Dependability and Survivability Evaluation of a Water Distribution Process with Arcade

Stephan Roolvink, Anne Remke, Mariëlle Stoelinga

Performability Modeling of Computer and Communication Systems 2009
1 Water distribution model

2 Arcade

3 Survivability in Arcade

4 Conclusions
Distribution station

Drinking water Reservoir 1
Drinking water Reservoir 2
pumping station
Distribution station
district 1
district 2
Distribution station

Valve 1 → input 1 → Valve 3 → Tank → Valve 6 → Output 2

Valve 2 → input 2 → Valve 5 → Output 1

Stephan Roolvink, Anne Remke, Mariëlle Stoelinga

Dependability & Survivability of a Water Distribution Process
Measures of interest

- Availability
- Reliability
- Survivability
Taxonomy of dependability

Availability

Availability is the probability of the system being in an operational state within a mission time assuming that components are repaired.
Taxonomy of dependability

Reliability according to [Sanders and Malhis, 1992]
Reliability is the probability of having no system failure within a certain mission time assuming that no component is repaired.
Survivability according to [Cloth and Haverkort, 2005]

Survivability is the ability of a system to recover predefined service levels in a timely manner after the occurrence of disasters.

\[
\text{survivability} \equiv \text{disaster} \Rightarrow \text{recoverability} \quad (1)
\]
\[
\text{recoverability} \equiv P_{\geq p}(trueU \leq t \text{ service}) \quad (2)
\]
What is Arcade (architectural dependability evaluation)?

Basic building blocks
- Components
- Repair units
- Spare management unit

Defining measure of interest
- Fault tree style

Measures of interest
- Availability
- Reliability

Boudali et al. [2008]
What is Arcade (architectural dependability evaluation)?

Basic building blocks
- Components
- Repair units
- Spare management unit

Defining measure of interest
- Fault tree style

Measures of interest
- Availability
- Reliability

Boudali et al. [2008]
What is Arcade (architectural dependability evaluation)?

Basic building blocks
- Components
- Repair units
- Spare management unit

Defining measure of interest
- Fault tree style

Measures of interest
- Availability
- Reliability

Boudali et al. [2008]
I/O-IMC (Input/Output Interactive Markov Chain)

- Finite-state machine
- 3 types of transitions
  - Markovian transitions
  - Direct-action transitions
  - Delayed-action transitions
I/O-IMC (Input/Output Interactive Markov Chain)

- Finite-state machine
- 3 types of transitions
  - Markovian transitions
  - Direct-action transitions
  - Delayed-action transitions
Distribution station model - parameters

- Rates are assumed values (work in progress)
  - Failure rates: $\lambda_{\text{valve\_open}} = \lambda_{\text{valve\_close}} = 1/2000$ and $\lambda_{\text{tank}} = 1/6000$
  - Repair rates: $\mu_{\text{valve}} = 1$ and $\mu_{\text{tank}} = 5/60$
- Assumption: stuck open cannot cause a system failure
- Model uses dedicated repair units
I/O-IMC of Distribution station model

(a) Valve I/O-IMC

(b) Tank I/O-IMC
Fault tree (for availability and reliability)
Steady state availability 0.84
Water distribution Model - Reliability over time

Reliability

Probability (R)

$t$ in hours

Stephan Roolvink, Anne Remke, Mariëlle Stoelinga

Dependability & Survivability of a Water Distribution Process
Extending Arcade for survivability

Needed to calculate survivability:

- Status information of components
  - Disable lumping in CADP (generates state space explosion)
  - Add atomic properties to states.
- Continuous Stochastic logic (CSL) model checking
  - Export CADP model to MRMC model checker
Extending Arcade for survivability

Needed to calculate survivability:

- Status information of components
  - Disable lumping in CADP (generates state space explosion)
  - Add atomic properties to states.
- Continuous Stochastic logic (CSL) model checking
  - Export CADP model to MRMC model checker
Extending Arcade for survivability

Needed to calculate survivability:

- Status information of components
  - Disable lumping in CADP (generates state space explosion)
  - Add atomic properties to states.
- Continuous Stochastic logic (CSL) model checking
  - Export CADP model to MRMC model checker
Extending Arcade for survivability

Needed to calculate survivability:

- Status information of components
  - Disable lumping in CADP (generates state space explosion)
  - Add atomic properties to states.
- Continuous Stochastic logic (CSL) model checking
  - Export CADP model to MRMC model checker
Stephan Roolvink, Anne Remke, Mariëlle Stoelinga

Dependability & Survivability of a Water Distribution Process
State space in CADP (Distribution station model)

Results:

- **Without** APs: 4869 states and 17861 transitions
- **With** APs: 35330 states and 405112 transitions
  - Reducing Fault tree out of the model
    (1458 states and 23328 transitions)
Results:

- **Without** APs: 4869 states and 17861 transitions
- **With** APs: 35330 states and 405112 transitions
  - Reducing Fault tree out of the model
    (1458 states and 23328 transitions)
Disasters

- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail
Survivability water distribution station

Disasters

- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail
Survivability water distribution station

Disasters

- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail
Survivability water distribution station

Service levels

- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up
Survivability water distribution station

Service levels

- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up
Survivability water distribution station

Service levels

- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up
Survivability water distribution station

Service levels

- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up
Service levels

- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up

![Diagram of water distribution station with valves and tank]
Survivability water distribution station - Service level 1

Recovery to Service level 1

Disaster 1: Valve 4 fails
Disaster 2: Tank fails
Disaster 3: Valve 1 and 3 fail
Survivability water distribution station - Service level 2

Disaster 1: Valve 4 fails
Disaster 2: Tank fails
Disaster 3: Valve 1 and 3 fail
Survivability water distribution station - Service level 3

Recovery to Service level 3

- Disaster 1: Valve 4 fails
- Disaster 2: Tank fails
- Disaster 3: Valve 1 and 3 fail

Stephan Roolvink, Anne Remke, Mariëlle Stoelinga
Extending the CADP model with APs enables model checking for survivability using MRMC.
- Increases the state space and thus model creation time.
- The calculated survivability values have been validated.
- Using a manually created model.
Future work

- Use quantitative survivability measures (water levels)
- Extend the water distribution station model
- Compare use CADP with Prism within Arcade to compute Availability, Reliability and Survivability.
