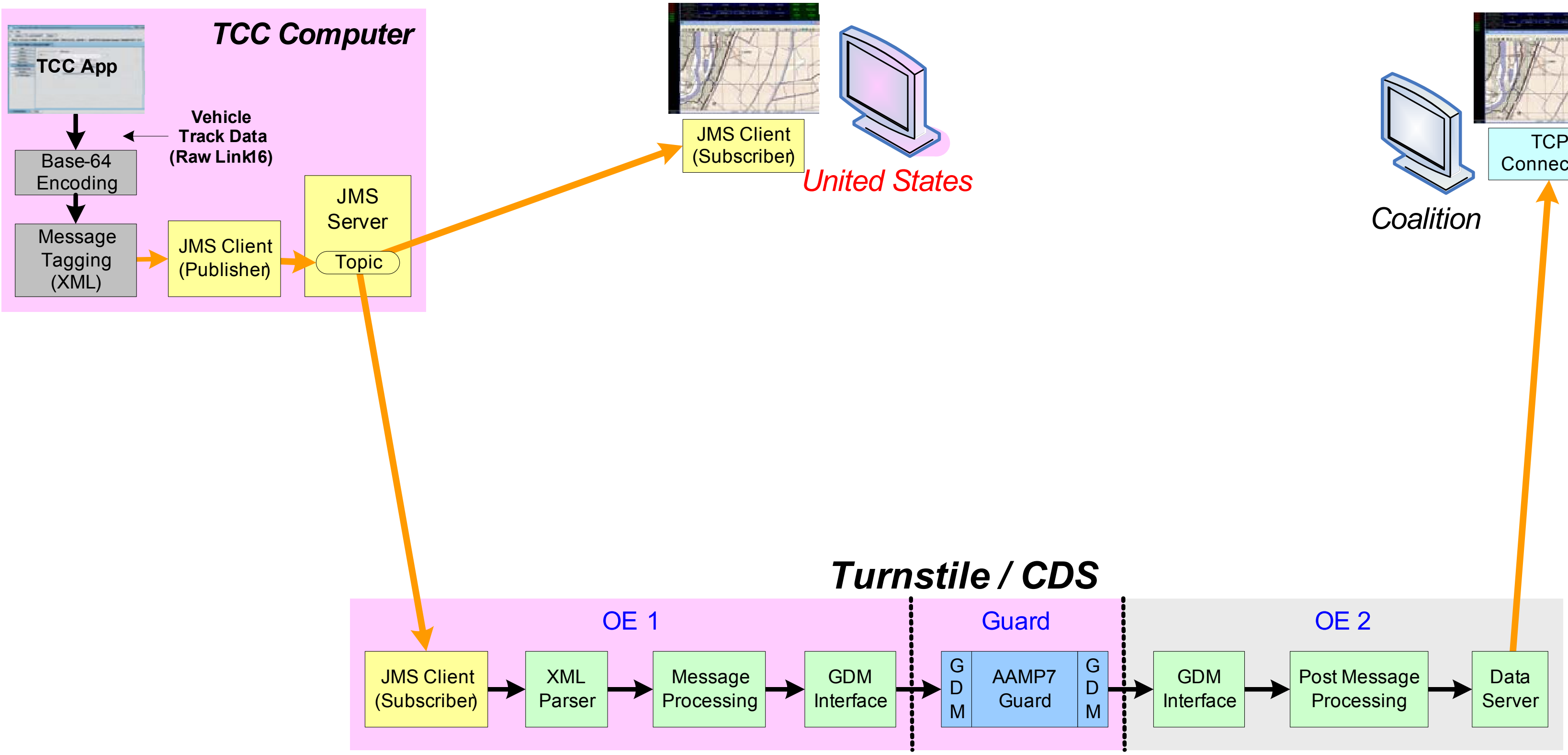
```
(defun acl-eval (acl msg)
 (if (atom acl) (if (equal acl :true) (acl-true) (undefined))
   (let ((op (car acl)))
     (cond
      ((null op) (false))
      ((equal op :and)
              (acl-and (acl-eval (arg 1 acl) msg) (acl-eval (arg 2 acl) msg)))
      ((equal op :or)
              (acl-or (acl-eval (arg 1 acl) msg) (acl-eval (arg 2 acl) msg)))
      ((equal op :not)
              (acl-not (acl-eval (arg 1 acl) msg)))
      ((equal op :equal)
              (if (bag::memberp (arg 1 acl) (toc msg))
                     (acl-equal (field-ref (arg 1 acl) msg) (arg 2 acl))
                   (undefined)))
      ((equal op :contains)
              (if (bag::memberp (arg 1 acl) (toc msg))
                     (acl-contains (field-ref* (arg 1 acl) msg) (arg 2 acl))
                   (undefined)))
      …))))
```

- Executable
- Maps to Informal Specification

Verification

- Functional Verification
  - The code implements the specification
- Precondition Elaboration
  - Standard “Frame Conditions”
    - Stack and Code don’t overlap
    - Stack is sufficiently large
  - Additional Low-Level Restrictions
    - AAMP Instruction Semantics are Preserved
    - Data Structures fit nicely into memory
  - Additional High-Level Constraints
    - Fed back into SPARK examiner

Demo Software Diagram



TCC Computer

TCC App

Vehicle Track Data (Raw Link16)

Base-64 Encoding

Message Tagging (XML)

JMS Client (Publisher)

JMS Server

Topic

JMS Client (Subscriber)

United States

TCP Connection

Coalition

Turnstile / CDS

OE 1

Guard

OE 2

JMS Client (Subscriber)

XML Parser

Message Processing

GDM Interface

G D M

AAMP7 Guard

G D M

GDM Interface

Post Message Processing

Data Server

Summary

Rockwell Collins' Turnstile cross domain platform is

- Accreditable to DCID 6/3 PL-5
- Compact
- Affordable
- Fast
- Flexible

Turnstile's architecture leverages the NSA MILS-certified AAMP7G microprocessor to minimize that which needs to be trusted in the guard.

Turnstile provides a very flexible cross-domain platform, with designed-in audit and self-test capability.

Current use cases include one-way and two-way guards.