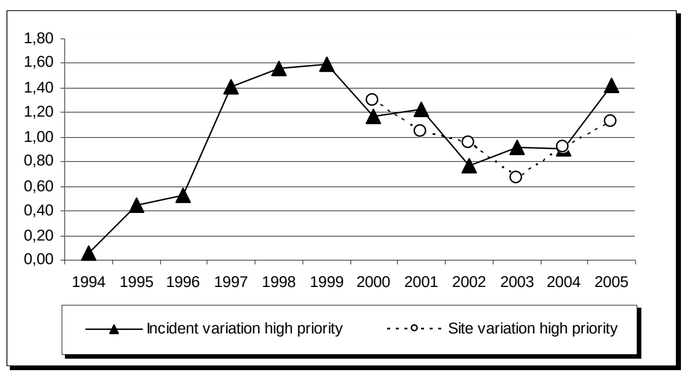
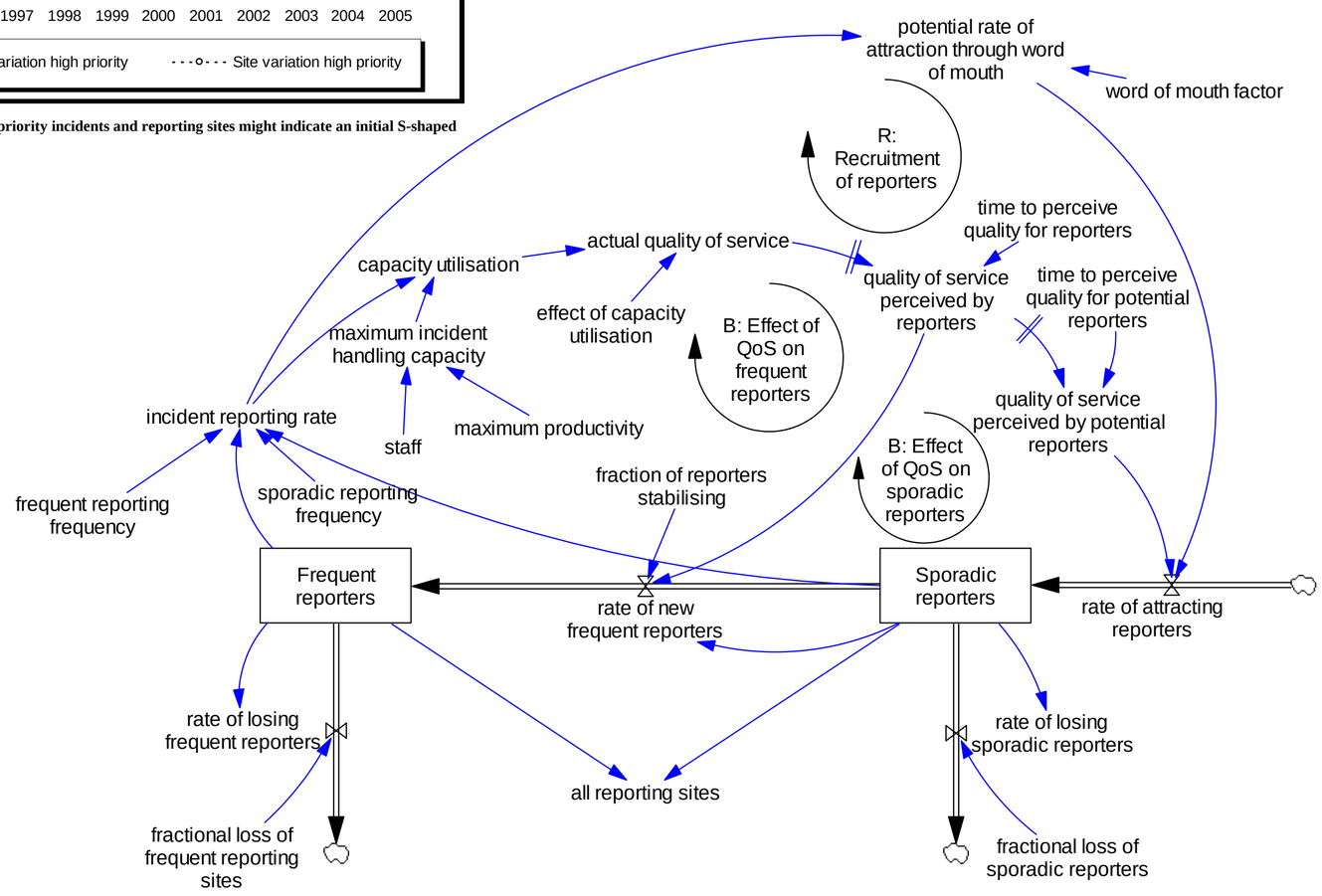
Persistent instabilities in the high-priority incident workload of CSIRTs

- Goal: To mitigate long-term instability in the workload and quality of service
- Object of study: high priority incidents in CSIRTs
- How: Workshops, face-to-face meetings, frequent teleconferences & virtual meetings with managing director and staff of CSIRT.
- Access to numerical data, docs and mental models
- Partner: One of Europe's largest and oldest coordinating CSIRTs
- CSIRT= Computer Security Incident Response Team



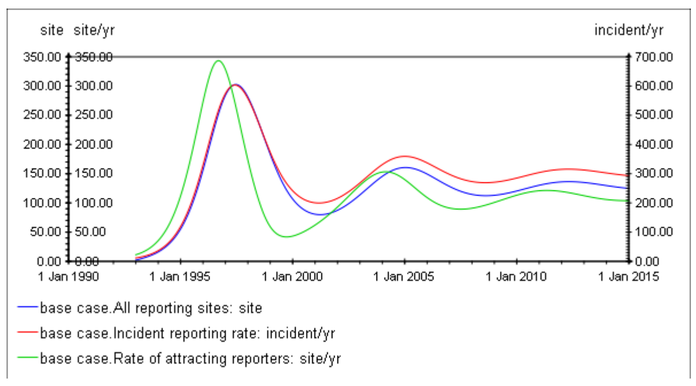
The fractional variation of high-priority incidents and reporting sites might indicate an initial S-shaped growth, followed by oscillations



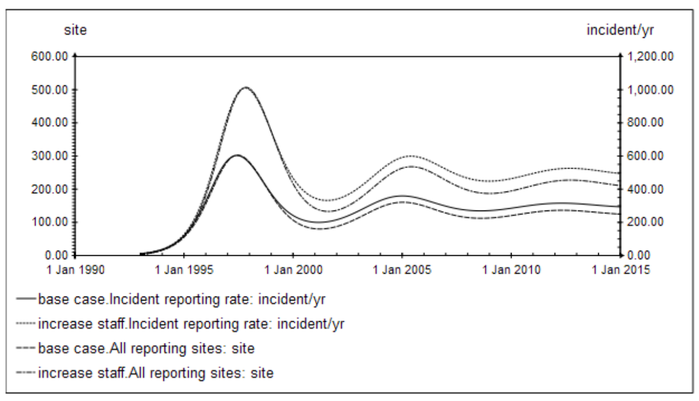
Despite the lack of site information for 1994-99, interviews with staff indicate that nos. of reporting sites had followed the same pattern as the high-priority incidents

Two groups of reporting sites: 1) Frequently reporting sites; 2) Sporadically reporting sites.

Recruitment rates depend on perceived QoS



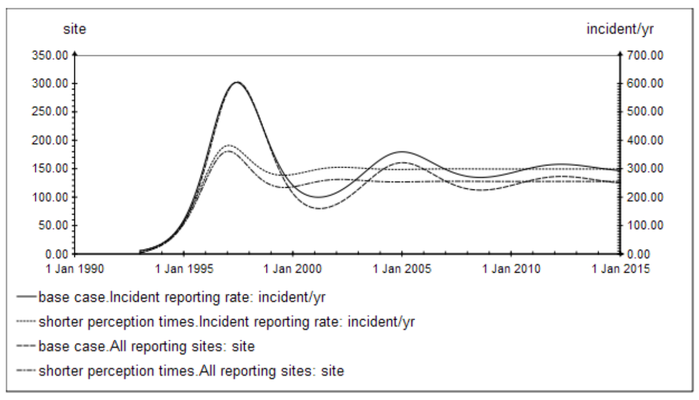
The base case shows a replication of the historical pattern for the incident reporting rate and the number of reporting sites (S-shaped growth, with ensuing overshoot and oscillations). The time horizon has been extended to 2015 to assess expected future development based on the model assumptions.



Adding more resources does not solve the problem. Owing to compensating feedback the workload will adjust to the new resources level, and S-shaped growth, overshoot and oscillations will follow with even larger amplitudes

Base Run: Initial S-shaped growth followed by damped oscillations, implying waste of resources and problems with QoS

Improving communication with clients and potential clients (reporting sites) to reduce perception times of level of service helps stabilize the oscillatory behaviour



Shortening the perception times tends to stabilize the workload for the CSIRT

Johannes Wiik[1], Jose J. Gonzalez[2], Pål I. Davidsen[3], Klaus-Peter Kossakowski[4]
[1]University of Agder, Faculty of Engineering and Science, Department of ICT, 4898 Grimstad, Norway
[2]University of Agder, Faculty of Engineering and Science, Department of ICT, 4898 Grimstad, Norway
[2]NISlab, Gjøvik University College, 2802 Gjøvik, Norway
[3]Institute for geography, University of Bergen, 5020 Bergen, Norway
[4]SEI Europe, Carnegie Mellon University, 60 322 Frankfurt, Germany

UNIVERSITY OF AGDER