Développer dans les systèmes embarqués critiques

Luc COYETTE
Bordeaux – July 1st, 2015
Agenda

• Embedded Software Characteristics

• Embedded Software Development

• Examples

• Summary
Embedded Software Characteristics
Embedded Software

Example of Flight Control Software

Control Flow

Data Flow

Sensors

Actuators
Embedded Software

Example of interactive GUI Application

Primary Flight Displays

Automotive Dashboards

UAV Ground Stations

Medical Displays
Embedded Software

SCADE Addresses the Applicative part
Embedded Software Development
SCADE System
System development phase

Operational Analysis

User Requirements

System Requirements

Software Requirements

Supports

Traceability

System Design

System Functions

System Architecture

Allocation

Synchronization
(detailed interfaces)

Software Design
SCADE Suite for Software Design

- Control Software Engineering:
  - Formally defined language
  - Created for HQ SW design
Architecture and LLRs in a SCADE Model

Architecture

LLRs

FlightController

throttleCmd

elevatorCmd

AlarmManager

JV_Speed_Alarm

JV_Alti_Alarm

<FlightMode>

AUTOPILOT

SpeedTarget = (speed) -> ( last 'SpeedTarget);

AltitudeTarget = (altitude) -> ( last 'AltitudeTarget);

MANUAL

SpeedTarget = (speed) /

AltitudeTarget = (altitude) -> ( last 'AltitudeTarget);

not AutoPilot

MCPspeed

MCPaltitude

UnitConvert KTtoKMH

UnitConvert FTtoM

SpeedTarget

AltitudeTarget
No global variable, no pointer, no side effect

No other data/control coupling means than explicit connexion

-- Formal interface
define node Integrator (U : real ; TimeCycle : real) returns (Y : real);

-- Local variables
var
delta : real;
last_Y : real;

-- Equations
let
delta = u * TimeCycle;
y = delta + last_Y;
last_Y = fby (y, 1, 0.0);
tel
**Rigorous Initialization Checks**

**pre**: delay one cycle

\[ y = az^{-1}x \rightarrow y = a \times \text{pre}(x) \]

\[ \rightarrow\text{: data flow initial value} \]

ERROR: NODE Count, VAR Counter,
The operator "pre" expects a well–initialized argument

Translation completed with
0 semantic error(s),
0 semantic warning(s).
Requirements to SCADE Models Traceability

Using the SCADE Requirements Management Gateway
void Button_ABC_N(inC_Button_ABC_N *inC, outC_Button_ABC_N *outC) {
    /* ABC_N::Button::SM1::SSM_SM1_dispatch_sel */
    SSM_Button_SM1_ST SSM_SM1_dispatch_sel = SSM_SM1_Unselected__ABC_N;
    if (outC->init) {
        outC->init = kcg_false;
        SSM_SM1_dispatch_sel = SSM_SM1_Unselected__ABC_N;
    } else {
        SSM_SM1_dispatch_sel = outC->M_pre_;
    }
    switch (SSM_SM1_dispatch_sel) {
    case SSM_SM1_Locked__ABC_N :
        outC->foreground = white_ABC_N;
        outC->background = green_ABC_N;
        if (inC->Unlock) {
            outC->M_pre_ = SSM_SM1_Preselected__ABC_N;
        } else {
            outC->M_pre_ = SSM_SM1_Locked__ABC_N;
        }
        break;
    case SSM_SM1_WaitUnlock__ABC_N :
        outC->foreground = black_ABC_N;
        outC->background = grey_ABC_N;
        if (inC->Unlock) {
            outC->M_pre_ = SSM_SM1_Unselected__ABC_N;
        } else {
            outC->M_pre_ = SSM_SM1_WaitUnlock__ABC_N;
        }
        break;
    [...]
}
Qualified Code Generation

• All functional safety standards have one goal:

SOFTWARE QUALITY

• SCADE Suite provides one Certified Code Generator for DO-178C at level A (aeronautics), as well for IEC 61508 at SIL 3 (industry), ISO 26262 at ASIL D (automotive), EN 50128 (railways), IEC 60880 (nuclear), ISO 62304 (medical).

• Approved & certified/qualified by more than 10 authorities worldwide
SCADE Test V&V

- No unit tests
- Test coverage on model level
- Certified verification tools:
  - MTC Model Test Coverage
  - Model Reporter
  - Test execution (host, ECU)
Executable Specification

Unique Collaboration Capabilities

Developers & Product Managers

Customers

Suppliers

Partners
Examples

Fluids  Structures  Electronics  Systems
SCADE Suite @ Cassidian

Program:
• EADS Cassidian BARRACUDA UAV

Application: Embedded Flight Control Software
• DO-178B Level A Certified

Results:
• Full code generation of the application from SCADE
SCADE Display @ XMobots

Program
  • Nauru 500A Series UAV

Application:
  • GCS-S19A & GCS-S10A
    Ground Control Stations

Results:
  • Saved money (development time, hardware, and higher quality SW)
  • More robust and reliable software
  • Better development process
  • Focus on model and not in the code
  • Ease of change and maintenance tasks

Plans to use SCADE Suite for UAV Flight Controls
Summary
A Complete SCADE-Based SW Life Cycle

System Development Phase

Software Requirement Phase

Software Architecture Phase

Software Design Phase

Software Implementation Phase

Software Testing Preparation Phase

Software Testing Phase

Software Integration Phase

Software Validation Phase

Software Maintenance Phase
What Is Unique About SCADE?

- SCADE products and solutions are developed specifically to address critical system and software applications.
- SCADE Suite and Display code generators are certifiable according to the following international safety standards:
  - DO-178B / DO-178C qualification up to Level A – A&D
  - IEC 61508 certification up to SIL 3 – Industrial & Energy
    - IEC 60880 full compliance – Nuclear Instrumentation & Control
    - IEC 62304 full compliance – Medical Systems
    - EN 13849 full compliance – Industrial Machines Safety
  - EN 50128 certification up to SIL 3/4 – Rail Transportation
  - ISO 26262 certification up to ASIL D – Automotive
- Same products qualified at the highest level of safety across 6 market segments by 10 safety authorities, worldwide.
### SCADE Benefits Summary

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Development Process Improvements</strong></td>
<td>SCADE enables Best Practices for:</td>
</tr>
<tr>
<td></td>
<td>• Model-Based Systems Engineering</td>
</tr>
<tr>
<td></td>
<td>• Integrated Multi-physics and Software Simulation</td>
</tr>
<tr>
<td></td>
<td>• Embedded Controls development</td>
</tr>
<tr>
<td></td>
<td>• Interactive Displays development</td>
</tr>
<tr>
<td><strong>Development Costs Reduction</strong></td>
<td>50% Development Costs Reduction</td>
</tr>
<tr>
<td><strong>Time-to-Certification Speed up</strong></td>
<td>2X Time-to-Certification Speed up</td>
</tr>
</tbody>
</table>
Questions?

scade-academics@ansys.com