Software Dependability under Emergency Conditions

Kim Weyns and Per Runeson
Department of Communication Systems, Lund University
P.O. Box 118, SE-211 00 LUND, Sweden
kim.weyns@telecom.lth.se

Abstract

Many governmental actors have an operative responsibility in times of emergency. For this task they are becoming more and more dependent on IT systems. First interviews with some emergency managers show that traditional emergency management and risk analysis not always manages to capture this critical dependency. The exact dependence on IT systems in a crisis is often hard to predict, and the reliability of these systems under special emergency conditions is hard to evaluate.

1. Introduction

Crises like earthquakes, power blackouts or terrorist attacks can disturb the normal workings of society and at the same time put an increased stress on the technical systems on which society depends in a time of emergency. In the aftermath of such a crisis, municipalities, regional governments and government agencies have an important role in the relief and recovery efforts.

During the last decade most government actors have become more and more dependent on software systems, both for their normal everyday tasks and for their roles in emergency situations. And for these tasks they often depend on both specially designed critical systems (such as the communication systems for emergency services) and normal commercial systems (such as the public telephone networks).

Most companies can afford a short interruption in their work flow during such exceptional events, usually resulting in some economic damage for which insurance is available. On the other hand, for many government actors a short period of inactivity is sometimes acceptable under normal working conditions, but absolutely unacceptable during crisis conditions, when their availability is critical and any hour of unavailability can cost many human lives.

This need for a high availability during extreme conditions poses special requirements on the dependability of their IT systems. Typical systems that are not highly critical under normal conditions but that can become critical under crisis conditions are for example telecommunication systems, geographical information systems (GIS) and demographic information systems.

2. Risk Analysis

For a government actor to evaluate its dependence on different IT systems requires a coordinated risk analysis, taking into account the effects of possible crises on those systems and an estimate of the reliability of these systems under crisis conditions.

In Sweden the Swedish Emergency Management Agency (SEMA) **Error! Reference source not found.** requires all governmental actors to conduct risk analyses for all their responsibilities with special attention for extreme events. Many techniques are available to conduct these risk analyses and with respect to crisis preparedness they are often scenario-based. These risk analyses are usually conducted by specially appointed emergency managers.

At the same time SEMA is also the author of a series of recommendations under the title ‘Basic level for IT Security (BITS)’ **Error! Reference source not found.**, mainly based on the ISO/IEC 17799 standard . This document, together with the original standard, is used by the IT-units of many Swedish government actors to obtain a basic level of IT dependability and to conduct risk analysis on their IT systems.

A first survey of some government actors has shown that the risk analyses on these two levels are not sufficiently coordinated. The emergency managers have problems to determine the dependability of the different systems they depend upon, and often have an over confidence in these systems. And the technical staff managing the IT systems often do not have the complete picture of the dependability requirements

that are posed upon the different systems they have responsibility for.

In practice, when an emergency does occur, unforeseen shortcomings in the dependability of the IT systems are often discovered.

For example, when the storm "Gudrun" hit Sweden in January 2005, a number of technical shortcomings in the telecommunications systems used in crisis relief were discovered. The storm damaged some important electricity and telecommunication lines and some mobile communication base stations, both directly and through power outage. The special conditions created by the storm revealed a critical need for more roaming across different mobile networks, and a shortage of power generators to power all the telecommunication systems during a blackout.

First research also shows that there is a big difference in how far different governmental actors have come in analysing there dependence on IT systems. Mostly larger cities and government actors from industries with a traditionally strong focus on safety (such as the transport sector) have come much further in this than smaller towns or counties.

3. Evaluating reliability

At the same time, the evaluation of the reliability of IT systems in extraordinary situations is very hard. Many of the possible extreme events in which a system is critical hopefully never happen in the whole lifetime of the system. Often the only historical data that is available is either from some few very specific crises or from emergency exercises conducted. These exercises can only achieve a limited level of realism, and are usually expensive to conduct. While the collection of data is very slow, the IT systems change very often, and the effect of these changes on the dependability of the system is not always clear.

For testing systems under crisis conditions usage profiles are needed, but in practice it is often hard to predict the exact usage of a given system in an emergency situation. A crisis can stress an IT system in unexpected ways, from the simultaneous failure of many components to an increase in input errors because of stressed operators.

4. Conclusion

Because our dependence on IT systems in crises is continuously increasing, there is an urgent need for more research on practical techniques to evaluate the reliability of software systems in emergency situations.

First research shows that there is especially need for a method that supports the coordination between technical and operational risk analysis. Of course the method should connect well to both current technical and operational risk analysis techniques.

Preferably the method should also support the decision-making process when installing a new system to help find the reliability requirements for such a system. The method should also be flexible to easily allow a re-evaluation of the dependence in the case of small changes in the actor's responsibilities or the interdependencies between the technical systems.

Because not all actors have the same resources to do these risk analyses equally thorough, the method should be flexible enough to be usable on a basic level with limited resources.

5. Acknowledgements

The work is partly funded by the Swedish Emergency Management Agency under grant for FRIVA, Framework Programme for Risk and Vulnerability Analysis of Technological and Social Systems, and partly by the Swedish Research Council under grant 622-2004-552 for a senior researcher position in software engineering

6. References

[1] http://www.krisberedskapsmyndigheten.se/

[2] SEMA, *Basic level for information security (BITS)*, Edita, Västerås 2006.

[3] ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management, International Organization for Standardization, 2005

LUND UNIVERSITY

Dependability of Software Systems in Crisis Situations

Kim Weyns, PhD student
Lund University, Sweden
kim.weyns@telecom.lth.se
http://serg.telecom.lth.se

IT Systems in Crisis Situations

- In the aftermath of a crisis (natural disaster, blackout, terrorist attack, …) governmental actors have an important role
  - Crisis relief
  - Information
    - » Dependence on IT systems

Solving a crisis:

- Storm Gudrun, Januari 2005
- Non-functioning communication system delayed repairs and relief efforts

Information flow in a crisis

[030911, 11:10]

Anna Lindh död – industriledare visar deltagande

Utrikesminister Anna Lindh avled i morse av de skador hon fick vid ett knivöverfall i Stockholm under gårdagen. Företrädare för svensk industri uttrycker sitt deltagande.

Anna Lindh

"Anna Lindh lämnar

Efter det att nyheten webbplatser med nyh överbelastning.

Text: Håkan Abrahamson

URL: http://www.nyteknik.se/pub/ipsart.asp?art_id=30066

When the news about the death of Anna Lindh was made public, most Swedish news websites were overloaded. Also, the government website was overloaded.

Simple Example

- Which IT systems should have backup power ?
  - Company
    - Most critical systems (based on economical impact of loss, …)
  - Governmental actor
    - Most critical systems IN THE EVENT OF A BLACKOUT

Governmental actors

- More urgent responsibilities in a crisis
  - Local government (county, municipality)
  - National government
- Systems that are only critical in very specific crisis situations
- Both special and COTS systems

Risk Analysis

- Emergency Management
  - Planning, Scenario analysis, … (SEMA)

- Technical Risk Analysis
  - ISO 17799/27001, Basic level for IT Security (BITS), FTA, FMECA, …

Usage Profiles in Crisis Situations

Predicting software reliability in crisis situations:

- Traditional way:
  - Testing according to the expected usage profile
- For crisis situations:
  - Often a higher reliability is required
  - Usage of the system can be substantially different from normal, and harder to predict
  - Overall system reliability is not necessarily a good measure of crisis reliability
  - Lack of historic data

Practical approach

Case studies at Swedish Crisis Actors:

- Identification of critical IT systems
- IT systems in Risk Analysis
- Standards used
- Past problems, Failure reports
- Reliability Requirements, Acceptance Testing
- …

Conclusion

- Increasing dependence on IT systems in crisis situations
- Need for
  - More research
  - Awareness of problem
  - techniques for connecting scenario analysis and technical risk analysis
    - Supporting evaluation and acquisition