Maanpuolustuskorkeakoulu

# Entropy Measures in Critical Infrastructure Graphs

# Critical Infrastructure

- Consists of assets and systems which are essential in maintaining vital societal functions
- For example electricity generation, telecommunication, water supply, transportation systems and financial services

# Critical Infrastructure (2)

- Critical infrastructure has become a noteworthy field of contemporary research
- Various methods and formalisms have been studied:
  - Graphs
  - Bayesian belief networks
  - Neural networks
  - Etc.

# Roots of entropy

- The concept of entropy in thermodynamics was invented by Rudolf Clausius in 1850s
- The term entropy comes from the Greek word *τροπή*, "transformation”
- In 1948 Claude E. Shannon proposed a information theoretic view of entropy in his paper ”*A Mathematical Theory of Communication*”

# The definition of entropy

- For a random variable X we define its *entropy* to be

  $$H(X) := -\sum P(X=x) \log P(X=x),$$

  where x goes through all possible states of X
- Entropy is the expected value of information associated to a single event:

  $$H(X) = E(-\log P(X))$$

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

# The definition of entropy (2)

- Information is usually measured in bits (a.k.a. shannons)
- 1 bit = 1 coin flip
- Entropy of an event can be thought of as a measure of uncertainty:

  hard to predict = high entropy

  easy to predict = low entropy

# DiSCI and SACIN

- This work is part of a larger research project, called Digital Security of Critical Infrastructures (DiSCI)
- Aim is to find solutions to control critical infrastructure threats on a national level
- Situational Awareness of Critical Infrastructure and Networks (SACIN) software framework was developed for monitoring critical infrastructure

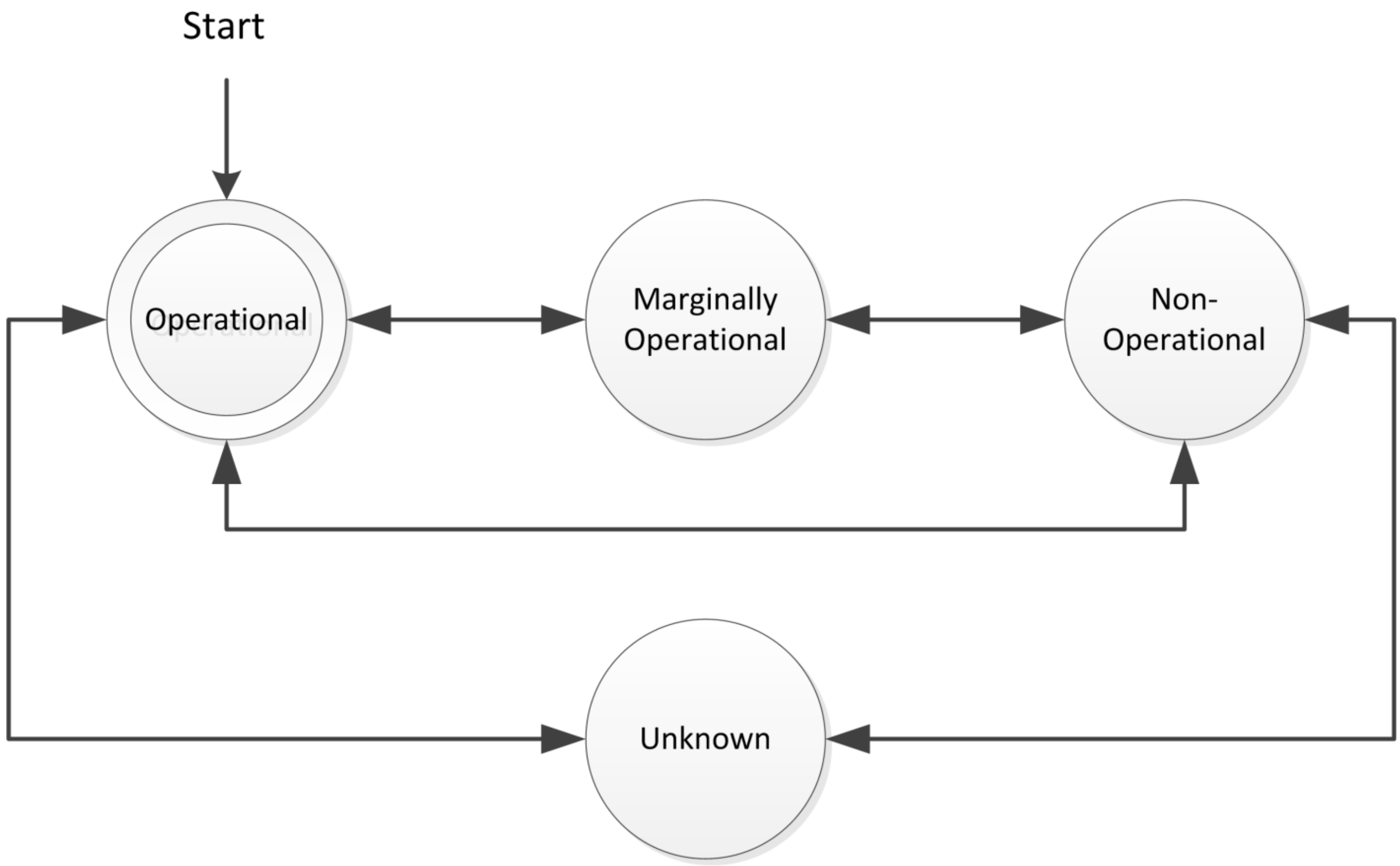
# Modelling critical infrastructure

- In situational awareness, we are mainly interested in critical infrastructure health and degree of operational capability
- The model should reflect this line of thought
- No exessive specifics about the systems should be included
- Flexible and extensible structure

# Critical infrastructure system (CIS)

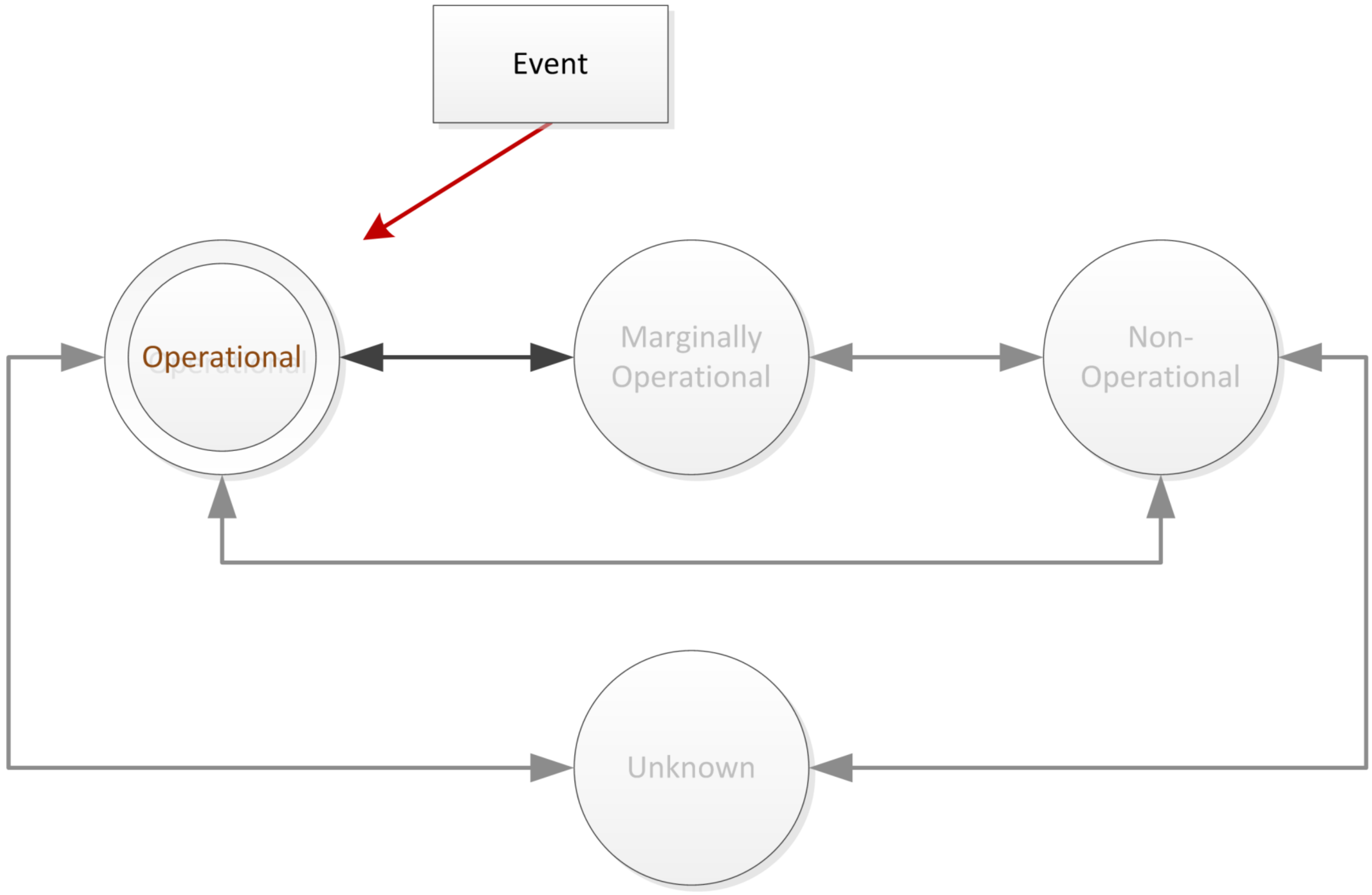
- Combines graphs and finite state machines
- Directed graph represents dependency relations
- Finite state machines (on nodes) can represent a facility, process or service

# Example state diagram



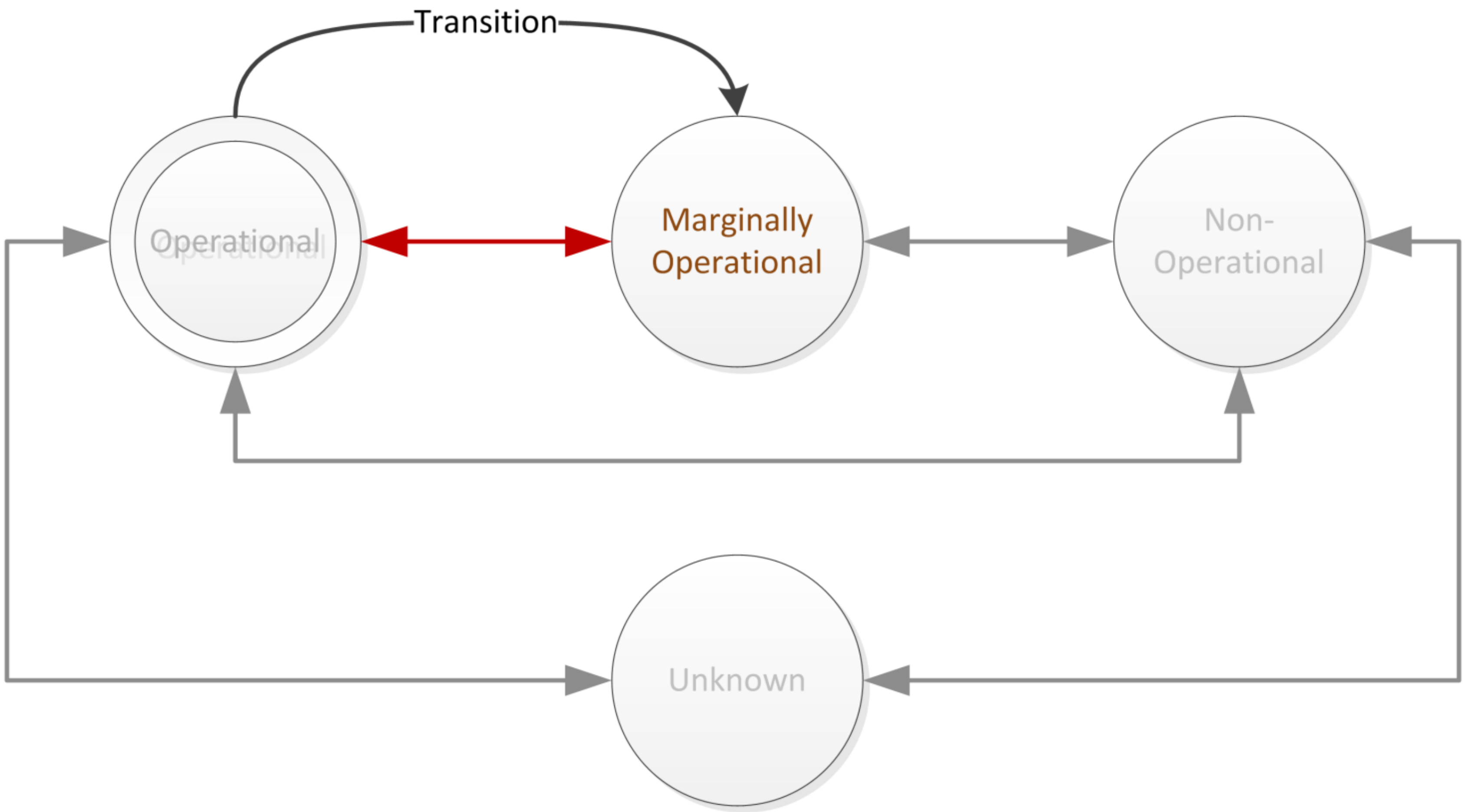

**Markus Klemetti, Samir Puuska**
**Sotatekniikan laitos**
**MPKK**

# Event causes transition



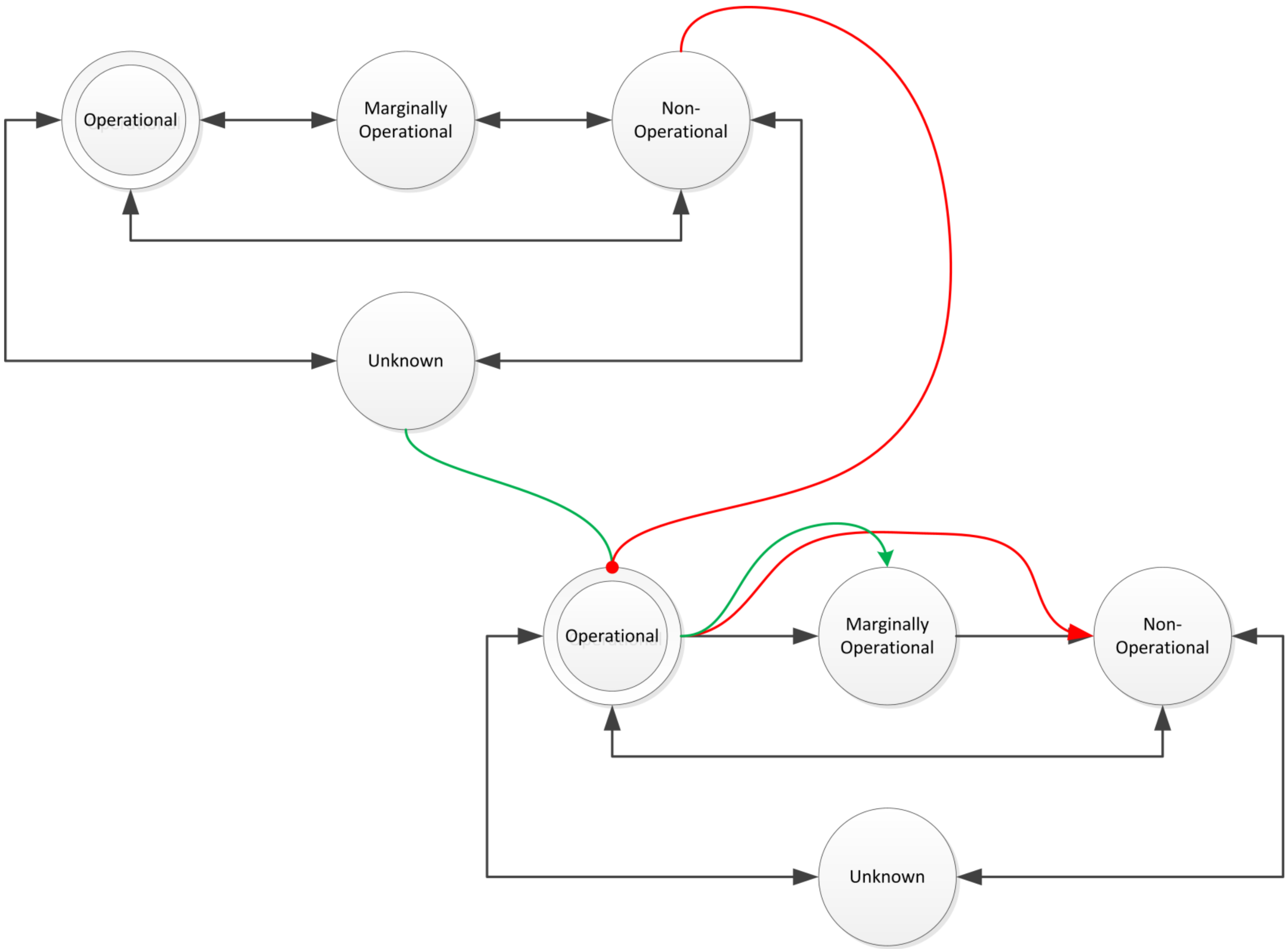

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

# State change

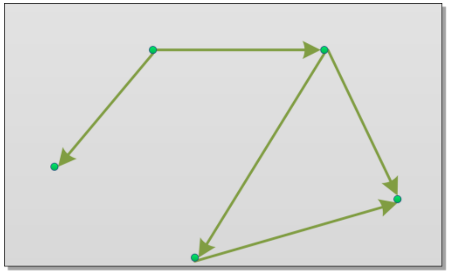


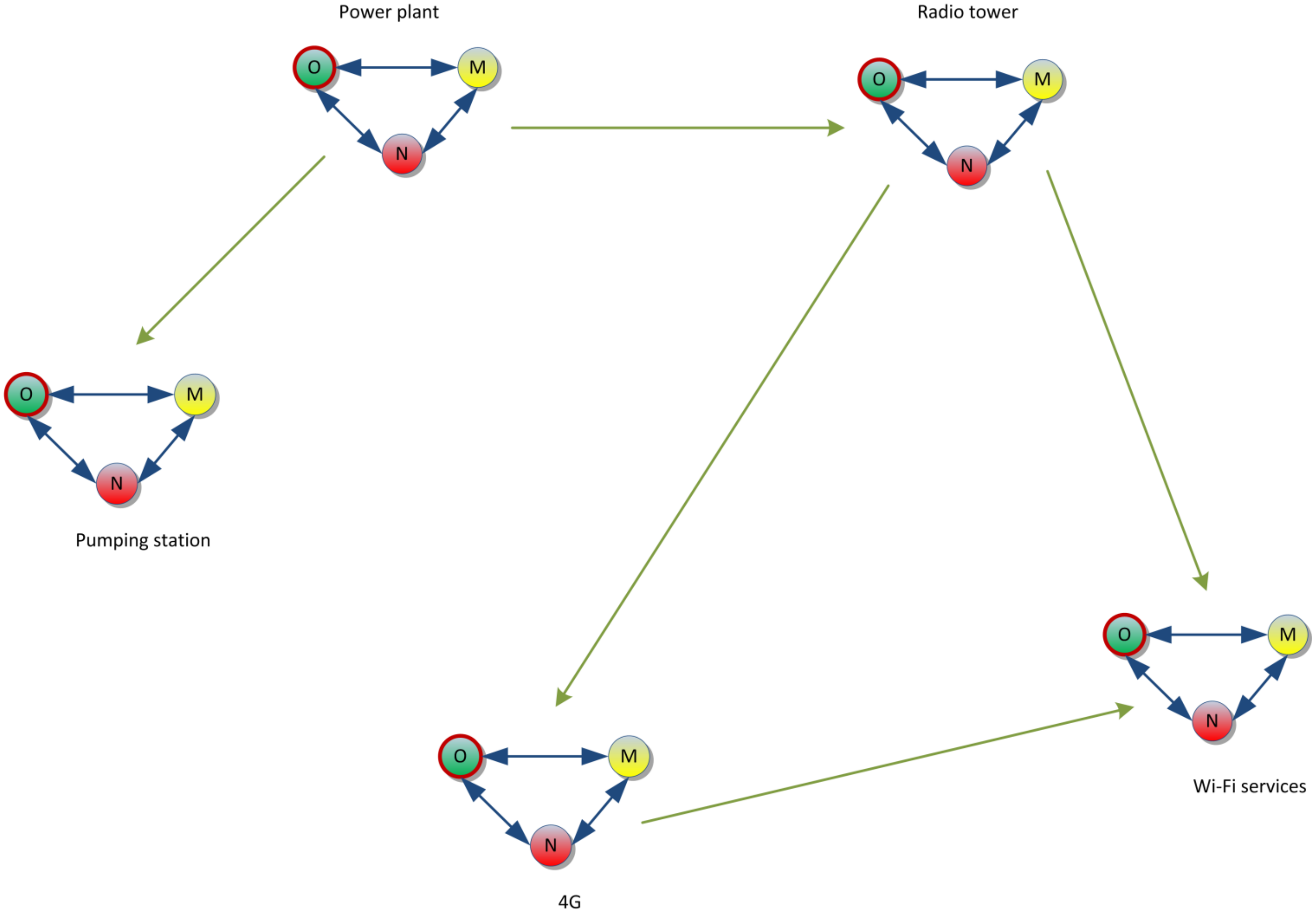

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

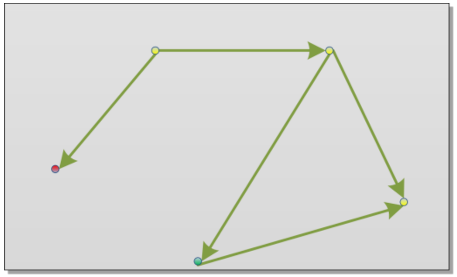
# State machines coupled

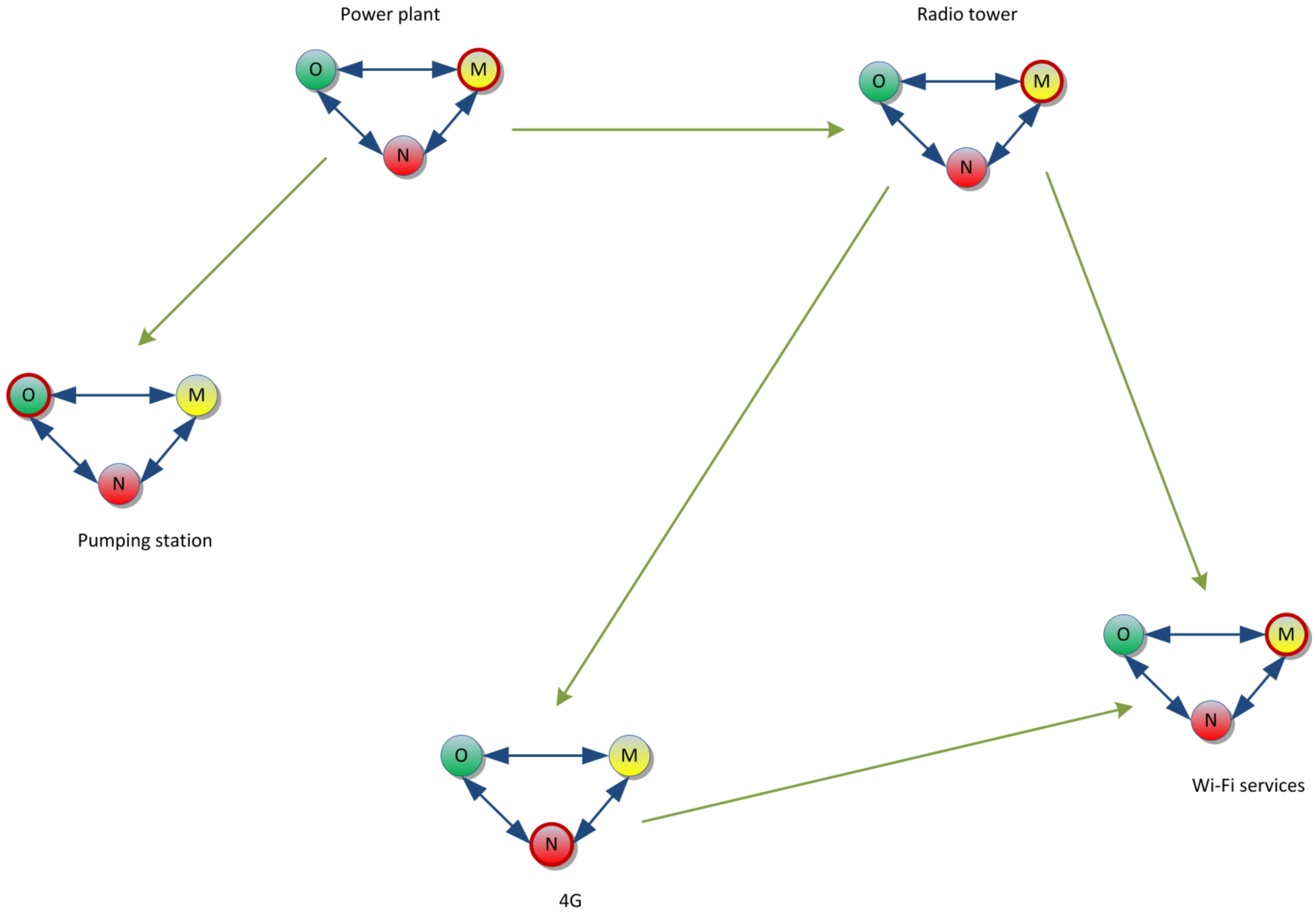



Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK




Power plant
O
M
N
Radio tower
O
M
N
O
M
N
Pumping station
O
M
N
Wi-Fi services
O
M
N
4G




Power plant
O
M
N
Radio tower
O
M
N
O
M
N
Pumping station
O
M
N
Wi-Fi services
O
M
N
4G

# Status function

- Attached to each finite state machine in the graph is a *status function* S: Q → [0,1], where
  – Q is the set of states of the machine
  – For each state q in Q, the number S(q) represents its severity, 0 implying the machine is not operational and 1 implying that the machine is fully operational.

# Implementing time and probabilities

- In this work we expand the critical infrastructure system model by associating a probability distribution to each node of the graph
- For simplicity we assume that sensor readings are always accurate
- Let M be a finite state machine that has states *operational (O), marginally operational (M)* and *non-operational (N),* with (previously observed) probabilities a, b and c, respectively.

# Implementing time and probabilities (2)

- Let X denote the state of the finite state machine M. At first we assume that X follows the default probability distribution

$$P(X = x) = \begin{cases} a, & \text{when } x = O \\ b, & \text{when } x = M \\ c, & \text{when } x = N \end{cases}$$

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

# Implementing time and probabilities (3)

- In case we get a sensor reading N, we define the new probability distribution for X as follows:

$$P(X = x) = \begin{cases} S(N)a(1 - e^{-kt}), & \text{when } x = O \\ S(N)b(1 - e^{-kt}), & \text{when } x = M \\ 1 - S(N)(a + b)(1 - e^{-kt}), & \text{when } x = N \end{cases}$$

where t denotes time elapsed since the event and k is a constant defined by the operator (k>0).

# Implementing time and probabilities (4)

- This way we get a probability that takes into account the uncertainty that occurs due to the passage of time.
- The initial probabilities a, b and c may have been collected by observing the operation of the sensor for a longer time period, or they may have been defined by the sensor operator.

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

# Implementing time and probabilities (5)

More generally, Let M be a finite state machine with states $A_1$, $A_2$,…,$A_n$ and initial probabilities $a_1$, $a_2$,…,$a_n$, respectively. If we get a sensor reading $A_j$, we define the new probability distribution for X as

$$P(X = x) = \begin{cases} S(A_j)a_1(1 - e^{-kt}), & \text{when } x = A_1 \\ S(A_j)a_2(1 - e^{-kt}), & \text{when } x = A_2 \\ \vdots & \\ 1 - S(A_j)(\sum_{i \neq j} a_i)(1 - e^{-kt}), & \text{when } x = A_j \\ \vdots & \\ S(A_j)a_n(1 - e^{-kt}), & \text{when } x = A_n \end{cases}$$

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK

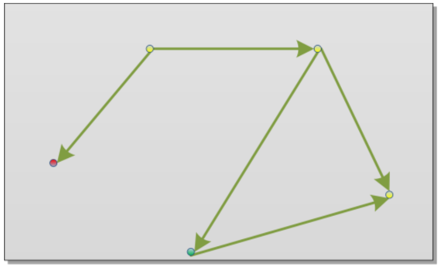
# Entropy in critical infrastructure systems

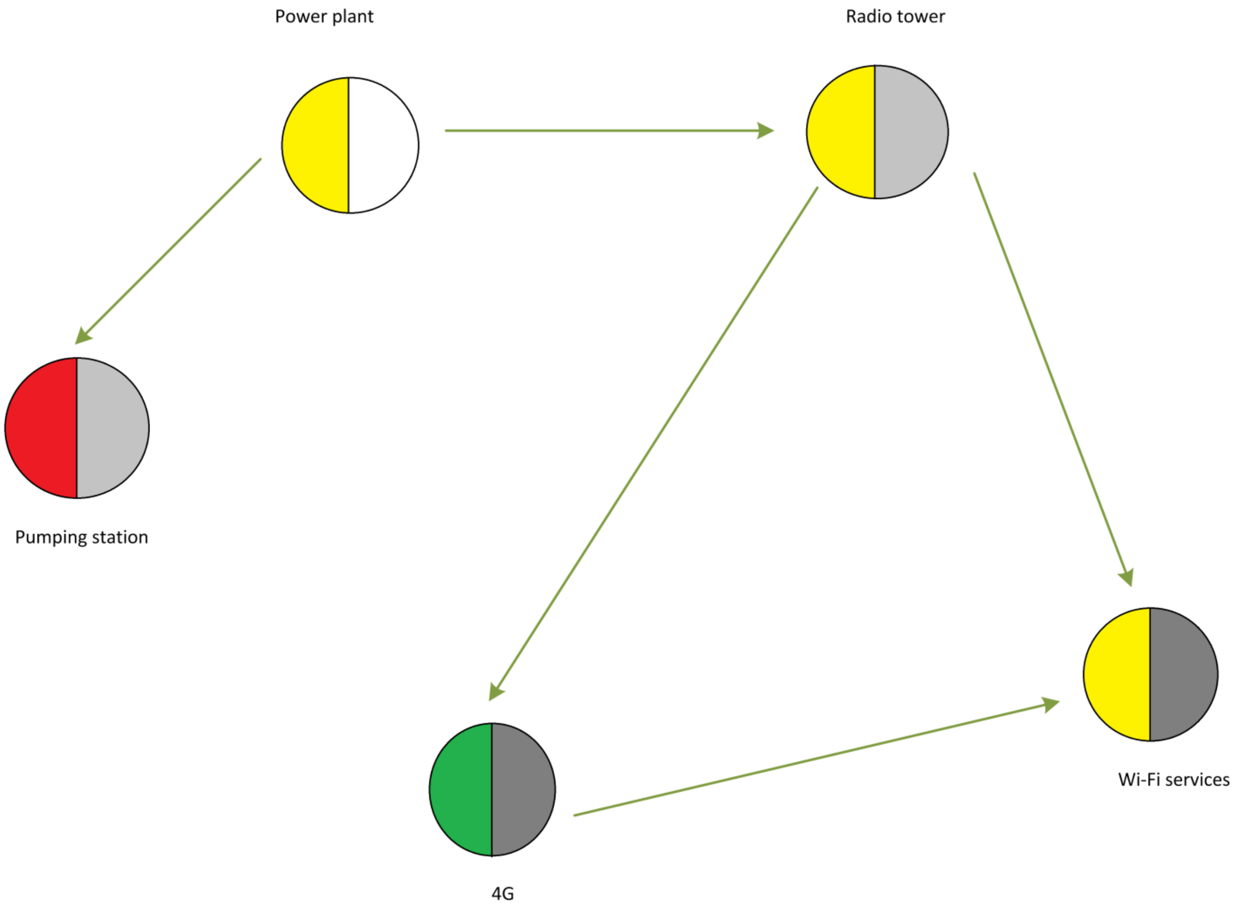
- By calculating the expected value E(S(X)), it is possible to estimate the status of the system in question.
- The entropy of the random variable X informs us of the reliability of the estimate (lower entropy being more reliable).

# Entropy in critical infrastructure system (2)

- There is no need to calculate any conditional probabilities. The causalities are taken into account by the underlying finite state machine structure.
- Setting up the system should be straightforward: Each finite state machine only requires
  - the initial probability distribution,
  - the constant k in the new distribution,
  - severity values between 0 and 1 for its states.

Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK






**Markus Klemetti, Samir Puuska**
**Sotatekniikan laitos**
**MPKK**

# Example

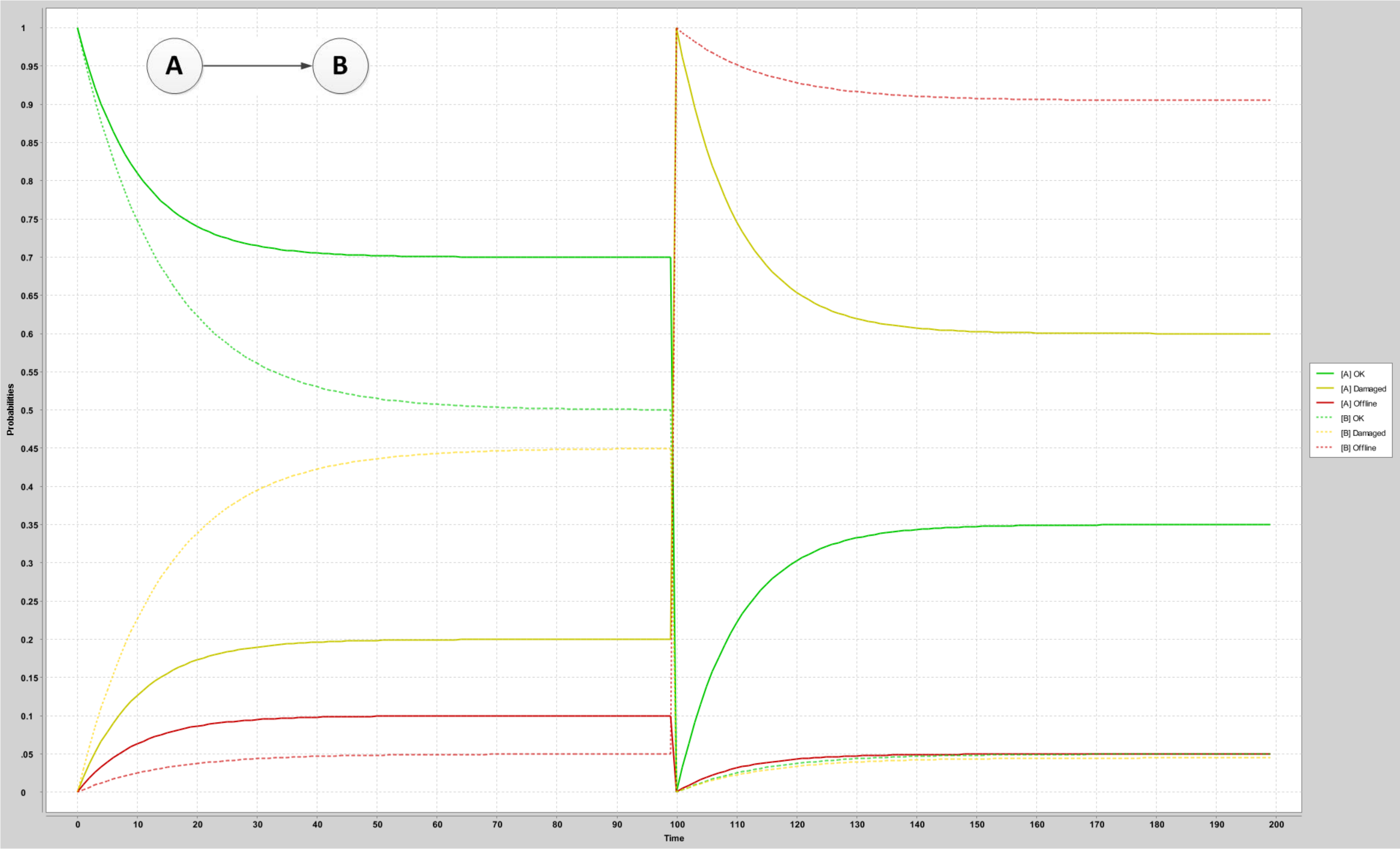
- Let A be a power plant and B be a radio tower. They each have states ”OK”, ”damaged” and ”offline”. The initial probabilities for A are

  0.7 for OK
  0.2 for damaged
  0.1 for offline

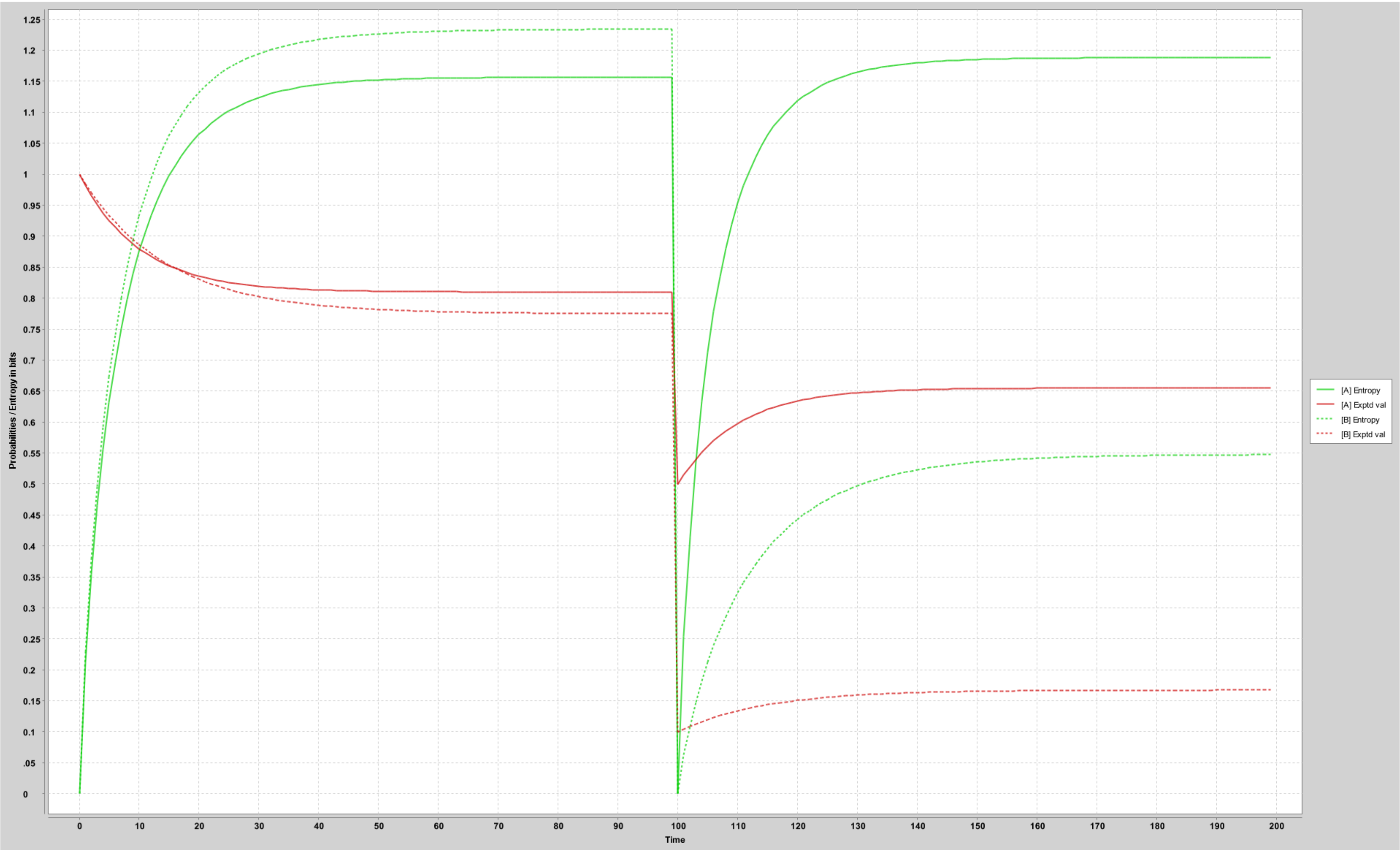
- The initial probabilities for B are

  0.5 for OK
  0.45 for damaged
  0.05 for offline

- In the beginning both A and B are known to be OK.
- When time=100 we get a sensor reading that A is damaged.




Markus Klemetti, Samir Puuska
Sotatekniikan laitos
MPKK


Probabilities / Entropy in bits
Time
[A] Entropy
[A] Exptd val
[B] Entropy
[B] Exptd val

*“Although our intellect always longs for clarity and certainty, our nature often finds uncertainty fascinating.”*

— Carl von Clausewitz

*“You should call it **entropy**, because nobody knows what entropy really is, so in a debate you will always have the advantage.”*

— John Neumann, suggestion to Claude Shannon on what to call his new formula for information