Международная конференция

Состояние и перспективы развития интегрированной модульной авионики

MASIw:
Model Based Toolset for IMA System Design and Integration

Alexey Khoroshilov (ISPRAS)

Москва, 29-30 октября 2012 г.
What is MASiW

- Model-based toolset aimed to automate IMA System Group (IMA-SG) activities

- IMA-SG is responsible for:
  - IMA System Design
  - IMA System Integration
  - IMA System Verification
  - Coordination of Platform Component Suppliers (PCS) and ATA-XX developers
  - IMA System Certification
IMA System

CPM
ARINC-653 RTOS Drivers

Mezzanines:
- GPU
- Mass Storage
- ...
IMA System

CPM1
ARINC-653 RTOS
Drivers

Mezzanines:
- GPU
- Mass Storage
- ...

PCI

AFDX switch

ARINC-664 (AFDX) Network

CPM2
ARINC-653 RTOS
Drivers
IMA System

CPM1
ARINC-653 RTOS Drivers

CPM2
ARINC-653 RTOS Drivers

Mezzanines:
- GPU
- Mass Storage
- ... (not specified)

AFDX switch

Data Concentrator

Remote Data Concentrator

Middleware:
- I/O routing
- ARINC-615A
- BITE
- Instrumentation

ARINC-825

ARINC-664 (AFDX) Network

PCI
IMA System

CPM1
ARINC-653 RTOS
Drivers

CPM2
ARINC-653 RTOS
Drivers

Data
Concentrator

Remote Data
Concentrator

AFDX
switch

Mezzanines:

GPU
Mass Storage
...

ARINC-664
(AFDC) Network

IMA Platform

ATA-21 SW1
ATA-31 SW
ATA-21 SW2
ATA-22 SW1
ATA-22 SW2
ATA-23 SW1
ATA-23 SW2

Data
Concentrator

ARINC-825

Sensor-211
Actuator-211
Sensor-212
Actuator-212
Sensor-221
Actuator-221
Sensor-222
Actuator-222
Actuator-231

ARINC-825 SW
ATA-21 SW
ATA-22 SW
ATA-23 SW

IMA-SG

- Model-based toolset aimed to automate IMA System Group (IMA-SG) activities

IMA-SG is responsible for:

- IMA System Design
- IMA System Integration
- IMA System Verification
- Coordination of Platform Component Suppliers (PCS) and ATA-XX developers
- IMA System Certification
IMA-SG is responsible for:

- IMA System Design
Top level A/C requirements:
- segregation
- power limitations
- spatial limitations
- etc.

IMA design standard:
- max processor load for initial design
- max bus load for initial design
- etc.
(2) Platform Components Stream

CPM1
ARINC-653 RTOS
Drivers

Mezzanines:
- GPU
- Mass Storage
- ...

AFDX switch

Data Concentrator

Remote Data Concentrator

Middleware:
- I/O routing
- ARINC-615A
- BITE
- Instrumentation

Platform components characteristics:
- performance
- memory
- I/O bandwidth
- power consumption
- etc.

Configuration variability

Usage domain rules
(3) ATA-XX Stream

- ATA-21
- ATA-22
- ATA-23
- ATA-31
- ATA-41
(3) ATA-XX Stream

- ATA-21
- ATA-22
- ATA-23
- ATA-31
- ATA-41

IMA Platform

out of IMA
(3) ATA-XX Stream
(3) ATA-XX Stream

ATA-41

ATA-21
ATA-21 SW1
ATA-21 SW2

ATA-31
ATA-31 SW

ATA-23
ATA-23 SW1
ATA-23 SW2

ATA-22
ATA-22 SW1
ATA-22 SW2

Sensor-211
Actuator-211
Sensor-212
Actuator-212
Sensor-221
Actuator-221
Sensor-222
Actuator-231
(3) ATA-XX Stream

Software partition reqs:
- period and duration
- memory needs
(3) ATA-XX Stream

Software partition reqs:
- period and duration
- memory needs

Communication reqs:
- bandwidth
- latency

ATA-41
ATA-21 SW1
ATA-21 SW2
ATA-21
ATA-31
ATA-31 SW
ATA-22
ATA-22 SW1
ATA-22 SW2
ATA-23
ATA-23 SW1
ATA-23 SW2
ATA-22
ATA-23
ATA-31
ATA-41

Sensor-211
Actuator-211
Sensor-212
Actuator-212
Sensor-221
Actuator-221
Sensor-222
Actuator-231
IMA System Design

(1) A/C Stream
- Top level A/C requirements:
  - Segregation
  - Power limitations
  - Spatial limitations
  - Etc.
- IMA design standards:
  - Mass processor load for initial design
  - Mass bus load for initial design
  - Etc.

(2) Platform Components Stream
- Middleware:
  - Avionics
  - ARINC-429
  - ARINC-664

- Platform component characteristics:
  - Performance
  - Memory
  - I/O bandwidth
  - Etc.

- Configuration variability
- Usage domain rules

(3) ATA-XX Stream
- Configuration:
  - Software partitioning
    - Special and duration
    - Memory needs

IMA System Designer
IMA System Design

Top level A/C requirements:
- segregation
- power limitations
- spatial limitations
- etc.

IMA design standard:
- max processor load for initial design
- max bus load for initial design
- etc.

Communication reqs:
- bandwidth
- latency

Software partition reqs:
- period and duration
- memory needs

Platform components characteristics:
- performance
- memory
- I/O bandwidth
- power consumption
- etc.

Configuration variability

Usage domain rules
IMA System Design

Top level A/C requirements:
• segregation
• power limitations
• spatial limitations
• etc.

IMA design standard:
• max processor load for initial design
• max bus load for initial design
• etc.

Communication reqs:
• bandwidth
• latency

Platform components characteristics:
• performance
• memory
• I/O bandwidth
• power consumption
• etc.

Software partition reqs:
• period and duration
• memory needs

Several design alternatives

Sensor-211
Actuator-211
Sensor-221
Actuator-221
Sensor-222
Actuator-231
Sensor-212
Actuator-212
Actuator-221
IMA System Design

Top level A/C requirements:
- segregation
- power limitations
- spatial limitations
- etc.

Software partition reqs:
- period and duration
- memory needs

IME design standard:
- max processor load for initial design
- max bus load for initial design
- etc.

Platform components characteristics:
- performance
- memory
- I/O bandwidth
- power consumption
- etc.

Communication reqs:
- bandwidth
- latency

IMA Platform

Configuration variability

Usage domain rules

Several design alternatives

And input data are not final => Change request processing
IMA System Design

(1) A/C Stream
- Top level A/C requirements:
  - segregation
  - power limitations
  - spatial limitations
  - etc.
  - IMA design standards
    - max processor load for initial design
    - max bus load for initial design
    - etc.

(2) Platform Components Stream
- CPM1, ARINC-429, RTOS Drives
- Mezzanines
- Processor
- Mass Storage
- AFAX switch
- Data Concentrator
- Remote Data Concentrator
- Middleware:
  - V0 routing
  - ARINC-815A
  - IMA instrumentation
- Platform components characteristics:
  - performance
  - memory
  - I/O bandwidth
  - etc.
- Configuration variability
- Usage domain rules

(3) ATA-XX Stream
- ATA-41
- ATA-31
- ATA-21
- ATA-22
- ATA-23
- ATA-31 SW
- ATA-21 SW
- ATA-22 SW
- ATA-23 SW
- Software partition requirements and duration

IMA System Designer

- Design Documents
- Safety Analysis Report
- Verification Report
MASIW is a model-based toolset based on Architecture Analysis & Design Language

- Architecture model
  - structural model
  - flows specification
  - software to hardware mapping
- extensible via properties and annexes
- constraints specification
- textual notation
- international standard: SAE AS5506A
Main features of MASIW-2012:

- modeling of IMA architecture from system-level specification down to implementation details of hardware and software components
AADL Model
AADL Model
AADL Model
Main features of MASIW-2012:

- modeling of IMA architecture from system-level specification down to implementation details of hardware and software components
- verification of resource allocation consistency, usage domain rules and project-specific constraints
REAL Constraints Checker

Requirement Enforcement Analysis Language

```plaintext
theorem scheduling_major_frame
foreach cpu in processor_set do
  check
    ((not property_exists
        (cpu,"ARINC653::Module_Major_Frame"))
    or (float (property (cpu,
        "ARINC653::Module_Major_Frame"))) >=
    sum (property (cpu,
        "ARINC653::Partition_Slots")))
end scheduling_major_frame;
```
Theorem REQUIRED_SIZE_MEMORY_PROPERTIES

Description:
Each memory component must have "VxWorks653::MemorySize" property.

<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Verification status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUPD.impl.address_space.sram.userMemory.alloc_cons</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.kernelMemory</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.nor</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space</td>
<td>MemoryInstance</td>
<td>FAILED</td>
<td>Memory MUPD.impl.address_space doesn't have &quot;VxWorks653::MemorySize&quot; property.</td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.hardware</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.eeprom12</td>
<td>MemoryInstance</td>
<td>FAILED</td>
<td>Memory MUPD.impl.address_space.eeprom12 doesn't have &quot;VxWorks653::MemorySize&quot; property.</td>
</tr>
<tr>
<td>MUPD.impl.address_space.kernelIO2</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.pex_io</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.utrc_buffer</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.kernelConfigRecord</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.userMemory.afdx_code</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.userMemory.afdx_io</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.eeprom34</td>
<td>MemoryInstance</td>
<td>FAILED</td>
<td>Memory MUPD.impl.address_space.eeprom34 doesn't have &quot;VxWorks653::MemorySize&quot; property.</td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.hmLog</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.portRegion</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.sram.userMemory</td>
<td>MemoryInstance</td>
<td>PASSED</td>
<td></td>
</tr>
<tr>
<td>MUPD.impl.address_space.nand</td>
<td>MemoryInstance</td>
<td>FAILED</td>
<td>Memory MUPD.impl.address_space.nand doesn't have &quot;VxWorks653::MemorySize&quot; property.</td>
</tr>
</tbody>
</table>

Theorem IO_SYS
Main features of MASIW-2012:

- modeling of IMA architecture from system-level specification down to implementation details of hardware and software components
- verification of resource allocation consistency, usage domain rules and project-specific constraints
- static schedule building for periodic ARINC-653 partitions and specialized middleware tasks
Pluggable scheduling algorithms
- Early Deadline First
- Rate Monotonic
- Custom limitations
- Special processing of middleware partitions and I/O device drivers
Main features of MASIW-2012:

- modeling of IMA architecture from system-level specification down to implementation details of hardware and software components
- verification of resource allocation consistency, usage domain rules and project-specific constraints
- static schedule building for periodic ARINC-653 partitions and specialized middleware tasks
- AFDX static analysis and simulation framework
Characteristics to be evaluated:

- Latency
- Time and reasons of delays
- Distribution of queues length
- Probability of message loses
IMA System Integration

- IMA-SG is responsible for:
  - IMA System Design
  - IMA System Integration
CPM Configuration

Module Configuration (MC)

Partition Global Config (PGC)

Partition Local Config (PLC)

ATA-XX Partition

Partition level config

Module level config

Responsibility of ATA-XX developer

Responsibility of IMA-SG

PLC includes
- partition-level HM;
- memory layout details;
- etc.

MW RTOS drivers

MW RTOS drivers
Main features of MASIW-2012:

- Modeling of IMA architecture from system-level specification down to implementation details of hardware and software components.
- Verification of resource allocation consistency, usage domain rules and project-specific constraints.
- Static schedule building for periodic ARINC-653 partitions and specialized middleware tasks.
- AFDX static analysis and simulation framework.
- Generation of configuration tables for VxWorks-653 RTOS and AFDX network elements.
Configuration Generation

<CoreOSDescription
  xmlns="http://www.windriver.com/vxWorks653/ConfigRecord"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.windriver.com/vxWorks653/ConfigRecord..\xml\cleanschema\CoreOS.xsd"
  KernelName="coreOS">
  <KernelConfiguration
    sysClkBaseHz="4000"
    unsafeMethodTimeout="0.5"
    memoryAllocationDisabled="false"
    watchdogTimerDuration="0"
    partitionVirtualAddress="0x40000000"
    kernelVirtualAddress="0x00100000"
    addressSpaceSize="0xFFFFFFFF"
    addressSpaceRegionAllocationUnit="0x10000000"/>

  <MemorySize MemorySizeBase="0x00000000"
    MemorySizeData="0x00000000"
    MemorySizeRoData="0x00000000"
    MemorySizeText="0x00000000"/>

  <HardwareConfiguration>
    <PhysicalMemory Size="0x1E000000" Base_Address="0">
      <kernelMemoryRegion Size="0x05000000"/>
      <kernelConfigRecordRegion Size="0x00010000"/>
      <portRegion Size="0x00020000"/>
      <hmLogRegion Size="0x00010000"/>
      <kernelRegion Size="0x00040000" PoolName="kr_hello1" WriteProtected="false"/>
      <kernelRegion Size="0x00040000" PoolName="kr_hello2" WriteProtected="false"/>
      <userConfigRecordRegion Size="0x00010000" Base_Address="0x64000000" Name="userCfgRgn"/>
      <raceMemoryRegion Size="0x00040000" Base_Address="0x65000000"/>
      <userMemoryRegion Size="0x17000000" Base_Address="0x67000000"/>
    </PhysicalMemory> 

    <!-- Region for utrc buffer -->
    <shared10 PoolName="utrc_buffer" Size="0x00200000" Base_Address="0x6E000000"/>
    <shared10 PoolName="alloc_cons" Size="0x02000000" Base_Address="0x1E000000"/>
    <shared10 PoolName="kernel102" Size="0x70000000" Base_Address="0x80000000"/>
    <shared10 PoolName="PHX-io" Size="0x00020000" Base_Address="0xF0000000"/>
    <sys controller base address -->
    <shared10 PoolName="hardware" Size="0x04000000" Base_Address="0xF8000000"/>
    <flash (SDRAM) base address -->
    <kernel10 PoolName="nor flash" Size="0x04000000" Base_Address="0xFC000000" VirtualAddress="0xFC000000"/>
  </HardwareConfiguration>

<Schedule Id="0">
  <PartitionWindow
    PartitionNameRef="Function_Prec"
    Duration="1000"
    ReleasePoint="true"/>

  <PartitionWindow
    PartitionNameRef="Function_Art"
    Duration="2000"
    ReleasePoint="true"/>

  <PartitionWindow
    PartitionNameRef="Function_Art"
    Duration="1000"
    ReleasePoint="true"/>

  <PartitionWindow
    PartitionNameRef="Function_Art"
    Duration="1000"
    ReleasePoint="true"/>

  <PartitionWindow
    PartitionNameRef="Function_Art"
    Duration="12000"
    ReleasePoint="true"/>

  </PartitionWindow>
</Schedule>
Future Works

- Usability improvements
- Architecture model – design documents integration
- Platform components architecture models library
- Requirements traceability
- Safety analysis
- Certification considerations
Thank you!

Alexey Khoroshilov
khoroshilov@ispras.ru