Model-based Engineering of Cyber-physical Systems using AADL

Sandeep K. S. Gupta and Tridib Mukherjee

Impact Lab (http://impact.asu.edu)
School of Computing & Informatics
Arizona State University
Outline

- Cyber-Physical Systems (CPS)
- CPS Design Requirements – safety & survivability
- AADL modeling for safety analysis
- AADL modeling for survivability analysis
- Discussion – CPS annex requirements
Cyber Physical Systems (CPS)

- Dynamic distributed large-scale systems to monitor, coordinate, control, integrate and facilitate physical process
- Cyber and physical components are integrated
- Operations in computing entities affect the physical world & vice versa.

Key Issues
- Physical Interactions
- Critical Applications
- Automated Design & Validation
Design Decisions

Critical applications should be able to avoid/handle dangerous physical conditions (e.g. life/property losses).

Survivability

Safety

Interactions between physical and cyber components should not detrimentally impact the physical conditions.

Security

Reliability

Real-time

Quality

This talk specifically focuses on the safety & survivability issues.
Safety in CPS
Body Sensor Networks (BSN)

- Medical sensors implanted/worn by human for health-monitoring.

- **Interference** – sensor activity causes heating in the tissue.
  - Heating caused by RF inductive powering
  - Radiation from wireless communication
  - Power dissipation of circuitry

**Environmental Interference in BSN**

**Safety** – tissue temperature should be within a threshold value

Dense Computer Rooms
(i.e. Data centers, Computer Clusters, Data warehouses)

- Inlet should be within the red-line temperature to avoid equipment failure

Interference Modeling in AADL

- Two approaches used
  - Property sets
    - can model the interferences as property types of the components
  - Error model annex
    - can model the interferences in terms of error propagation

- Interference is modeled as the fraction of energy propagation.

- Component energy consumption depends on the which mode (state) the component is in.

- In the safety analysis, the actual energy propagation is calculated based on the interference and the component energy consumption.
Modeling Interference with Property Sets

system implementation Node.node1
modes
  idle: initial mode;
  Working: mode;
  idle-[e1]->Working;
properties
  Interference::inter =>(0.6, 0.4);
  Interference::nodes_name=>(“node2”, “node3”); end Node.node1;

system implementation Node.node3
modes
  idle: initial mode;
  Working: mode;
  idle-[e1]->Working;
properties
  Interference::inter =>(1.0);
  Interference::nodes_name =>(“node3”); end Node.node3;

property set Interference is
  inter: list of aadlreal applies to (all);
  nodes_name: list of aadlstring applies to (all);
end Interference;

..
Modeling Interference with Error Annex

```java
package Safety_Model
public
annex Error_Model {**
  error model Interference
  features
    Idle: initial error state;
    Working: error state;
    Start: error event {Occurrence => fixed p};
    SelfInt: in out error propagation {Occurrence =>
      fixed 0.0};
    Node1Int: in out error propagation {Occurrence =>
      fixed 0.0};
    Node2Int: in out error propagation {Occurrence =>
      fixed 0.0};
    Node3Int: in out error propagation {Occurrence =>
      fixed 0.0};
  end Interference;

  error model implementation Interference.node1
  transitions
    Idle-[out node2Int]-->Idle;
    Idle-[out node3Int]-->Idle;
    Working-[out node2Int]-->Working;
    Working-[out node3Int]-->Working;
  properties
    Occurrence => fixed 0.6 applies to node2Int;
    Occurrence => fixed 0.4 applies to node3Int;
  end Interference.node1;
**};
end Safety_Model;
```
Additional Modeling Issues

- Parameterize the modes
  - Energy consumption in a mode can depend on various parameter values
    - e.g. power consumption of a server in data center depends on CPU utilization
  - Parameterization can be achieved through property sets
  - Parameterization of modes is not possible in error annex

- Parameterize the properties in the property sets
  - Dynamics in the physical property values
  - Individual property types in the property set may themselves be property sets
    - e.g. interferences may not be static and may depend on the physical parameters
  - Using a property set as a property type in another property set is not allowed
Survivability in Critical CPS*

Critical Cyber-Physical Infrastructure

- **Utilities**
  - Advanced Electric Power Grid
  - Water Distribution
  - Pressure Pipes Gas/Oil

- **Search & Rescue**
  - Disaster Response, etc.

- **Computational Critical Infrastructure**
  - Data Centers
  - GPS Systems

- **Monitoring Systems**
  - Pervasive Health Monitoring
  - Monitoring of fire and chemical radiation plumes
  - Wild-life Monitoring
  - Forest Monitoring
Handling Critical Events in CPS

Critical Event Detection
- Detect fire using information from sensors
- Notify 911
- Provide information to the first responders

Additional Critical Events Detection
- Trapped People & Rescuers
- Detect trapped people
- Analyze the Spatial Properties
  - How to reach the source of fire;
  - Which exits are closest;
  - Is the closest exist free to get out;
- Determine the required actions
  - Instruct the inhabitants to go to nearest safe place;
  - Co-ordinate with the rescuers to evacuate.

Survivability – effectiveness of response plan to avoid disasters (life/property losses)
Criticality & Critical Event Management

- **Critical events**
  - Causes emergencies/crisis.
  - Leads to loss of lives/property.

- **Criticality**
  - Effects of critical events on the smart-infrastructure.
  - Critical State – state of the system under criticality.
  - Window-of-opportunity \((W)\) – temporal constraint for criticality.

- **Survivability**—effectiveness of the criticality response actions in minimizing the disasters.
Criticality Response behavior Model (CRM) for Survivability Analysis

- **State-based stochastic model**
  - System in different critical states for different criticalities.
    - States are organized in an hierarchical manner
  - Similar to AADL System Modes.

- **Critical Events**
  - Makes mode transitions down the state hierarchy
  - Enhancements capturing
    - Criticality characteristics (e.g. window-of-opportunity)

- **Mitigative Link**
  - Makes mode transitions up the state hierarchy.
  - Enhancements capturing
    - Probability of actions’ success considering uncertainties due to human involvement.

CRM for fire emergencies in Offshore Oil & Gas Production Platforms (OGPP)

Criticalities
- **c1** – Fire Alarm.
- **c2** – Imminent danger e.g. health hazards.
- **c3** – Assistance required to others e.g. trapped personnel.
- **c4** – Evacuation path not tenable.

Window-of-opportunity
- Survival time under asphyxiation.

State transition probabilities derived from established probability distribution in [1].

AADL based criticality response system architecture specification

..

system implementation OGPF.impl
subcomponents
  FM: system FireMonitoringComponent.impl;
  EM: system EvacuationMonitoringComponent.impl;
  DM: system DecisionMakingComponent.impl;
  ...

system implementation DecisionMakingComponent.impl
subcomponents
  Pl: process CRM.impl;
  ...
end DecisionMakingComponent.impl
  ...


Criticality Specification

:~
  process implementation CRM.impl
  subcomponents
    thread: thread Criticalities&Responses.impl;
  :
  end DecisionMakingComponent.impl
  :
  thread Criticalities&Responses
  features
    c1: in event port; --fire alarm
    c2: in event port; --imminent health hazard
    c3: in event port; --assistance required to others
    c4: in event port; --non-tenable path
    a1: out event data port; --responses
  :
  end Criticalities&Responses;
  :
  :
State and State Transition Specification

```
thread implementation Criticalities&Responses.impl1
modes
Normal: initial mode;      --normal state
s1: mode;                  --state (1)

s1243: mode;               --state (1243)

Normal [c1] > s1;         --CL at the normal state
s1 - [c2] -> s12;         --CLs at state (1)
s1 - [c3] -> s13;          --CL at state (3)
s12 - [c3] -> s123;       --CLs at state (12)
s12 - [c4] -> s124;       --CL at state (12)
s13 - [c4] -> s134;       --CL at state (13)
s123 - [c4] -> s1234;     --CL at state (123)
s124 - [c3] -> s1243;     --CL at state (124)

end Criticalities&Responses;
```

- Events in System
- System Modes
- Event Dependent Mode Transition
- State Transitions
- Critical States
- Criticalities
- Response Actions
- Windows of Opportunity
- Action Times
- Mode Properties
- AADL Constructs
- CRM Components

Impact

Arizona State University
State and State Transition Specification

```
property set state_properties is
  actions: list of aadlstring applies to (all);
  mlProbs: list of aadlreal applies to (all);
  clProbs: list of aadlreal applies to (all);
  critStates: list of aadlstring applies to (all);
  actionTime: list of aadlreal applies to (all);
  window-Opp: list of aadlreal applies to (all);
  policySpec: Enumeration (maxq, MP, MI, MMC,
                SCAMET, LMPT) applies to (all);
  modeName: aadlString applies to (all);
end state_properties;

thread implementation Criticalities&Responses.impl

properties
  state_properties::policySpec -> maxq;
  state_properties::mlProbs -> (0.5376)
    in modes (s1);
  state_properties::clProbs -> (0.2613, 0.2011)
    in modes (s1);
  state_properties::critStates -> ("s12", "s13")
    in modes (s1);
  state_properties::window-Opp -> (10.0)
    in modes (s1);
  state_properties::modeName -> "Fire in OGPP"
    in modes (s1);

end Criticalities&Responses.impl;
```

State and State Transition Specification

Criticalities

System Modes

Critical States

Events in System

State Transitions

Event Dependent Mode Transition

Mode Properties

Response Actions

Windows of Opportunity

AADL Constructs

mapped to

CRM Components

ARIZONA STATE UNIVERSITY
Conclusions

- AADL property set used for modeling CPS to analyze safety and survivability
- AADL error annex used for modeling interferences to analyze safety
- Issues faced
  - Unable to link Error Annex parser with plug in development project
  - Not sure about the initial configuration of annex parsers in plugin.xml
  - Sample example would be very helpful.
- Future Work
  - Property sets and error modes need to be parameterized
    - nested property sets
    - properties associated to the error modes
  - Model dynamics in the physical parameters
  - Composition of models from individual subsystem models
    - derive system-level global stochastic model by combining multiple sub-system-level local stochastic models
    - e.g. fire in a hospital has two sub-systems
      - fire management and medical emergency management
Questions/Suggestions/Discussion

Impact Lab (http://impact.asu.edu)

Creating Humane Technologies for Ever-Changing World

Acknowledgements: Sailesh Kandula
Additional Slides
Physical Interactions (Interference)

Cyber-Physical System
(distributed view)

Interference to the environment

Self-Interference (to itself)

Cross-interference

Computing node

Interference from the environment

environment

cyber subsystem
Heat Interference in BSN

Temperature rise in sensor surroundings

\[ \rho C_p \frac{dT}{dt} = K \nabla^2 T + \rho SAR - b(T - T_b) + P_{\text{circuitry}} + Q_m \]

**Temperature Rise: Pennes Bio-heat Equation**
Survivability in terms of **Q-value** or *Qualifiedness* of actions

- probability of reaching normal state based on
  1. Probabilities of MLs.
  2. Probabilities of CLs at intermediate states.
  3. Conformity to timing requirements.

**Q-value** is a quantitative measure to evaluate crises response.

AADL based tool developed to analyze Q-value of response actions.
Manageability as \( Q \)-value

- Manageability from any arbitrary critical state \( x \)
  - \( i \) an immediate upstream state.

\[
Q_{x,i,n} = \begin{cases} 
  p_{x,i} P_{i,n} & \text{if } W \text{ met} \\
  0 & \text{if } W \text{ NOT met}
\end{cases}
\]

\[
P_{i,n} = \begin{cases} 
  1 & \text{if } i = n \\
  (1 - \sum_{(i,j) \in CL(i)} p_{i,j}) \sum_{(i,k) \in ML(i)} p_{i,k} P_{k,n} + \sum_{(i,j) \in CL(i)} p_{i,j} P_{j,n} & \text{if } i \neq n \text{ & } W \text{ met} \\
  0 & \text{if } W \text{ NOT met}
\end{cases}
\]
Mapping of AADL constructs to specify CRM components

- **Events in System** mapped to **Criticalities**
- **System Modes** mapped to **Critical States**
- **Event Dependent Mode Transition** mapped to **State Transitions**
- **Mode Properties** mapped to **Response Actions**, **Windows of Opportunity**, and **Action Times**
Analysis of CPS

- Safety analysis
  - Interference should not be detrimental to the physical and other cyber components
    - e.g. heat generated by performing tasks in implanted body sensors should be within a threshold value to avoid tissue damage.

- Survivability analysis
  - Critical events should be effectively responded to avoid dangerous failures
    - e.g. providing proper access to equipment if fire is detected in a smart-building infused with sensors and actuators.