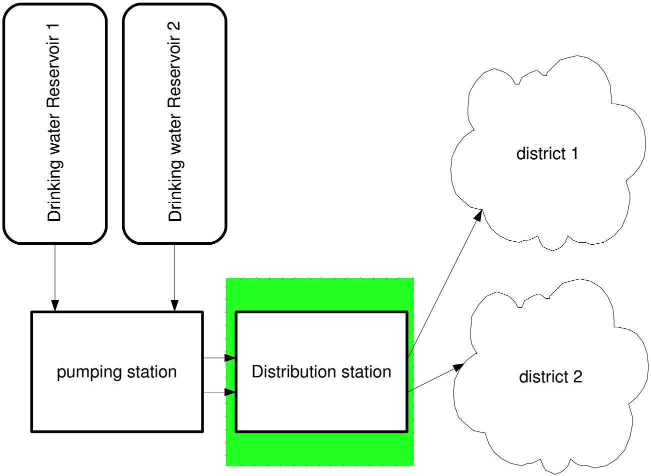
Dependability and Survivability Evalution of a Water Distribution Process with Arcade

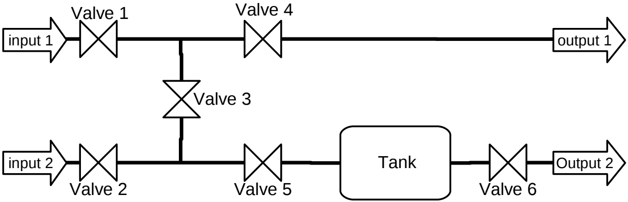
Stephan Roolvink, Anne Remke, Mariëlle Stoelinga

Performability Modeling of Computer and Communication Systems 2009

Distribution station



Distribution station



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.

Taxonomy of dependability

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**.

$$survivability \equiv disaster \Rightarrow recoverability \tag{1}$$

$$recoverability \equiv \mathcal{P}_{\geq p}(true\,\mathcal{U}^{\leq t} service) \tag{2}$$

What is Arcade (architectural dependability evaluation)?

Basic building blocks

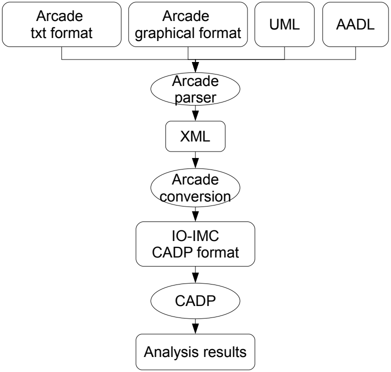
- Components
- Repair units
- Spare management unit

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

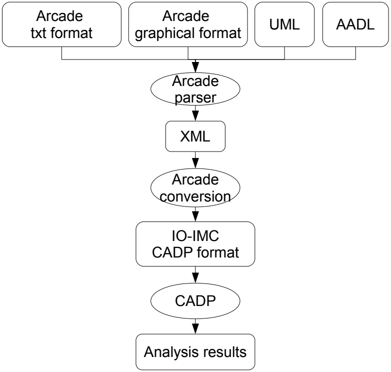
- Components
- Repair units
- Spare management unit

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

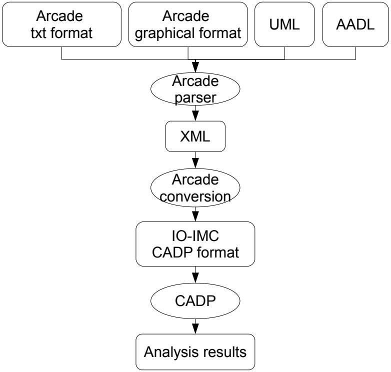
- Components
- Repair units
- Spare management unit

Defining measure of interest

- Fault tree style

Measures of interest

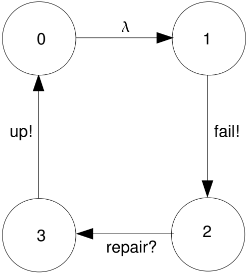
- Availability
- Reliability

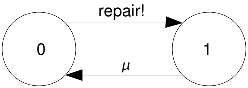


Boudali et al. [2008]

I/O-IMC (Input/Output Interactive Markov Chain)

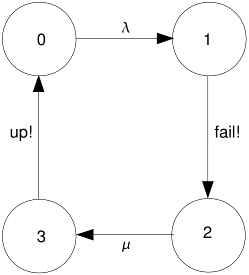
- Finite-state machine
- 3 types of transitions
  - Markovian transitions
  - Direct-action transitions
  - Delayed-action transitions





I/O-IMC (Input/Output Interactive Markov Chain)

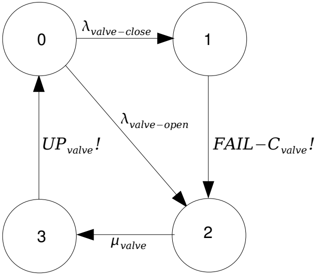
- Finite-state machine
- 3 types of transitions
  - Markovian transitions
  - Direct-action transitions
  - Delayed-action transitions



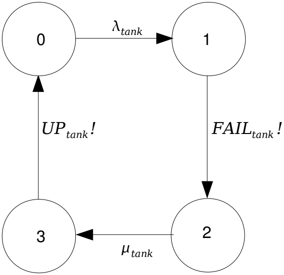
Distribution station model - parameters

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

I/O-IMC of Distribution station model

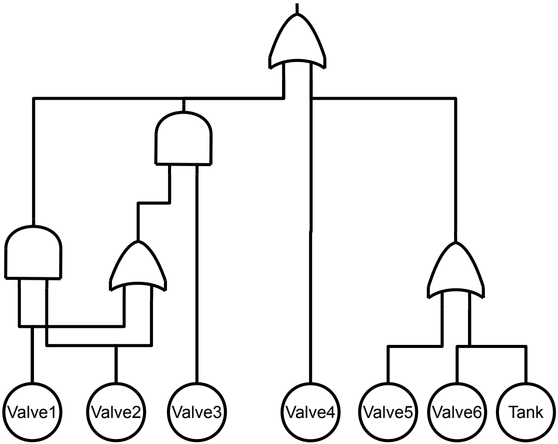


(a) Valve I/O-IMC

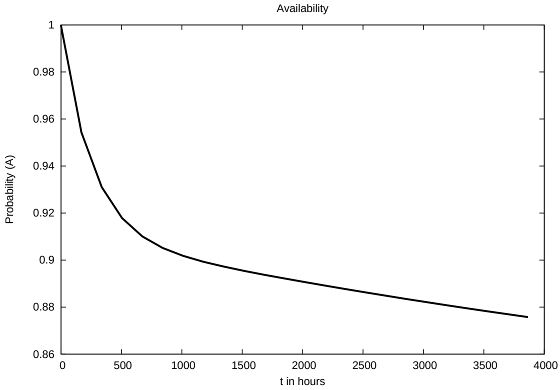


(b) Tank I/O-IMC

Fault tree (for availability and reliability)

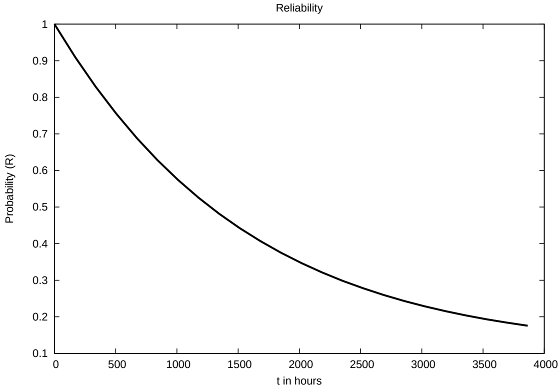


Distribution station model - Availability over time



Steady state availability 0.84

Water distribution Model - Reliability over time



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:

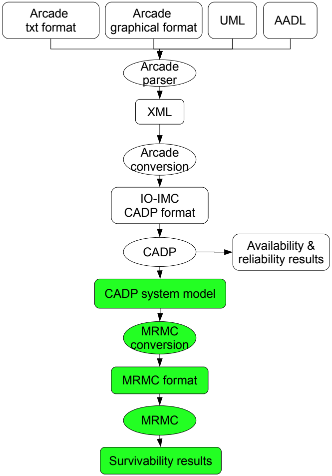
- Status information of components
  - Disable lumping in CADP (generates state space explosion)
  - Add atomic properties to states.
- Continuous Stochastic logic (CSL) model checking
  - Export CADP model to MRMC model checker

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

Arcade toolchain



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)

State space in CADP (Distribution station model)

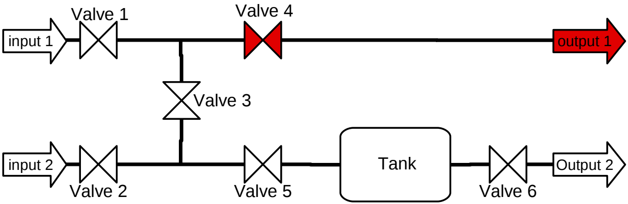
Results:

- **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)

Survivability water distribution station

Disasters

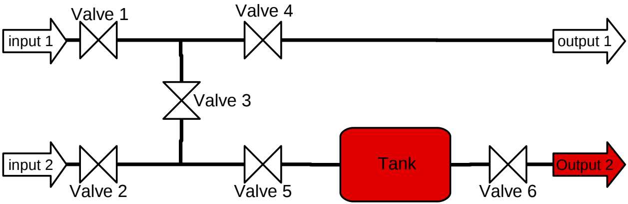
- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail



Survivability water distribution station

Disasters

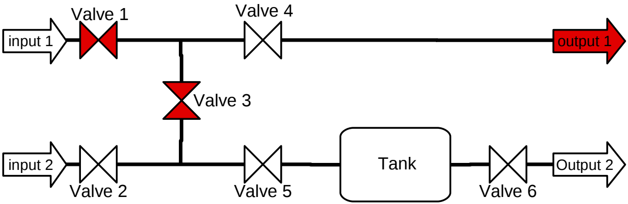
- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail



Survivability water distribution station

Disasters

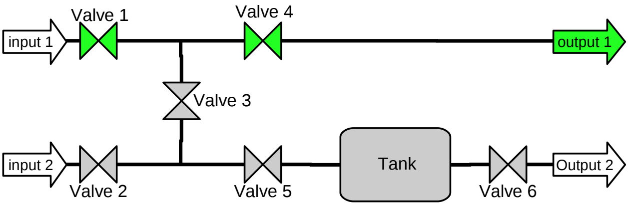
- **Disaster 1**: Valve 4 fails
- **Disaster 2**: Tank fails
- **Disaster 3**: Valve 1 and 3 fail



Survivability water distribution station

Service levels

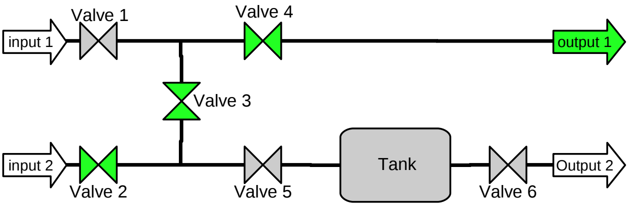
- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up



Survivability water distribution station

Service levels

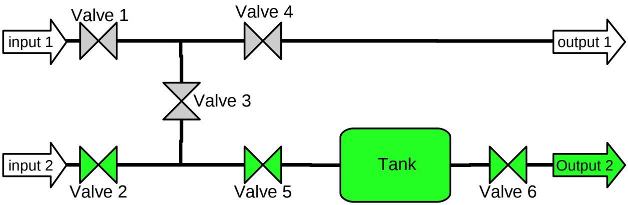
- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up



Survivability water distribution station

Service levels

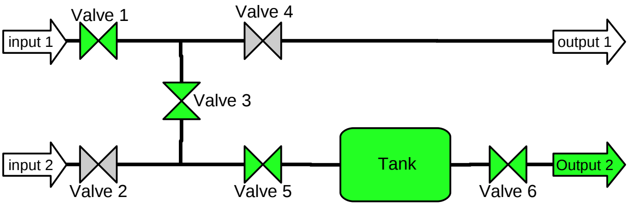
- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up



Survivability water distribution station

Service levels

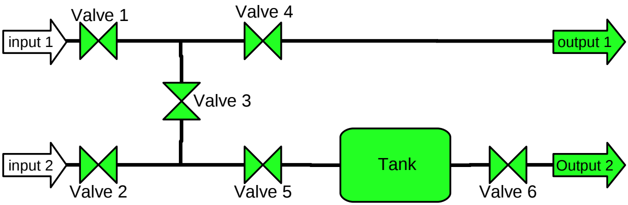
- **Service level 1**: Distribution to district 1 is up
- **Service level 2**: Distribution to district 2 is up
- **Service level 3**: All components are up



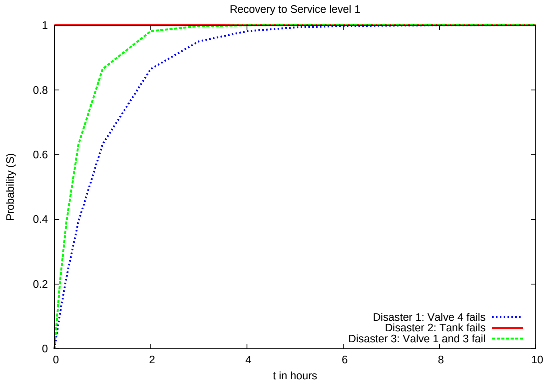
Survivability water distribution station

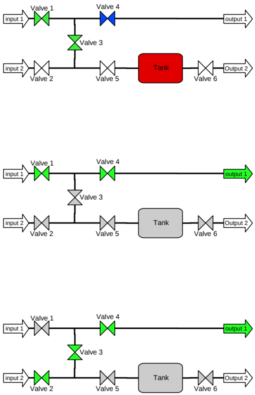
Service levels

- **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

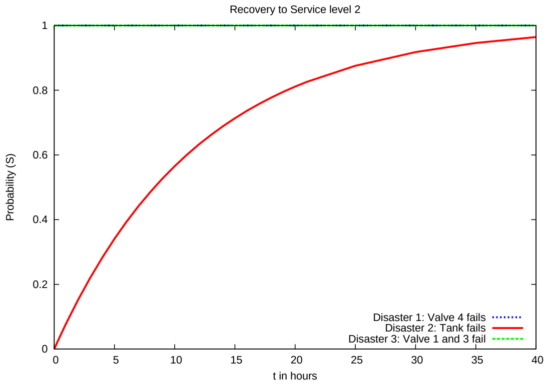


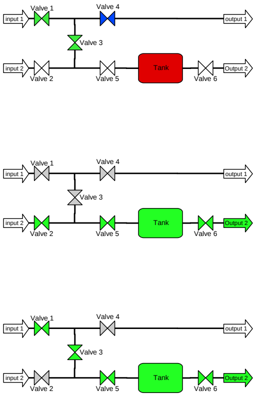
Survivability water distribution station - Service level 1



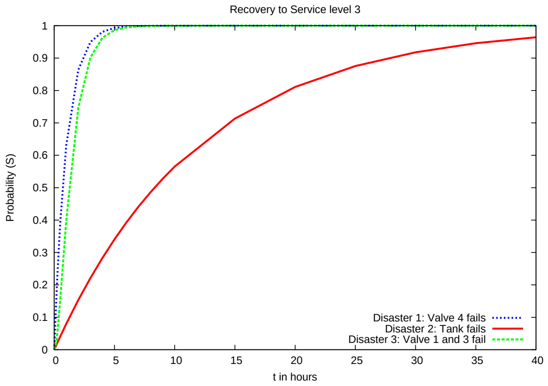


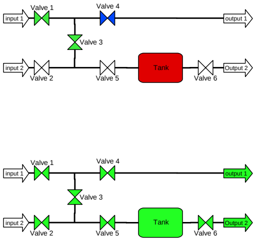
Survivability water distribution station - Service level 2





Survivability water distribution station - Service level 3





Conclusions

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

H. Boudali, P. Crouzen, B. R. Haverkort, M. Kuntz, and M. Stoelinga. Architectural dependability evaluation with Arcade. In *Proceedings of the 38th Annual IEEE/IFIP Int. Conference on Dependable Systems and Networks*, pages 512–521. IEEE Computer Society Press, 2008.

L. Cloth and B.R. Haverkort. Model checking for survivability! In *Proceedings of the 2nd Int. Conference on the Quantitative Evaluation of Systems*, pages 145–154. IEEE Computer Society Press, 2005.

W. H. Sanders and L. M. Malhis. Dependability Evaluation Using Composed SAN-Based Reward Models. *Journal of Parallel and Distributed Computing 15*, pages 238–254, 1992.