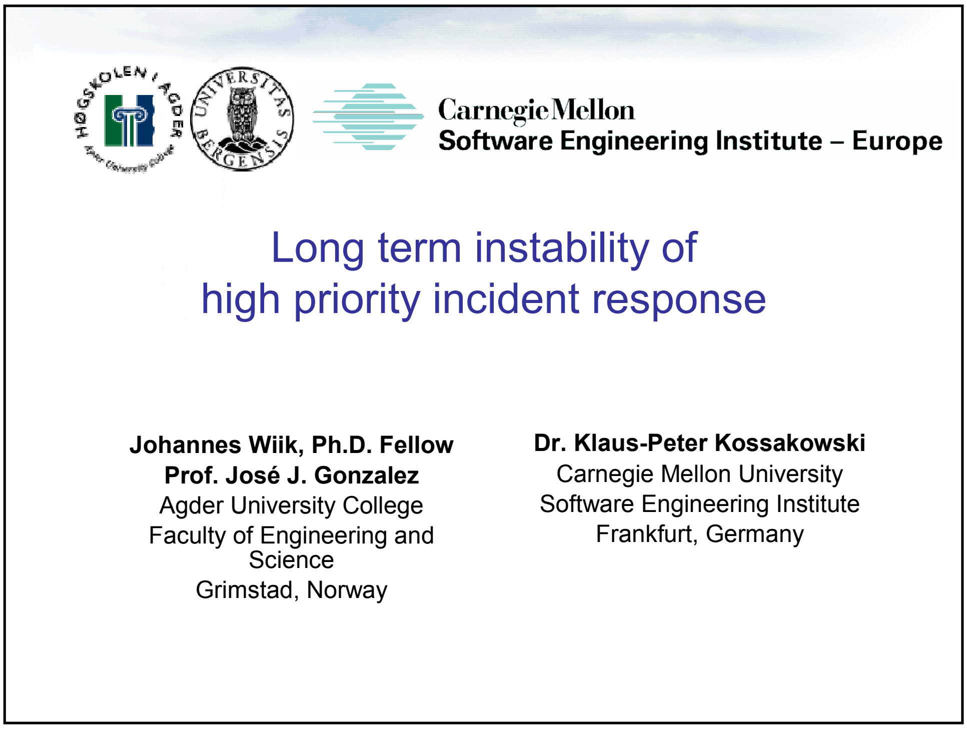
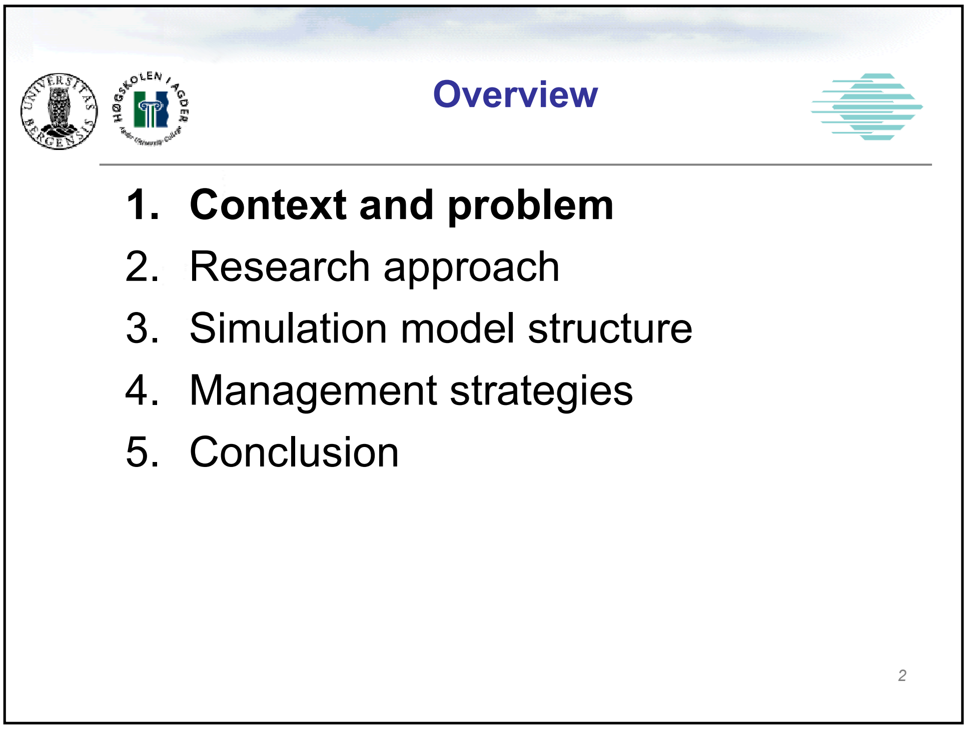


Carnegie Mellon
Software Engineering Institute – Europe

Long term instability of high priority incident response

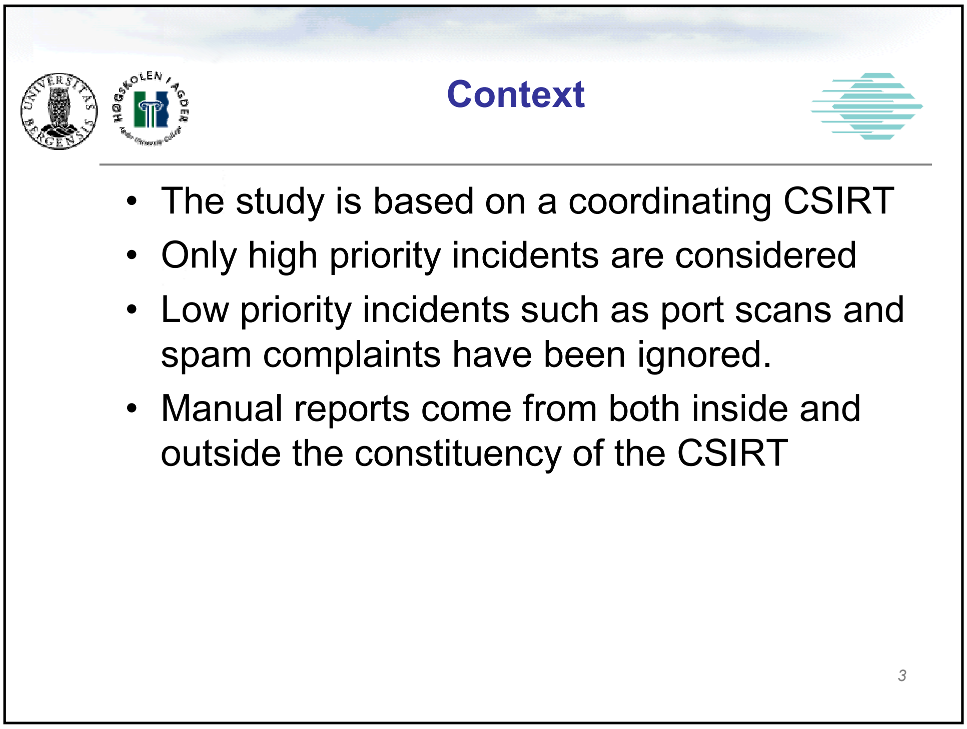
Johannes Wiik, Ph.D. Fellow
Prof. José J. Gonzalez
Agder University College
Faculty of Engineering and Science
Grimstad, Norway

Dr. Klaus-Peter Kossakowski
Carnegie Mellon University
Software Engineering Institute
Frankfurt, Germany



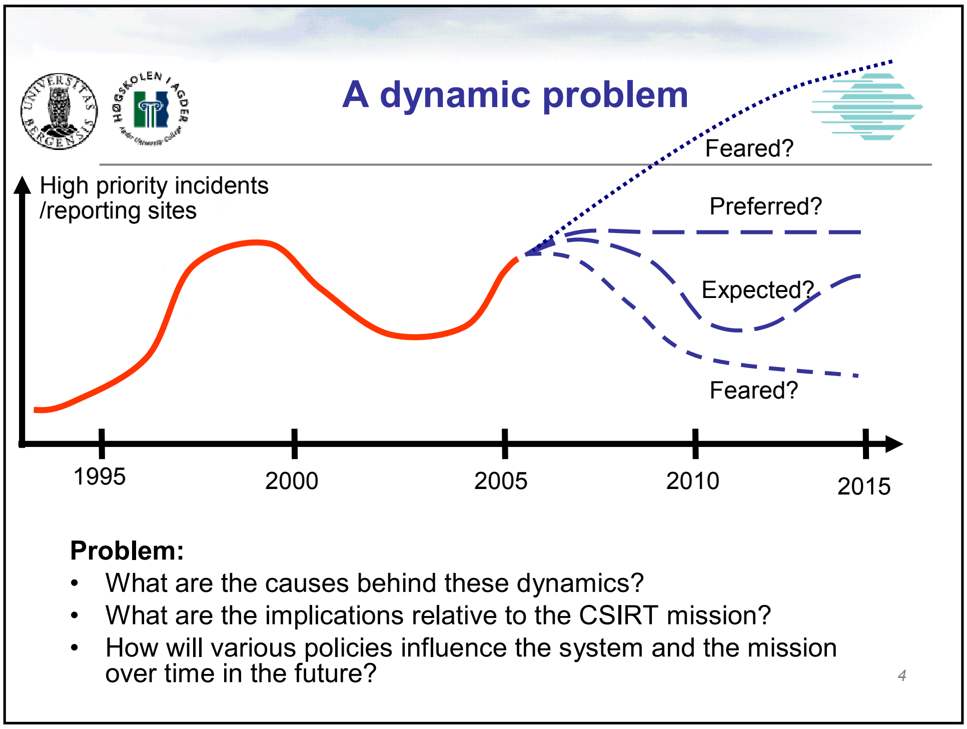
Overview

1. **Context and problem**
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion



Context

- The study is based on a coordinating CSIRT
- Only high priority incidents are considered
- Low priority incidents such as port scans and spam complaints have been ignored.
- Manual reports come from both inside and outside the constituency of the CSIRT



A dynamic problem

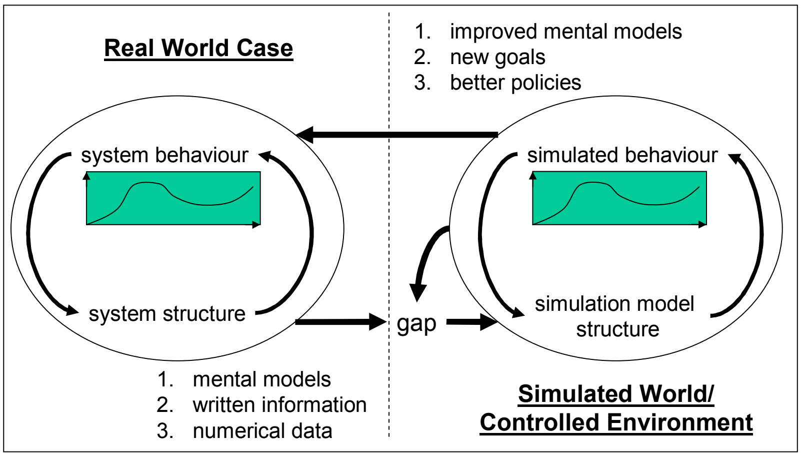
Problem:

- What are the causes behind these dynamics?
- What are the implications relative to the CSIRT mission?
- How will various policies influence the system and the mission over time in the future?

Overview

1. Context and problem
2. **Research approach**
3. Simulation model structure
4. Management strategies
5. Conclusion

Approach: Build a simulation model of the real case



Real World Case

system behaviour

system structure

1. mental models
2. written information
3. numerical data

gap

1. improved mental models
2. new goals
3. better policies

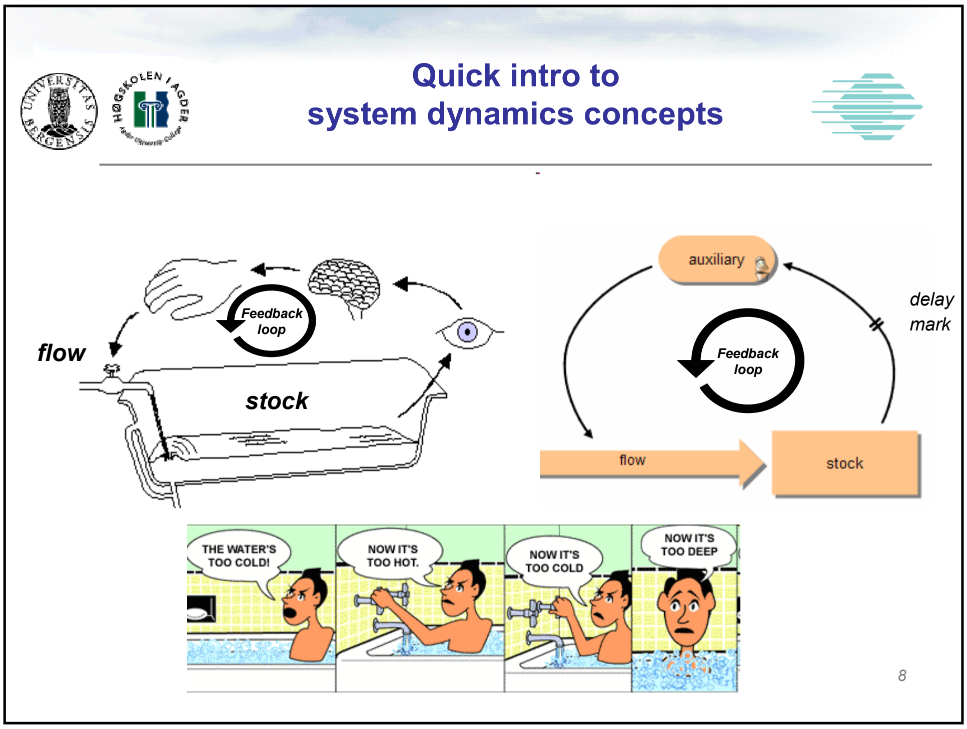
simulated behaviour

simulation model structure

Simulated World/ Controlled Environment

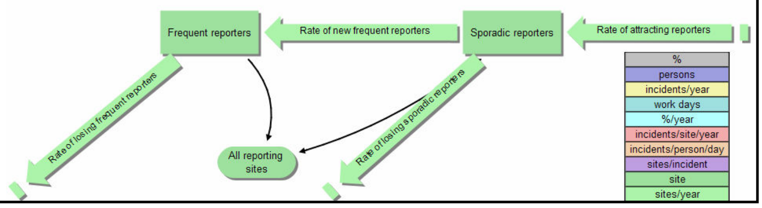
Overview

1. Context and problem
2. Research approach
3. **Simulation model structure**
4. Management strategies
5. Conclusion

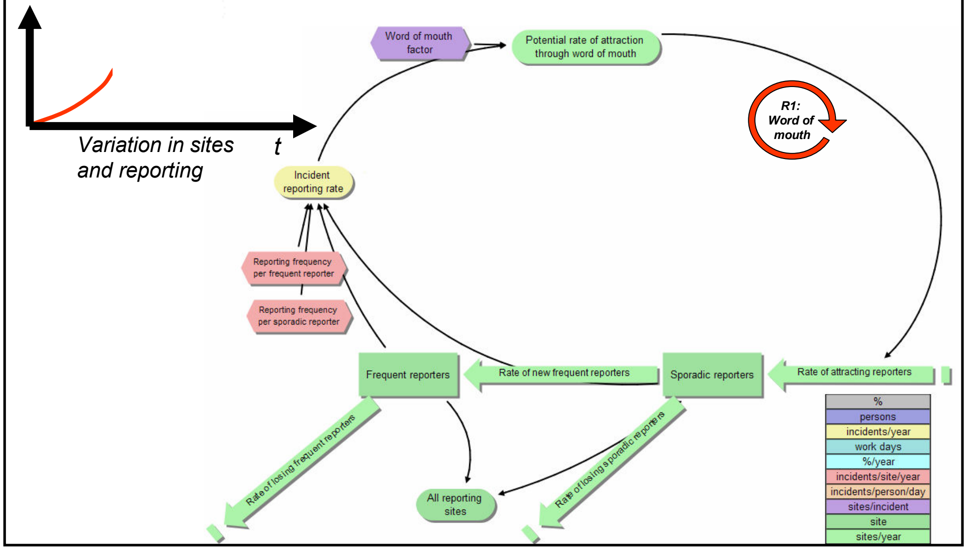


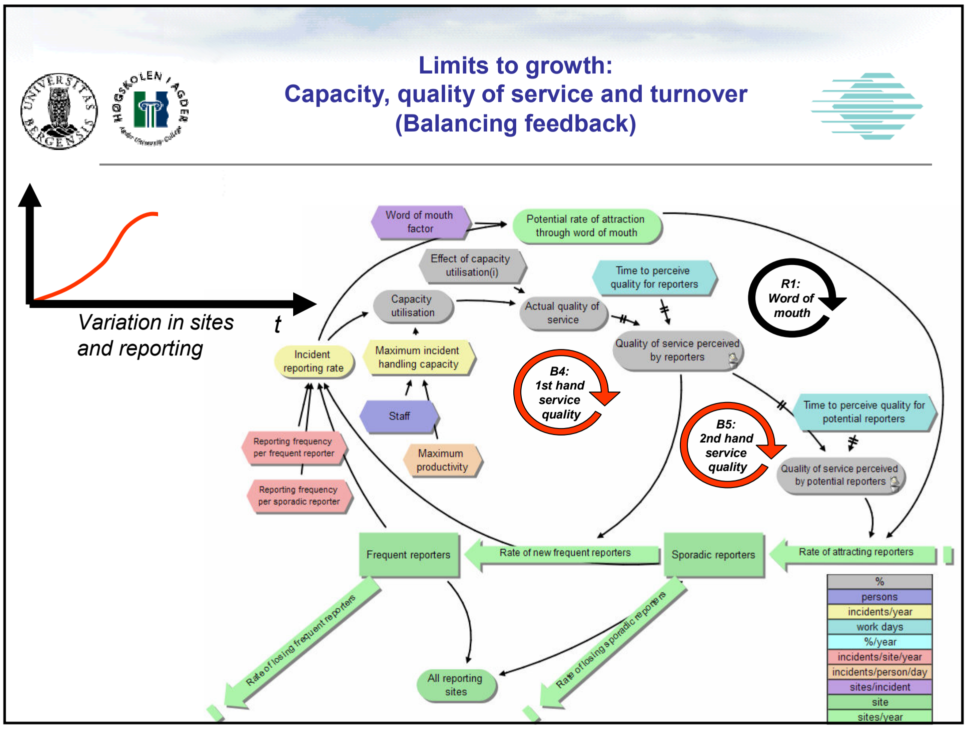
Quick intro to system dynamics concepts

Reporting sites enter and leave



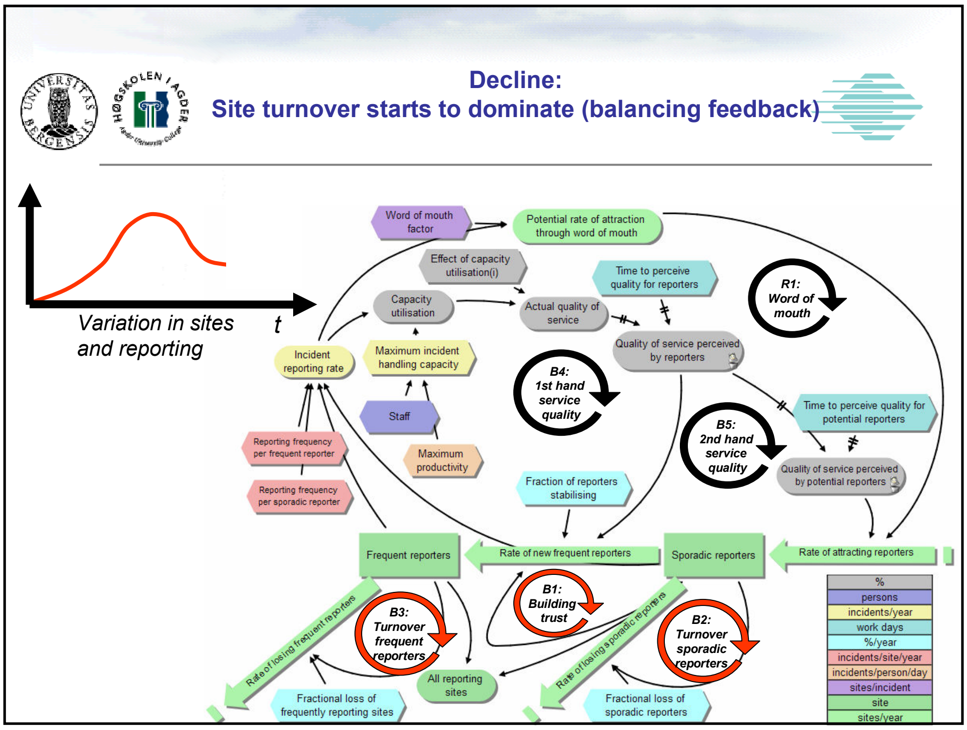
The growth process: Word of mouth (Reinforcing feedback)


Variation in sites and reporting
t
Word of mouth factor
Potential rate of attraction through word of mouth
R1: Word of mouth
Incident reporting rate
Reporting frequency per frequent reporter
Reporting frequency per sporadic reporter
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
Rate of losing frequent reporters
All reporting sites
Rate of losing sporadic reporters
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year



Limits to growth: Capacity, quality of service and turnover (Balancing feedback)

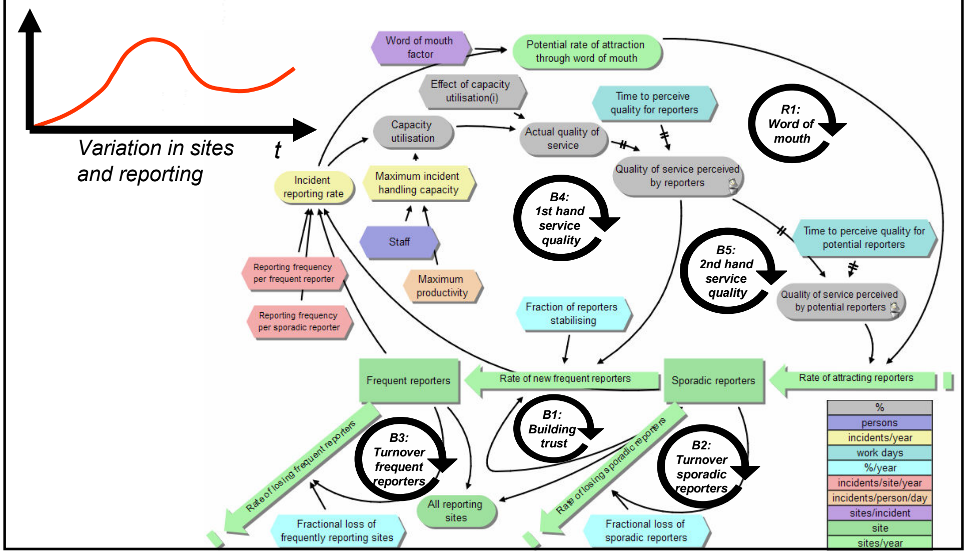
Variation in sites
and reporting
t
Word of mouth factor
Potential rate of attraction through word of mouth
Effect of capacity utilisation(i)
Time to perceive quality for reporters
R1: Word of mouth
Capacity utilisation
Actual quality of service
Quality of service perceived by reporters
Incident reporting rate
Maximum incident handling capacity
B4: 1st hand service quality
Time to perceive quality for potential reporters
Staff
B5: 2nd hand service quality
Reporting frequency per frequent reporter
Maximum productivity
Quality of service perceived by potential reporters
Reporting frequency per sporadic reporter
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
Rate of losing frequent reporters
All reporting sites
Rate of losing sporadic reporters
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year



Decline: Site turnover starts to dominate (balancing feedback)

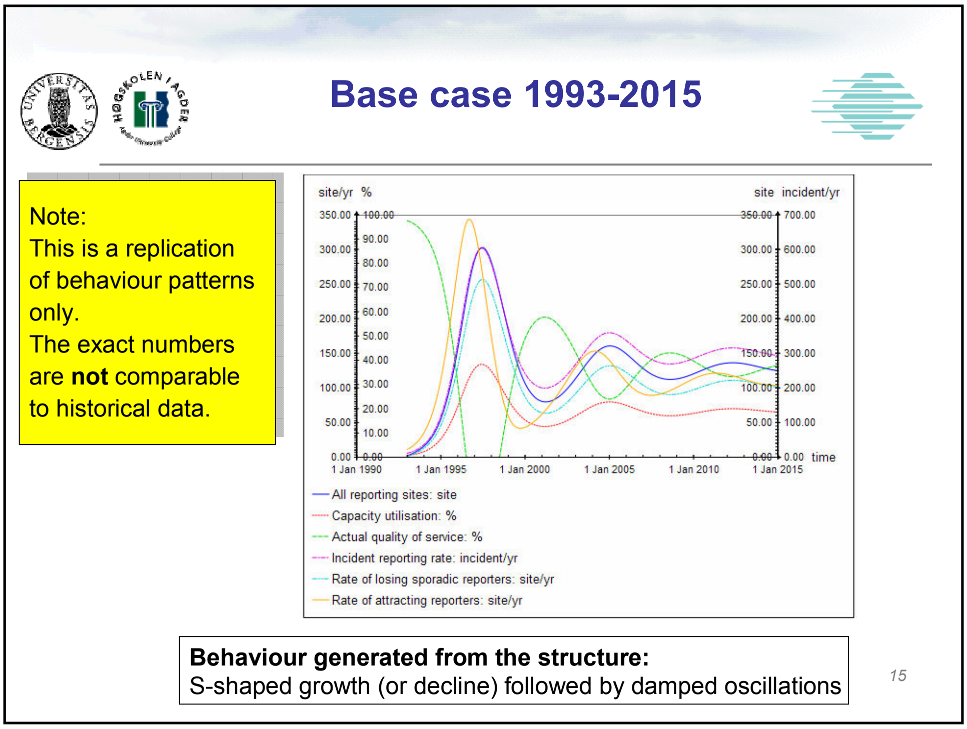
Variation in sites
and reporting
t
Word of mouth factor
Potential rate of attraction through word of mouth
Effect of capacity utilisation(i)
Time to perceive quality for reporters
R1: Word of mouth
Capacity utilisation
Actual quality of service
Quality of service perceived by reporters
Incident reporting rate
Maximum incident handling capacity
B4: 1st hand service quality
Time to perceive quality for potential reporters
Staff
B5: 2nd hand service quality
Reporting frequency per frequent reporter
Maximum productivity
Fraction of reporters stabilising
Quality of service perceived by potential reporters
Reporting frequency per sporadic reporter
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
B1: Building trust
B3: Turnover frequent reporters
B2: Turnover sporadic reporters
Rate of losing frequent reporters
All reporting sites
Rate of losing sporadic reporters
Fractional loss of frequently reporting sites
Fractional loss of sporadic reporters
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year

Overshoot, undershoot and oscillations: Changes in reporting sites and perception of quality (Delays)


Variation in sites and reporting
t
Word of mouth factor
Potential rate of attraction through word of mouth
Effect of capacity utilisation(i)
Time to perceive quality for reporters
R1: Word of mouth
Capacity utilisation
Actual quality of service
Quality of service perceived by reporters
Incident reporting rate
Maximum incident handling capacity
B4: 1st hand service quality
Staff
Maximum productivity
B5: 2nd hand service quality
Time to perceive quality for potential reporters
Quality of service perceived by potential reporters
Reporting frequency per frequent reporter
Reporting frequency per sporadic reporter
Fraction of reporters stabilising
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
B1: Building trust
B3: Turnover frequent reporters
B2: Turnover sporadic reporters
Rate of losing frequent reporters
Rate of losing sporadic reporters
All reporting sites
Fractional loss of frequently reporting sites
Fractional loss of sporadic reporters
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year

Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. **Management strategies**
5. Conclusion

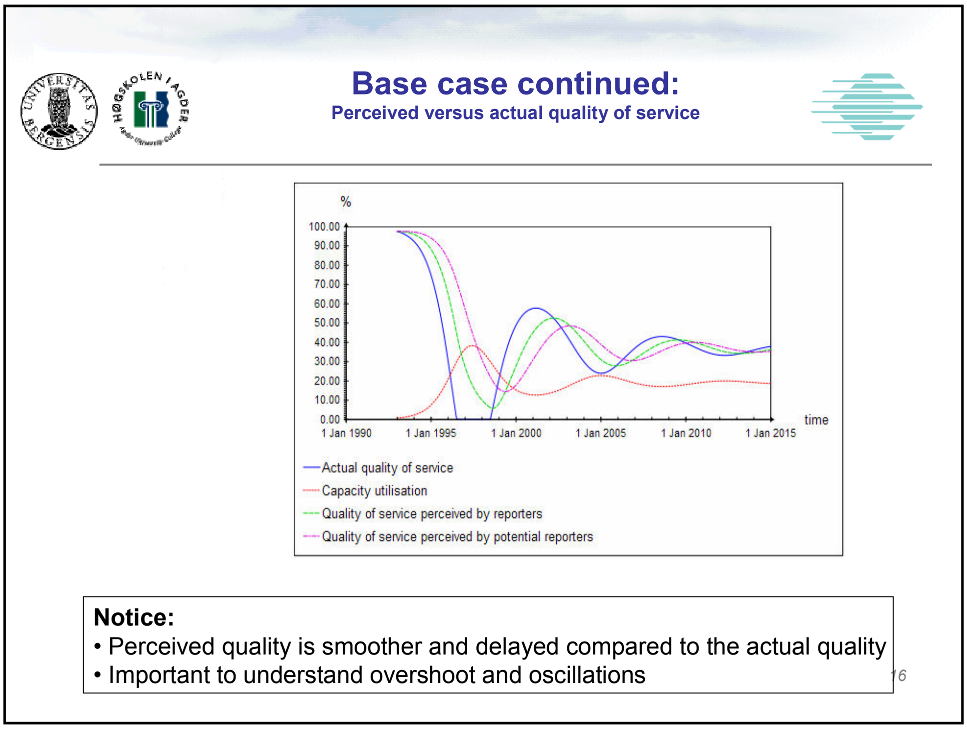


Base case 1993-2015

Note:
This is a replication of behaviour patterns only.
The exact numbers are **not** comparable to historical data.

Behaviour generated from the structure:
S-shaped growth (or decline) followed by damped oscillations

15



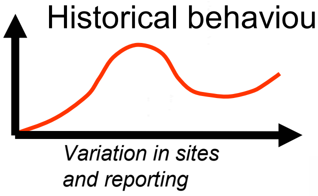
Base case continued:

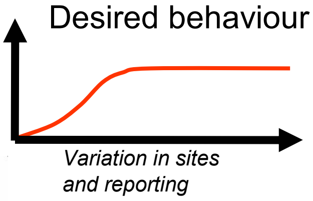
Perceived versus actual quality of service

Notice:
- Perceived quality is smoother and delayed compared to the actual quality
- Important to understand overshoot and oscillations

16

A new goal:
Stable balance



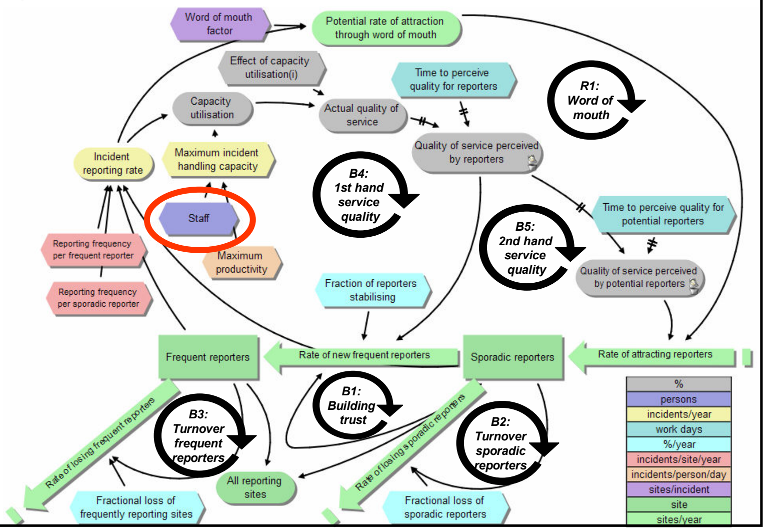


workload/
reporting

workforce/
capacity

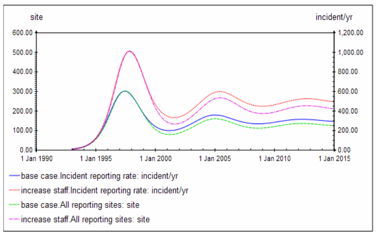
17

What-if 1:
We double the staff


Word of mouth factor
Potential rate of attraction through word of mouth
Effect of capacity utilisation(i)
Time to perceive quality for reporters
R1: Word of mouth
Capacity utilisation
Actual quality of service
Quality of service perceived by reporters
Incident reporting rate
Maximum incident handling capacity
B4: 1st hand service quality
Staff
Time to perceive quality for potential reporters
B5: 2nd hand service quality
Reporting frequency per frequent reporter
Maximum productivity
Quality of service perceived by potential reporters
Reporting frequency per sporadic reporter
Fraction of reporters stabilising
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
B1: Building trust
B3: Turnover frequent reporters
B2: Turnover sporadic reporters
Rate of losing frequent reporters
Rate of losing sporadic reporters
All reporting sites
Fractional loss of frequently reporting sites
Fractional loss of sporadic reporters

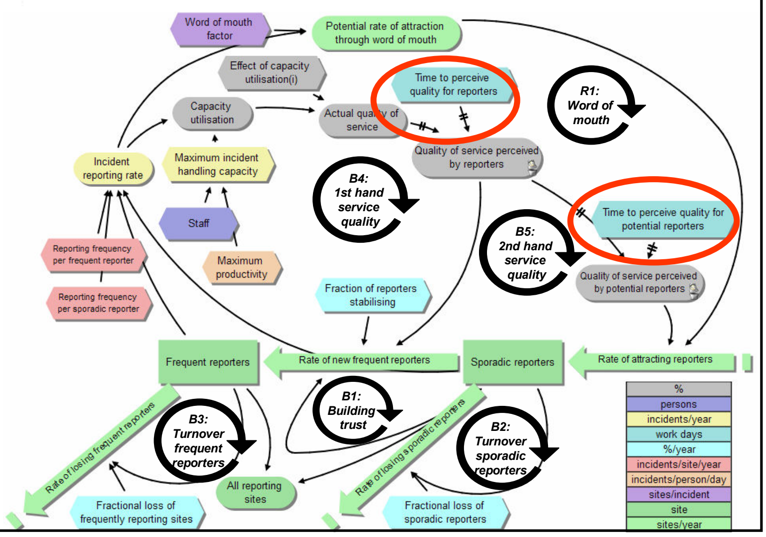
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year

What-if 1:
We double the staff?

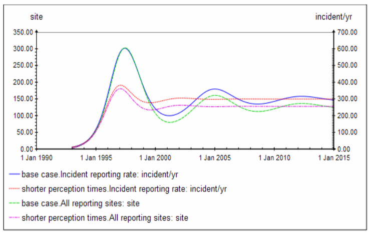


1. No change in behaviour pattern
2. The system adjusts to the new situation, but the problem persists (and gets slightly worse)
3. A fix that fails! Counterintuitive?

What-if 1:
We reduce perception times to half?


Word of mouth factor
Potential rate of attraction through word of mouth
Effect of capacity utilisation(i)
Time to perceive quality for reporters
R1: Word of mouth
Capacity utilisation
Actual quality of service
Quality of service perceived by reporters
Incident reporting rate
Maximum incident handling capacity
B4: 1st hand service quality
Staff
Time to perceive quality for potential reporters
B5: 2nd hand service quality
Reporting frequency per frequent reporter
Maximum productivity
Quality of service perceived by potential reporters
Reporting frequency per sporadic reporter
Fraction of reporters stabilising
Frequent reporters
Rate of new frequent reporters
Sporadic reporters
Rate of attracting reporters
B1: Building trust
B3: Turnover frequent reporters
Rate of losing frequent reporters
B2: Turnover sporadic reporters
Rate of losing sporadic reporters
All reporting sites
Fractional loss of frequently reporting sites
Fractional loss of sporadic reporters
%
persons
incidents/year
work days
%/year
incidents/site/year
incidents/person/day
sites/incident
site
sites/year

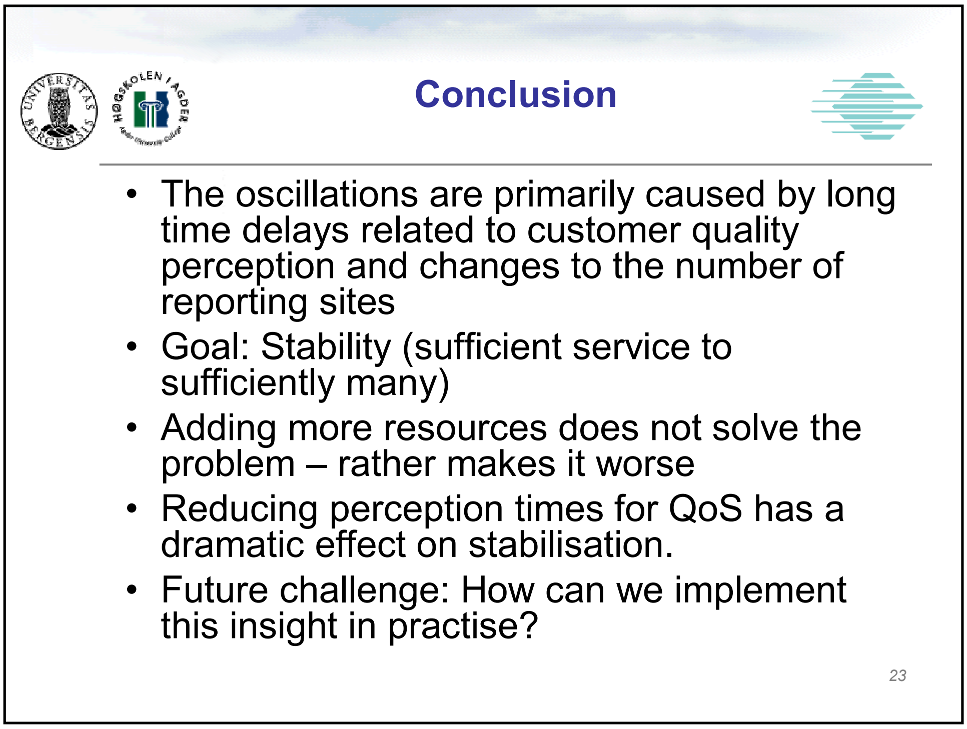
What-if 2:
We halve perception times?



- Significant stabilisation of workload and reporting sites
- What does this mean? How can this be done?

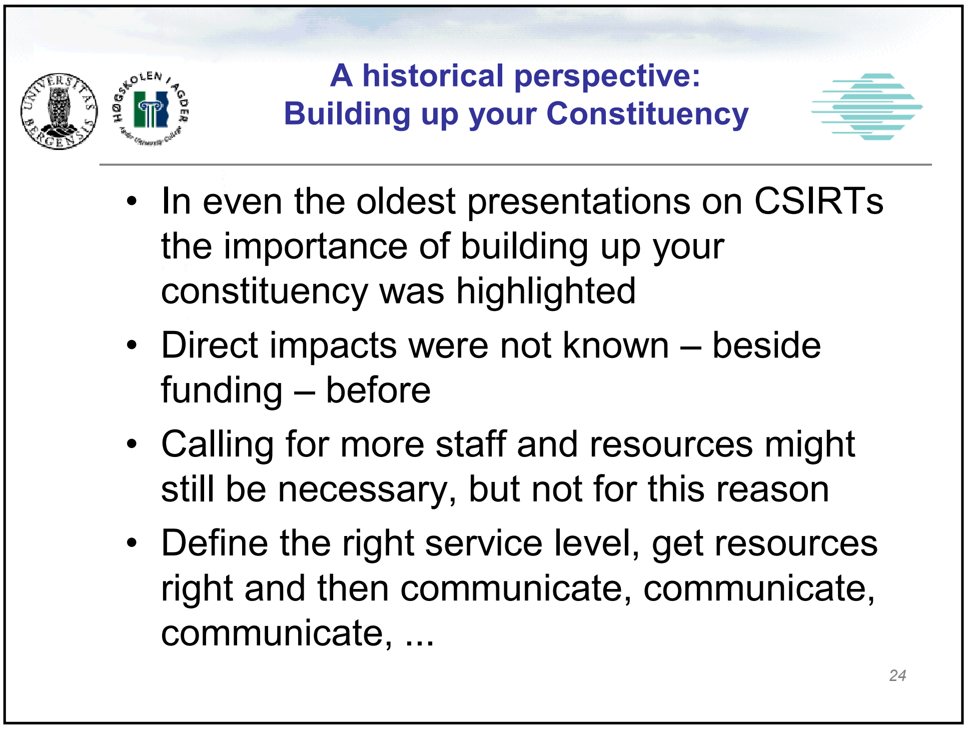
Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. **Conclusion**



Conclusion

- The oscillations are primarily caused by long time delays related to customer quality perception and changes to the number of reporting sites
- Goal: Stability (sufficient service to sufficiently many)
- Adding more resources does not solve the problem – rather makes it worse
- Reducing perception times for QoS has a dramatic effect on stabilisation.
- Future challenge: How can we implement this insight in practise?



A historical perspective: Building up your Constituency

- In even the oldest presentations on CSIRTs the importance of building up your constituency was highlighted
- Direct impacts were not known – beside funding – before
- Calling for more staff and resources might still be necessary, but not for this reason
- Define the right service level, get resources right and then communicate, communicate, communicate, ...