Fault Tolerant Technology

MULTI DOMAIN
ARINC 653
AGENDA

- ARINC 653 Review
- Computer Architecture
- Malware
- Fault Tolerance
- Performance
ARINC 653

Operating System for the IMA

APplication EXecutive (APEX)

Spatial and Temporal Partitions

Health Monitor & Recovery
DRAWBACKS ARINC 653

- CPU overhead
- Complete partition failures
- Malware vulnerabilities
Virtual systems are not immune to malware, despite what some people may believe.

Symantec
ANDROID APP GAINS CONTROL INSIDE AN AIRPLANE

“It does not work on certified flight hardware”
FAA & EASA
Android malware spread to the planes only because employees were charging their phones with the USB port in the cockpit.

Mikko Hypponen
UNITED 737/800 HACKED

PASS OXYGEN ON anyone?
- Chris Roberts
MULTI DOMAIN ARCHITECTURE

DID (How)

PAD (When)

PAD (Where)
HARDWARE VIEW

Single Domain

CPU
Memory Controller

APEX
Kernel
Application Partition 1
Application Partition 2
Application Partition 3
Application Partition 4
I/O

Multiple Domain

CPU
Memory Controller

I/O
Kernel
APEX

Application Partition 1
Application Partition 2
Application Partition 3
Application Partition 4
I/O

single-domain diagram

multiple-domain diagram
FEATURE COMPARISON

Single Domain

1. Detects Viruses
2. CPU Overhead

Multiple Domain

1. Prevents Viruses
2. No CPU Overhead
Containers respond 7x faster
CLOUDY PERFORMANCE: STEADY STATE PACKING

**Docker: Compute Node Steady-State CPU (segment: 31s – 243s)**

- CPU Usage in Percent
- Averages: 0.2, 0.03
- Time (31s – 243s)
- usr, sys
- 31 seconds, 243 seconds

**KVM: Compute Node Steady-State CPU (segment: 95s – 307s)**

- CPU Usage in Percent
- Averages: 1.91, 0.36
- Time (95s – 307s)
- usr, sys
- 95 seconds, 307 seconds
CLOUDY PERFORMANCE: STEADY STATE PACKING

Docker / KVM: Compute Node Used Memory (Overlay)

- **Docker**
  - Delta: 734 MB
  - Per VM: 49 MB

- **KVM**
  - Delta: 4387 MB
  - Per VM: 292 MB

Memory Used

Axis Title

Graph showing the memory usage comparison between Docker and KVM.
HARDWARE VIEW

Single Domain

- CPU
- Memory Controller
- Application Partition 1
- Application Partition 2
- Application Partition 3
- Application Partition 4
- APEX
- Kernel
- I/O

Multiple Domain

- CPU
- Memory Controller
- Application Partition 1
- Application Partition 2
- Application Partition 3
- Application Partition 4
- APEX
- Kernel
- I/O
- Application Partition 1
- Application Partition 2
- Application Partition 3
- Application Partition 4
- I/O
ARINC 653

Multi Domain Architecture

- Near bare metal performance in the guest
- Fast network operation
- Reduced resource consumption (CPU, MEM) on the compute node
FEATURE COMPARISON

Single Domain

1. Detects Viruses
2. CPU Overhead
3. Partition Failure

Multiple Domain

1. Prevents Viruses
2. No CPU Overhead
3. Component Failure
# ARINC 653

<table>
<thead>
<tr>
<th>Single Domain</th>
<th>Multiple Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; Hardware</td>
<td>&gt; Hardware</td>
</tr>
<tr>
<td>- Partition Level</td>
<td>- Component Level</td>
</tr>
<tr>
<td>&gt; Sensor</td>
<td>&gt; CPU</td>
</tr>
<tr>
<td>&gt; PUF Definition</td>
<td>&gt; Component</td>
</tr>
<tr>
<td></td>
<td>&gt; Sensor</td>
</tr>
<tr>
<td></td>
<td>&gt; Virus Prevention</td>
</tr>
</tbody>
</table>
## ARINC 653

<table>
<thead>
<tr>
<th>Single Domain</th>
<th>Multiple Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Software</td>
<td>▶ Software</td>
</tr>
<tr>
<td>▶ Partition Level</td>
<td>▶ Thread Level</td>
</tr>
<tr>
<td>▶ Stateless Recovery</td>
<td>▶ State Recovery</td>
</tr>
<tr>
<td>-</td>
<td>▶ Forensic Analysis</td>
</tr>
<tr>
<td>▶ Detects Viruses</td>
<td>▶ Prevents Viruses</td>
</tr>
</tbody>
</table>
MULTI DOMAIN ARCHITECTURE

Meets ARINC 653 APEX standards

Container Performance

VM versatility

Prevents Malware
Fault Tolerant Technology

THANK YOU