Enabling Requirements Engineering for Real-Time Critical Systems with Rational DOORS and INCHRON Tool-Suite

Uwe Brodtmann, CEO INCHRON

June 6, 2013
INCHRON GmbH

Company History

1996: Start of fundamental research
2003: INCHRON founded
2006: Investment from Hasso Plattner Ventures
2009: Premium Member AUTOSAR
2011: Global Reseller Agreement IBM Rational

Partners

Customers

Memberships
Timing Requirements – from Different Views

- Real-Time Requirement of vehicle function
- Real-Time Requirement of control algorithm
- Performing SW-components

⇒ Detailed definition of timing requirements
⇒ consideration of all involved components
A V-model perspective on timing

**Specification**
- Signal detection
- Pre-processing
- Object Verification
- Tracking
- Decision
- Braking

**Design**
- Signal detection
- Pre-processing
- Object Verification
- Tracking
- Decision
- Braking

**Implementation**
- Timing Requirement: $\Delta t \leq 300 \text{ ms}$

**Integration & Test**
- Detection of timing errors

**Timing Requirement:** $\Delta t \leq 300 \text{ ms}$
Levels in E/E-Systems
E/E-System for a Driver Assistance System
E/E-System – Multiple Suppliers
Function Network

Timing Requirement: $\Delta t \leq 300$ ms

Vehicle Movement

Signal detection
Pre-processing
Tracking
Object Verification
Decision
Braking
Vehicle Movement
Event Chain in E/E-System

- Signal detection
- Pre-processing
- Object Verification
- Tracking
- Decision
- Braking
- Vehicle Movement

Timing Requirement: $\Delta t \leq 300$ ms
Limited System View of OEM
Limited System View of Tier 1

\[ \Delta t \leq 250 \text{ ms} \]

\[ \Delta t \leq 50 \text{ ms} \]
Multiple Suppliers of SW Components
Event Chain on Time Axis
Tier 1: Event Chain Evaluation
Tier 1: Event Chain Evaluation
Tier 1: Event Chain Evaluation

Timing Requirement: $\Delta t \leq 250$ ms – Failed!

Event chain broken
Data lost
Tier 1: Event Chain Evaluation

- Preemption by other task
- Clock drift and delayed by other task
Event Chain Evaluation – End-to-End
Timing Model of Dynamic System Behavior
System Architecture and Requirements

Real-Time Data Sheet
- CPU and Bus Load
- Event Chain Latencies
- Event Chain Synchronization
- Signal Rate, Loss or Age
- Runnable's Response Time
- Runnable's Execution Rate and Order
- Runnable's Activation Condition
- IRQ's Loss or Blocking

Timing-Model

Real-Time Data Sheet
- CPU and Bus Load
- Event Chain Latencies
- Event Chain Synchronization
- Signal Rate, Loss or Age
- Runnable's Response Time
- Runnable's Execution Rate and Order
- Runnable's Activation Condition
- IRQ's Loss or Blocking

Requirements Table
- Group General
  - Recursion limited to 0
  - No RTOS errors allowed
- Group Event Chains
  - Event Chain EC_Segment02
  - Event Chain EV_Segment03
- Group Response Times
  - Response Time act1_100ms
  - Response Time act1_50ms
  - Response Time act1_T_R0T
  - Response Time act1_10ms
  - Response Time act1_20ms
  - Response Time act1_15ms
  - Response Time act1_120ms
  - Response Time act1_10ms

Add... Help Delete
Real-Time Data Sheet in Early Design Phase

- CPU and Bus Load
- Event Chain Latencies
- Event Chain Synchronisation
- Signal Rate, Loss or Age
- Runnable’s Response Time
- Runnable’s Execution Rate and Order
- Runnable’s Activation Condition
- IRQ’s Loss or Blocking

Timing-Model

OEM
Continuous Integration and Test
Continuous Integration and Test

Real-Time Data Sheet
- CPU and Bus Load
- Event Chain Latencies
- Event Chain Synchronization
- Signal Rate, Loss or Age
- Runnable's Response Time
- Runnable's Execution Rate and Order
- Runnable's Activation Condition
- IRQ’s Loss or Blocking

Timing-Model
A V-model perspective on timing

Timing Requirement: $\Delta t \leq 300$ ms

Specification

Model-based analysis and simulation

Design

Integration & Test

Implementation

Signal detection
Pre-processing
Object Verification
Tracking
Decision
Braking

Detection of timing errors

Signal detection
Pre-processing
Object Verification
Tracking
Decision
Braking

Timing Requirement: $\Delta t \leq 300$ ms

Implementation
Integration: Rhapsody – chronSIM – DOORS

System in UML

UML-Profile
+ SW/HW-Architecture
+ Execution Times
+ Stimulation

DOORS Req.

DOORS Data

Roundtrip to DOORS

Requirement Status

Dynamic Behavior

Timing Model

T₀ → Tₘ
Integration: Rhapsody – chronSIM – DOORS

Modeling functional and dynamic behavior in Rhapsody
- One model – no consistency problems

Timing and performance analysis of dynamic architecture
- Sensitivity analysis on dynamic behavior
- What-if analysis for design alternatives
- Impact analysis for change requests

Managing functional and timing requirements in DOORS
- Improve product quality
- Evaluate requirements model based
Modeling External Stimulation

Flexible Stimulation Patterns for Tasks and ISRs
Modeling Tasks and ISRs

Definition of Tasks and ISRs

Scheduling Parameters
Modeling Functions and Net Exec. Times

Task Net Execution Times

Function Net Execution Times

Function Execution Order and Condition
Allocation of Tasks and IRQs to CPU Resources

HW Resources

Tasks and ISRs Allocation
Simulation of Dynamic Behavior

- Task Response Time Histogram
- Process State Diagram
- Process Timing Box-Plot
- CPU Load Diagram
Requirements Interchange via OSLC

- Read text based requirements from DOORS
- Add formal, technical requirements for timing and performance
Evaluate Requirements in Real-Time Simulation

- Requirement Histogram
- Bad and Good Cases
Requirements Interchange via OSLC

- Read text based requirements from DOORS
- Add formal, technical requirements for timing and performance
- Simulate, analyze and test
- Feed results back to DOORS
Real-Time Requirement Analysis

Requirements analysis live and in html-report

Html-Report
- Detailed summary of system timing
- Profile for each process, task, ISR
- Document with links and diagrams
- Statistics with histograms
Integration: Rhapsody – chronSIM – DOORS

- No entry hurdles
  - Import of OIL files, modeling in C
  - First usable results produced after only two days
- Very short turnaround times
- Total time effort for this project approx. 2 weeks

"The feasibility of such change requests can now be analyzed in 1/3 of the usual time. This saves time and money, allows fast feedback to the customer and gives more confidence in the modified system. “

- chronSIM is a valuable tool. Without, several problems fixed would still be present in our system today.
- It took us only 10 days of training and occasional consulting to get to a very high level of expertise
- Support from INCHRON has always been excellent.
- The tool was worth the investment.

„We have found errors already in simulation, that we would have found 12 months later in testing.“
For more information

- http://www.inchron.com
- http://www.youtube.com/watch?v=dzfn2-o7eqU
Daily Apple TV giveaway

- Complete your session surveys online each day at a conference kiosk or on your Innovate 2013 Portal!
- Each day that you complete all of that day’s session surveys, your name will be entered to win the daily Apple TV!
- On Wednesday be sure to complete your full conference evaluation to receive your free conference t-shirt!
Thank You!