Applications of STPA in Software Testing

Anders Dinsen

Consulting Test Manager

Copenhagen Denmark

@andersdinsen
ad@asym.dk

Case: Debt collection in the public sector in Denmark

@andersdinsen
ad@asym.dk

Legal and efficient debt collection

Diagram contents: Claimant collection processes, Case workers, Legacy collection processes, Automated collection processes, Claimants, Claim data processing, Debtors, Payment processing
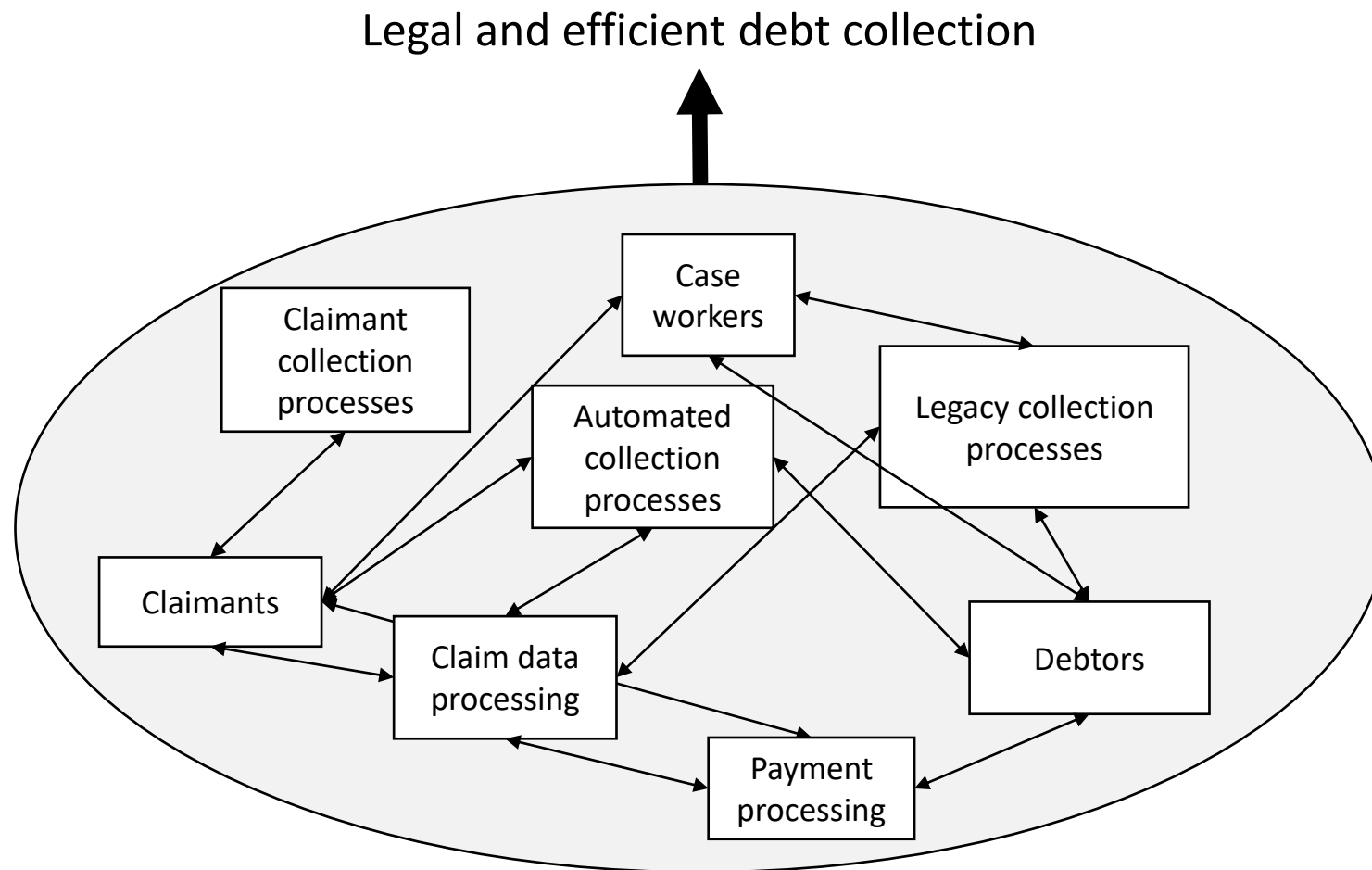
- Debt collection to all of the the public sector is centralized in a government agency.

- It has many automated and case-worker initiated automated processes.

- Legality is obviously important but is not trivial.

- Legality is an emergent property similar to safety in socio-technical systems.

- Another emergent property of such a system is efficiency, i.e. how efficiently can it collect debt.

The importance of verbal abstraction

@andersdinsen
ad@asym.dk
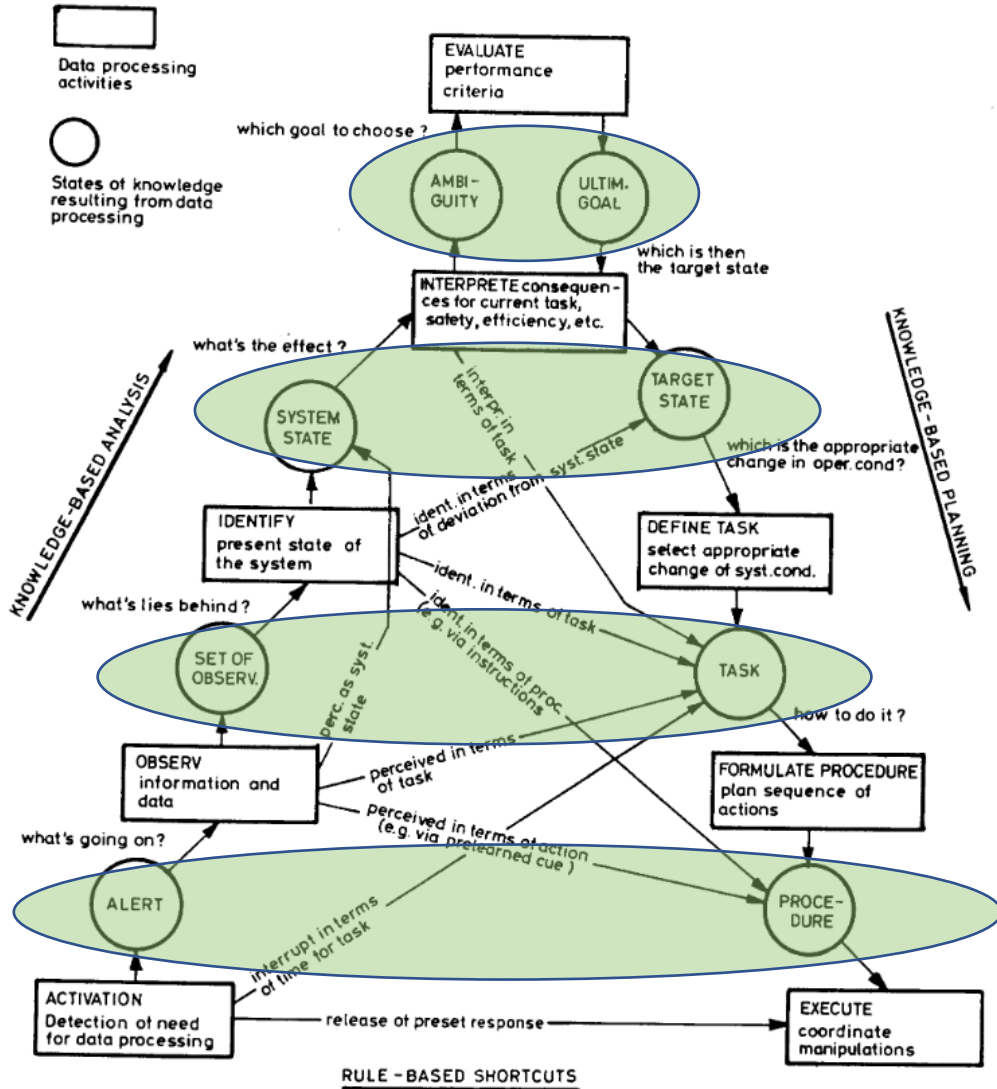
Jens Rasmussen (1982) analyzed verbal protocols developing a model of possible decision sequences of human operators in industrial processs plants.

This identified a number of statements of "states of knowledge" which can be arranged in a rational sequence.

These states of knowledge can be found too when testing pure software systems:

- A bug or defect found in testing represents an alert to someone
- The analysis of observations can trigger tasks or further analysis: Is there a requirement breach
- Further analysis will dive into the possible effects and outcomes of the defect.
- A state of ambiguity is often reached in which we need to decide how to act on a bug.

From Jens Rasmussen, Morten Lind: A Model of Human Decision Making in Complex Systems and its Use for Design of System Control Strategies, 1982

Data processing activities

States of knowledge resulting from data processing

EVALUATE performance criteria

which goal to choose ?

AMBI-GUITY   ULTIM. GOAL

which is then the target state

INTERPRETE consequen-ces for current task, safety, efficiency, etc.

what's the effect ?

SYSTEM STATE   TARGET STATE

interpr. in terms of task

which is the appropriate change in oper. cond?

IDENTIFY present state of the system

ident. in terms of deviation from syst. state

DEFINE TASK select appropriate change of syst.cond.

ident. in terms of task

what's lies behind ?

SET OF OBSERV.

perc. as syst. state

ident. in terms of proc. (e.g. via instructions)

TASK

how to do it ?

OBSERV information and data

perceived in terms of task

FORMULATE PROCEDURE plan sequence of actions

what's going on ?

perceived in terms of action (e.g. via prelearned cue)

ALERT

interrupt in terms of time for task

PROCE-DURE

ACTIVATION Detection of need for data processing

release of preset response

EXECUTE coordinate manipulations

KNOWLEDGE-BASED ANALYSIS

KNOWLEDGE-BASED PLANNING

RULE-BASED SHORTCUTS

Asbtractly Defining Testing

@andersdinsen
ad@asym.dk

Emergent properties
Increasing complexity

Fact – Cause – Observation
- "A test can prove the precense of a bug, not its absence" (P. W. Dijkstra, 1969).
- Explorative testing is still a very important testing method.

Goal – Result
- Software testing has been used to systematically test and validate systems against requirements at least since the early 1970's.
- Various test engineering and analysis methods are employed to do this.

Purpose – Effect
- As digitization transforms businesses measuring the effects on business becomes important.
- Tradesmen of the Roman empire used to melt gold in the testa, a clay pot, to prove its value.
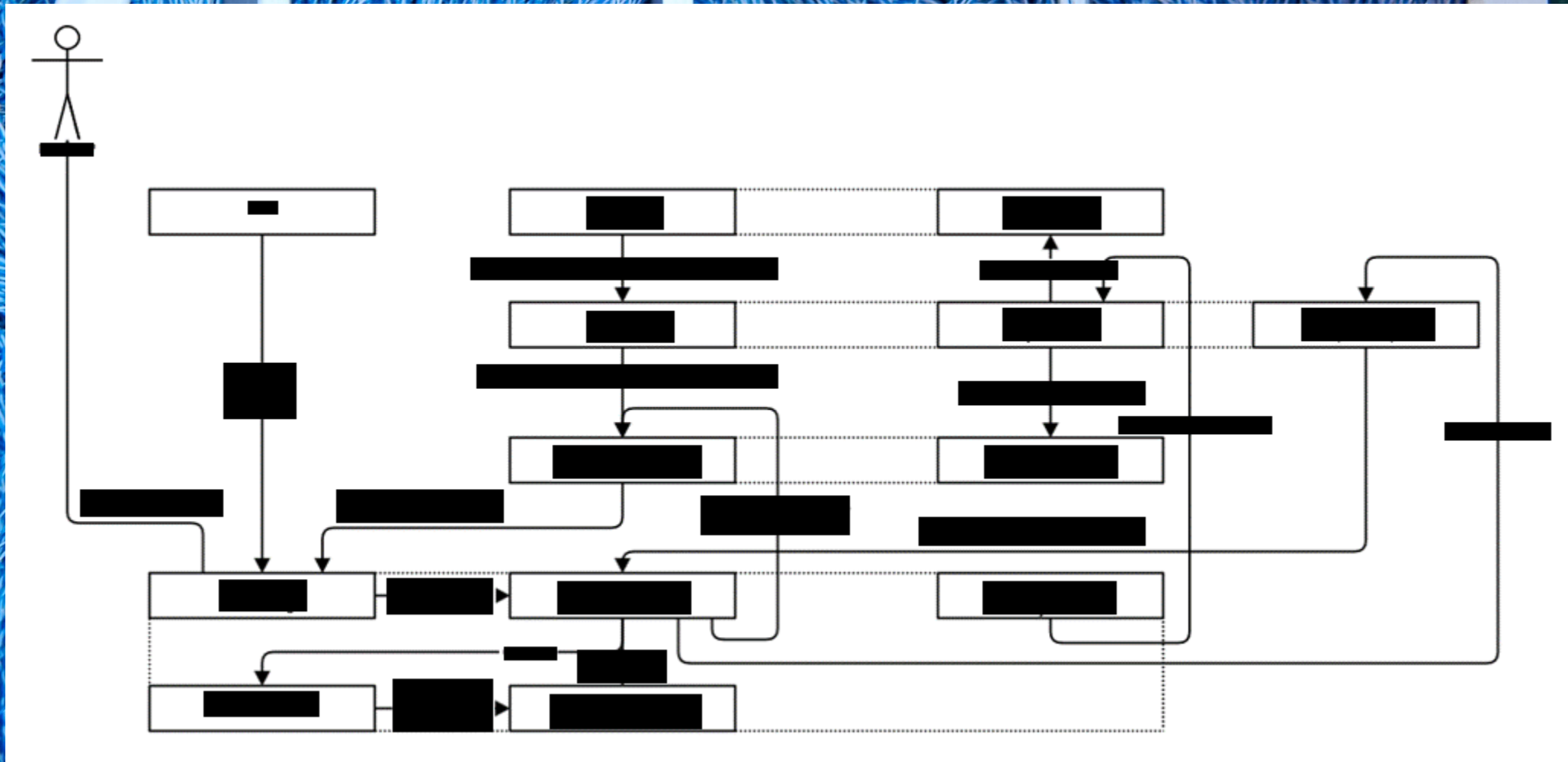
Meaning – Value
- "Quality is value to some person" (G. Weinberg)
- Performance, safety, and security testing is becoming increasingly important

The problem of 'testability'

@andersdinsen
ad@asym.dk

- Testability is an emergent property of a system describing how well it can be tested.

- Test environment infrastructures usually mimic production environments.

- Dynamics in development and system complexity oftens result in severe testability problems when we approach the higher levels of abstraction.

Test environments mirror production

Service infrastructure

System A   System B   System C

But systems are independently maintained
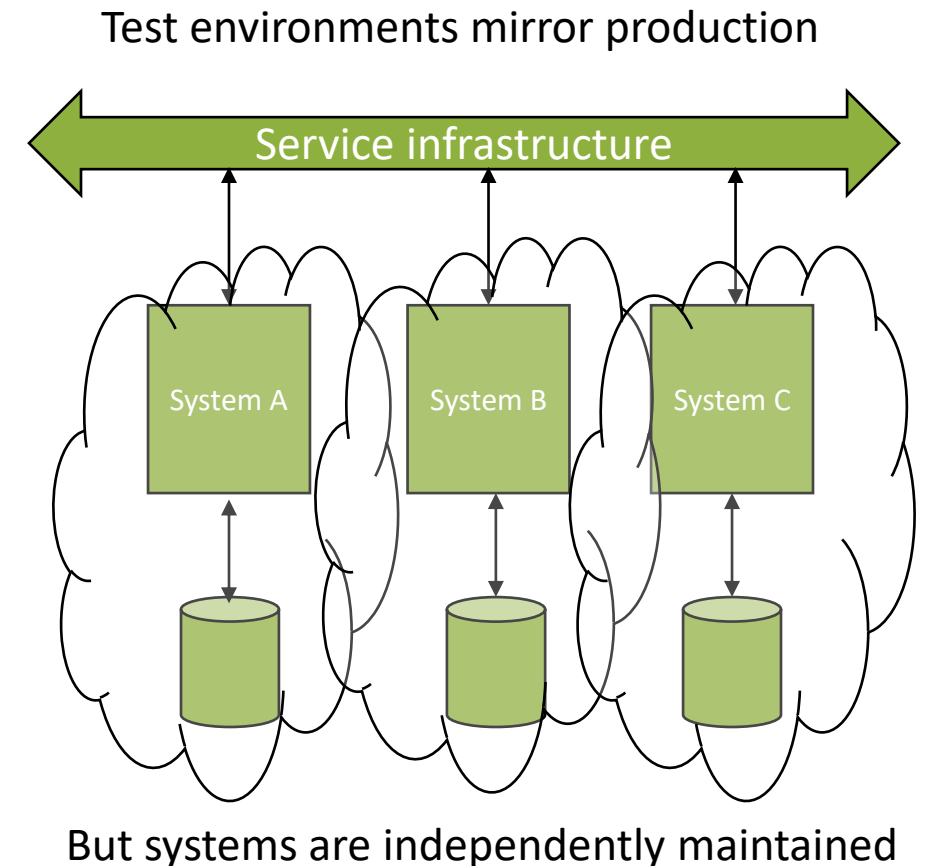
'Engineering' a control structure

A "lateral" approach to control structure workshop facilitation

@andersdinsen
ad@asym.dk

Random entry idea

Moving and challenging the idea: "Could it be otherwise?"

"Why?" questioning to identify logical boundaries: "Why is it like this?"

Ed de Bono, e.g. Lateral Thinking for Management

Lessons Learnt Applying STPA to Software Testing

@andersdinsen
ad@asym.dk

- With increased complexity of systems and and emergent properties testing needs to work on more abstract levels than before.

- STPA can help dealing with the complexity. Testability of complex systems can be improved with STPA

- Control structures can be difficult to analyze. A lateral approach to facilitation has been found to work well.

- The dynamics of agile, iterative, and continous delivery add complexity - but are here to stay.

- STPAs top-down approach can be made robust to change and iterative development.