FORMAL ANALYSIS OF DELAYS IN WATERWAY SYSTEM OPERATIONS WITH TIMED AUTOMATA MODELING

LEONARD PETNGA
LEONARD.PETNGA@UAH.EDU
UNIVERSITY OF ALABAMA IN HUNTSVILLE

MARK AUSTIN
AUSTIN@ISR.UMD.EDU
UNIVERSITY OF MARYLAND

EVANGELOS I. KAIASAR
EKAISAR@FAU.EDU
FLORIDA ATLANTIC UNIVERSITY

17-20 October 2017
2017 International Urban Freight Conference (I-NUF)
Motivation & State-of-the-art

Research Gaps, Methodology

Formal Methods for Delay Analysis: MBSE & Timed Automata

Case Study: Delays Analysis in a Two-lock Waterway System

Concluding Remarks and Future Work
Introduction

Market Demand

Competition

Maritime Transportation

75%

Operating Efficiency

Cost Efficiency

Automation Capabilities

Adoption of CPS
Motivation

Increasing demand

Exhibit 3
Global maritime trade by volume, 2012-20200

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5</td>
<td>9.9</td>
<td>10.1</td>
<td>10.4</td>
<td>10.7</td>
<td>11.0</td>
<td>11.3</td>
<td>11.6</td>
<td>11.9</td>
</tr>
</tbody>
</table>

Aging infrastructure

US inland waterway system

Delays....

... and Accidents

Motivation

Increasing demand

Exhibit 3
Global maritime trade by volume, 2012-20200

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5</td>
<td>9.9</td>
<td>10.1</td>
<td>10.4</td>
<td>10.7</td>
<td>11.0</td>
<td>11.3</td>
<td>11.6</td>
<td>11.9</td>
</tr>
</tbody>
</table>

Aging infrastructure

US inland waterway system

Delays....

... and Accidents
**Motivation**

**Under-appreciated critical infrastructure...**

- **Inland waterway System**: 12K miles; 240 lock chambers; 300 commercial ports
- **Backbone of economy**: 1 barge ≈ 16 rail cars ≈ 70 semi-trailer trucks; 1 gallon of fuel can move 1 tons of good over 616 miles; > 566 million tons/year;
- **Neglected**: Old locks (>50 years); Av. 52 interruptions/day (2009); 25 years worth of delays system-wide (2011); underfunded.

**...Despite advances in systems automation**

- **Smart chips on ships**: embedded sensing, communication, control and computing technologies
- **Traffic management**: Information technologies(GUI for monitoring), laser and radar for fault tolerance.
Delay Analysis: State-of-the-art and Research Gap

Research on delays in waterways:

Gap: Need for formal modeling techniques
- Whole VS sum of parts: system perspective Vs piece-wise approach to modernization ==> Systems Engineering
- Verification of the correctness of functionality: more functionality to computer (embedded/local computational intelligence)
- Study of existing systems/problems: Delays & their impacts (safety, performance, cost)
Objective and Scope

- Investigate, understand and make use of
  - Model-based systems engineering (MBSE),
  - System behavior modeling of networks of timed automata, and
  - Composition and model checking of timed automata.

- To develop a mathematical framework for the formal analysis of delays in waterway system design and operations with timed automata modeling.

- And demonstrate its essential features in a case study examining delays and their impacts during crossing a simplified two-stage lock system.
MBSE for Waterway Systems

- Man-made Waterways are Systems
  - Safety-critical: lost of property & lives if accident + environmental impacts
  - Event-driven ➞ reactive system
  - Complex design: embedded computer, multi-physics
  - Complex management and operation

- System development
  - Models over documents
  - Multi-level approach
  - Design: Decomposition VS composition
  - Semi-formal and formal languages (SysML + Modelica)
  - Computation support for simulation and design space exploration
  - Issues: multi-level heterogeneity and abstractions

- Expected results
  - Virtual system prototypes
  - Cost and Time effective and accurate
Model-Based Development and Validation of Waterway System Operations

Interaction among objects

Simplified models

Activity Diagrams

Sequence Diagrams

Models of System Behavior and System Structure.

Trade-off Analysis
Detailed Simulation
Design Space Exploration
Model Checking

High-Level Requirements.

Revise Use Cases and Scenarios....

Constraints

Use Case 1
- scenario 1
- scenario 2

Use Case 2
- scenario 3
- scenario 4

Sequences of tasks

Sequence of messages between objects.
System Behavior Modeling with Timed Automata

- **Automaton**: a machine/controller designed to automatically follow a predetermined sequence of operations, or respond to predetermined instructions

- **Timed (finite) Automata**:
  - Annotated/constrained state-transition graph of automata with timing as real-valued clocks
  - Finite automata as canonical model of finite-state computation supported by theory and formalisms e.g., Buchi automata (NDFA), Muller automata (DFA & NDFA)

**Example**: 2-state deterministic Muller automaton accepting the \( w \)-regular language \( L_0 = (a+b)^* a^w \) over alphabet \( \{a, b\} \)

- **Real-time systems** (e.g., Waterway system):
  - System behavior as set of executions i.e. sequences of states and system events represented by (timed) automata
  - Set of sequences = formal language \( \Rightarrow \) Use of timed automata for verification and specification of systems and verification
  - Timed automata to specify delays in Waterlock operations in this work
Illustrations of timed automata

Ex. 1: \( L_1 = \{((ab)^w, t) | i, (2i < 2i + 2) \} \)

- **Behavior 1:** One clock \( x \)
  1. Start in \( S_0 \), then read symbol \( a \); Clock \( x \) initialized to 0 along the transition to \( S_1 \)
  2. While in \( S_1 \) count elapsed time since last occurrence of \( a \)
  3. Read symbol \( b \) and transition back to \( S_0 \) only if \( x < 2 \)

- **Specification 1:** the delay between \( a \) and the following \( b \) is always less than 2; thus the language

\[
L_1 = \{((ab)^w, t) | i, (2i < 2i + 2) \}
\]

Ex. 2: \( L_2 = \{((abcd)^w, t) | j, ((4j_3 < 4j_1 + 1) (4j_4 > 4j_2 + 2)) \} \)

- **Behavior 2:** Two clocks \( x, y \)
  1. \( x \) initialized to 0 from \( S_0 \) to \( S_1 \) reading \( a \)
  2. \( y \) initialized to 0 from \( S_1 \) and \( S_2 \) reading \( b \)
  3. \( c \) happens within time 1 of \( a \), between \( S_2 \) & \( S_3 \)
  4. Delay from \( b \) and \( d \) is always > 2

- **Specification 2:** the automaton cycles among states \( S_0, S_1, S_2 \) & \( S_3 \) following language

\[
L_2 = \{((abcd)^w, t) | j, ((4j_3 < 4j_1 + 1) (4j_4 > 4j_2 + 2)) \}
\]
**CONTROL DELAYS**

Occurs between the time the measurement signal is sampled and the time this measure is used in the actuator

Affects the performance of the system (MoEs)

**PHYSICAL DELAYS**

Occurs due to unintentional actions and external factors from the environment

May affect both system performance and safety

---

**Formal Analysis of Canal Systems Delays - Taxonomy**

<table>
<thead>
<tr>
<th>Family</th>
<th>Category</th>
<th>Description</th>
<th>Type</th>
<th>Delay Type &amp; Example</th>
</tr>
</thead>
</table>
| Physical (HW)   | Communication Delay (DO)| Extra time taken by a dysfunctional actuator/component (gate, valve or pump) to perform a task | $H_1$    | Component delay  
|                 |                        |                                                                              |          | *Ex.*: Gate actuator dysfunction                           |
|                 | Subsystem Delay (DS)   | A non-binding subsystem (ship, tugboat) takes more time than allowed to execute a task | $H_2$    | Subsystem Delay (Hybrid delay)  
|                 |                        |                                                                              |          | *Ex.*: Slow boat in the lock chamber                        |
|                 | Cycle Delay (DY)       | Water displacements into the system are delayed by inefficiencies in flows (pipe, external objects,...) | $H_3$    | Cycle Delay  
|                 |                        |                                                                              |          | *Ex.*: Water displacement slowed/blocked                    |
Consequences of Delays

Procedure:

1. Model behavior system using activity diagram
2. Identify pair of (current and successor) tasks
3. Apply delay type \( (H_1, H_2, H_3) \) to task ("Delayed task")
4. Characterize effect on successor task
5. Synthetize and interpret the result ("Result")
6. Characterize consequences on system (safety, performance, or both)

<table>
<thead>
<tr>
<th>Id</th>
<th>Delayed Task</th>
<th>Code Type</th>
<th>Successor Activity (delay risk)</th>
<th>Result</th>
<th>Consequences</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>Opening a gate.</td>
<td>EOG ( H_1 )</td>
<td>Towing ship in ( L(A(H_2)) )</td>
<td>( H_{12} )</td>
<td>Collision ship-gate</td>
<td>Gate (any)</td>
</tr>
<tr>
<td>05</td>
<td>Closing a gate.</td>
<td>ECG ( H_1 )</td>
<td>Opening valve 2 - after gate 0(( H_1 ))</td>
<td>( H_{11} \rightarrow H_2 )</td>
<td>Increased cycle time.</td>
<td></td>
</tr>
<tr>
<td>06</td>
<td>Opening a valve.</td>
<td>EOV ( H_3 )</td>
<td>Opening another valve (( H_3 ))</td>
<td>( H_1 \rightarrow H_2 )</td>
<td>Ship instability and increased cycle time.</td>
<td></td>
</tr>
<tr>
<td>07</td>
<td>Closing a valve.</td>
<td>ECV ( H_1 )</td>
<td>Closing another valve (( H_1 ))</td>
<td>( H_1 \rightarrow H_2 )</td>
<td>Increased cycle time.</td>
<td></td>
</tr>
<tr>
<td>08</td>
<td>Transferring water (sequence).</td>
<td>SE ( H_3 )</td>
<td>Closing valve (( H_1 ))</td>
<td>( H_{21} \Rightarrow H_3 )</td>
<td>Increased cycle time.</td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>Reinitializing system (reservoir and lock).</td>
<td>RIE ( H_3 )</td>
<td>Closing reservoir Valve (( H_1 ))</td>
<td>( H_{31} \Rightarrow H_3 )</td>
<td>Increased cycle time.</td>
<td></td>
</tr>
</tbody>
</table>
UPPAAL: Tool Support for Delay Simulation

UPPAAL:
- Integrated tool environment for modeling, validation and verification of real-time systems
- System behavior as Networked NDFA based on Temporal Logic and Model checking via state-space exploration
- Query the model in UPPAAL language to check system level properties (e.g.: bounded liveness, reachability and deadlock)
Case Study: Delay Analysis in a 2-lock system

**System**
- Two-step, two ways lock system (Ex: Miraflores in Panama)
- Post-panamax ships
- Automated operations
- SysML & OpenModelica (MBSE)

**Procedure for (Delay) Analysis**
- Create Model (optimal design) system using MBSE
- Perform timing analysis (component, subsystem, system)
- Select analysis tool (e.g: UPPAAL) and verify system
- Create and verify Delay models
- Update component - especially the controller – models with delays
- (Re)verify the system with delays
Ship has waited too long in the lock and is now delayed! This will ultimately increase cycle time (Moe)....but the system recovers.

The Controller takes note of "delay" information, subsequently modifies ShipBoat path accordingly.

The Controller takes note of "delay" information, subsequently modifies ShipBoat path accordingly.

Models of Delay: Delays affecting MoEs

==> system is Deadlock free and can recover from the delay – mostly H₃ types
Delay of towing the Ship, no more buffer time $\Rightarrow$ ship is hit by the gate (accident $\Rightarrow$ system safety requirement violated)

External intervention (human) needed to fix the problem

$\Rightarrow$ system is **NOT** Deadlock free and can **NOT** recover from the delay (the gate collides with the ship) – mostly H1 and H2
**Hybrid Delays:** affect Performance & Safety

---

**Delay of Ship:** buffer time used to help the system recover (only Moe affected)

**Delay of Ship:** no more buffer time ➞ ship is hit by the gate (accident ➞ system safety requirement violated)

---

**Hybrid delay:** one of the most critical and difficult to understand in the system (multiple effects).
## Models of Delay: Verification Summary

<table>
<thead>
<tr>
<th>Delay model</th>
<th>Property N.</th>
<th>Requirement/Property</th>
<th>Type</th>
<th>UPPAAL language</th>
<th>Verification result</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>1</td>
<td>The system can recover from this of delay (i.e., it’s deadlock-free).</td>
<td>Safety</td>
<td>A[] not deadlock</td>
<td>Property is satisfied</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Whenever a ship is delayed in a lock, the cycle time will ultimately be increased.</td>
<td>Liveliness</td>
<td>ShipBoat.Delay_H2 → ShipBoat.IncrsgCycleTime</td>
<td>Property is satisfied</td>
</tr>
<tr>
<td>02</td>
<td>3</td>
<td>This system will ultimately break (not deadlock prone)</td>
<td>Safety</td>
<td>A[] deadlock</td>
<td>Property is satisfied</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>A delay in the ship towing process can ultimately lead to a collision with the gate</td>
<td>Safety</td>
<td>E[] Ship.TowToLA imply ShipBoat.BCollisionShipGate_H21</td>
<td>Property is satisfied</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>A delay in the ship towing process can ultimately impact the performance of the system</td>
<td>Safety</td>
<td>E[] Controller.CheckTowToLA imply Controller.CheckWaitInLA</td>
<td>Property is satisfied</td>
</tr>
</tbody>
</table>

⇒⇒ Impact of delay on cycle time (Moe) and safety demonstrated through the use of reachability rule (corresponding undesirable states are reachable!)
Type H1 delays: Valve & Gate operations

Type H2 delays: Towing and Clearing operations

Type H3 delays: Water transfer and system re-initialization

\[\Rightarrow \text{All primary (three) types of delays captured by the model of the controller}\]

\[\Rightarrow \text{Complexity of the design of the control system increased}\]
Concluding Remarks and Future Work

- Analysis and modeling of physical delays in the water lock system uncovered the mechanisms through which the delays affect system operations
- Cycle delays affect system measure of effectiveness

- Extend the simulation model to various marine transportation use cases, including, cargo operations
- Employ empirical measurements for Canal-Lock mechanisms for safe marine operations
Leonard Petnga: leonard.petnga@uah.edu
Mark Austin: austin@isr.umd.edu
Evangelos Kaisar: ekaisar@fau.edu