MISSOURI S&T
SeNDeComp
Sensor Networks and Dependable Computing

Facilitating Model–Based Design and Assurance for Sustainability

Student: Natasha Jarus, Ph.D. Candidate
Advisors: Sahra Sedigh Sarvestani and Ali Hurson
Department of Electrical and Computer Engineering

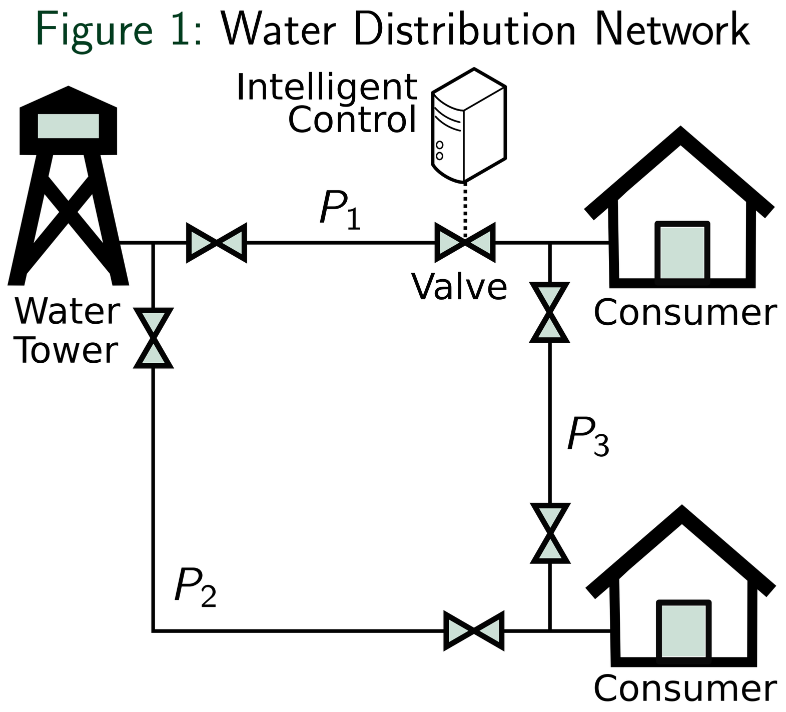
IGSC 2018

Introduction

In large–scale critical infrastructure, sustainability and dependability often conflict. For instance, intelligent and sustainable water distribution requires:

- Conservation of water and power;
- Reliability, availability, and resilience;
- Security against physical and cyber attacks;
- Safe operation, even during component failures; and
- High utilization of system capacity.

Figure 1: Water Distribution Network



Model–Based Design and Assurance

- Models are used to verify that a given system design or implementation meets specified requirements.
- **Effective verification and assurance requires comprehensive and consistent models.**
- No single model captures all aspects of a complex system's behavior.
- An array of models encompassing system dynamics, dependability, safety, and security is required.
- All of these models need to remain up–to–date and consistent.

Model transformation can facilitate the challenging task of maintaining consistency across models of a system as its design or implementation evolve.

Goals of Model Transformation

- **Facilitate creation of consistent and accurate models.**
- **Prevent** (some) **modeling mistakes.**

Requirements for Model Transformation

- **Broad applicability**, e.g., ability to relate:
  - Continuous– and discrete–time models and
  - Topological and dependability models.
- **Provable Correctness.**

Each model of a system serves as an approximation of that system's behavior—in other words, its semantics. **Correct approximation of semantics is key to provably correct model transformation.**

Research Objectives

This doctoral research aims to create:

- A **formalization** of how system and model semantics can be approximated.
- A method for **correctly transforming** system models.
- A method for correctly **combining models** of different types.

Proposed Approach: Abstract Interpretation

- Models are approximations of system behavior.
- **Given a model of a system, we can deduce some properties of that system.**
- **Given some properties of a system, we can derive one or more models consistent with those properties.**

Mathematically, **we define a domain for properties describing the system ($\mathbb{P}$roperties). Each type of model representing the system is defined by a separate domain whose elements are sets of models of that type.** For example, all reliability models could be defined as $\mathbb{M}\mathbf{odel}_\mathbf{R}$.

The elements of each domain are ordered by specificity: the more specific a description of properties or a set of models, the greater the information it conveys. For instance, a property stating that a component's reliability is 0.8 is more specific than one that gives the range of 0.7 to 0.9.

We relate these domains through:

- **Abstraction**: $\alpha : \mathbb{P}\mathbf{roperties} \to \mathbb{M}\mathbf{odel}$ identifies models that capture the specified properties.
- **Concretization**: $\gamma : \mathbb{M}\mathbf{odel} \to \mathbb{P}\mathbf{roperties}$ deduces the properties that hold for every member of a set of models.

These functions are related:

$$P \sqsubseteq (\gamma \circ \alpha)(P),\ \forall P \in \mathbb{P}\mathbf{roperties}$$
$$(\alpha \circ \gamma)(M) \subseteq M, \forall M \in \mathbb{M}\mathbf{odel}$$

If α and γ were inverses, every model type would have to fully describe system behavior. Since this cannot be, we relax that relationship:

- **Abstracting models from properties, then concretizing properties, should not add any inconsistent properties**, but may not preserve all the original properties.
- **Concretizing properties, then abstracting models from them, should recover the initial set of models (or a subset).**

Correctness

The correctness relation holds when elements of a domain correctly describe a system. If an element P of $\mathbb{P}$**roperties** describes a system S, we write $S\ R_{\mathbb{P}}\ P$.

$R_{\mathbb{P}}$ induces correctness relations for each type of model: $S\ R_{\mathbb{M}}\ M$ if and only if $S\ R_{\mathbb{P}}\ \gamma(M)$.

Example of Model Transformation

Consider a topology model for Figure 1, specifying:

- Each consumer requires 10 gallons per minute (gpm) of water.
- The water tower supplies at least 20 gpm.
- Pipe P_1 has a capacity of 20 gpm.
- Pipes P_2 and P_3 each have a capacity of 10 gpm.

We can deduce a number of properties from this topology model, including interconnections between and capacities of components. **Crucially, we can deduce interdependencies among components:**

- If P_1 fails, total demand cannot be met.
- If either P_2 or P_3 fail, the system can still supply all the demand.
- If both P_2 and P_3 fail, the system cannot supply all the demand.

We can derive a reliability model from these deduced properties. For brevity, in this example the focus is only on physical failures. This system has four states:

- **A**: System fully functional
- **B**: P_2 failed
- **C**: P_3 failed
- **D**: System cannot meet demand

Each pipe failure causes a transition among these states. A transition probability matrix (TPM) captures the likelihood of transitions associated with each failure. (Pipe P_i has reliability p_i and unreliability q_i.)

TPM for P_1

	A	B	C	D
A	p_1	0	0	q_1
B	0	p_1	0	q_1
C	0	0	p_1	q_1
D	0	0	0	1

TPM for P_2

	A	B	C	D
A	p_2	q_2	0	0
B	0	1	0	0
C	0	0	p_2	q_2
D	0	0	0	1

TPM for P_3

	A	B	C	D
A	p_3	0	q_3	0
B	0	p_3	0	q_3
C	0	0	1	0
D	0	0	0	1

The system is initially fully functional (state **A**) and is considered functional in every state except **D**. This information, along with the TPMs, give us the **system's reliability**:

$$R = p_1(p_2p_3 + p_2q_3 + q_2p_3)$$

Current Status and Future Work

- Core theory has been accepted to the 2019 IEEE International Symposium on High Assurance Systems Engineering.
- A detailed case study on relating reliability and topology models is in progress.
- The next task will be relating discrete– and continuous–time models.
- Model composition is a long–term goal.

This research is funded by the Missouri S&T Intelligent Systems Center and the U.S. Department of Education.

October 2018