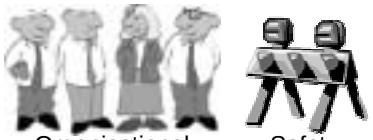
Archetypes for Organisational Safety

Karen Marais
Nancy G. Leveson

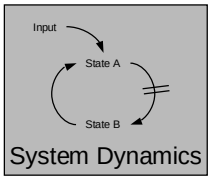
IRIA 2003
16 September 2003
See http://shemesh.larc.nasa.gov/iria2003/

Outline



Organisational Behaviour

Safety Engineering



Safety Archetypes

- Motivation
- System Dynamics
- The Archetypes

Safety Archetypes—Motivation

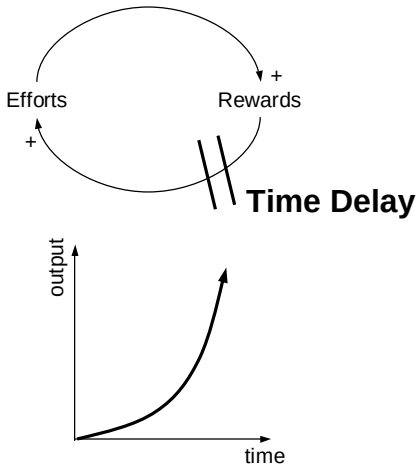
- How can we represent dynamic change in systems?
- Use **system dynamics**; but
- Difficult to build system dynamics models
  - Does not come naturally to non-experts
  - Usually achieved in ad hoc and time-consuming manner
- Many systems exhibit **common behaviour and flaws in the safety culture** that lead to accidents—archetypes
- Use archetypes to **accelerate and focus** modeling

System Dynamics

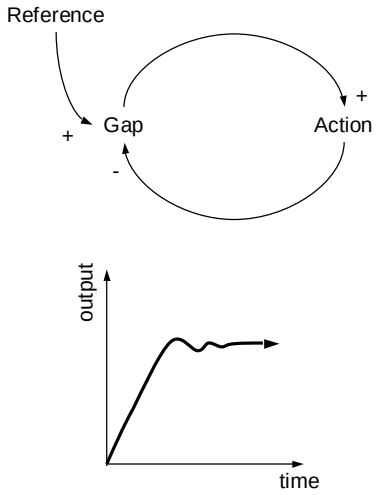
- Framework for dealing with "**dynamic complexity**"
  - Cause and effect not obviously related
- Counterintuitive or unexpected behaviour often arises when we have the **incorrect mental model**
- Use system dynamics to correct mental models
- Looking at dynamics of systems can improve
  - Understanding of accidents
  - Investigation recommendations
- Most dynamics are generated by a small set of basic patterns of behaviour—**archetypes**

Building Blocks

Reinforcing Loop



Balancing Loop

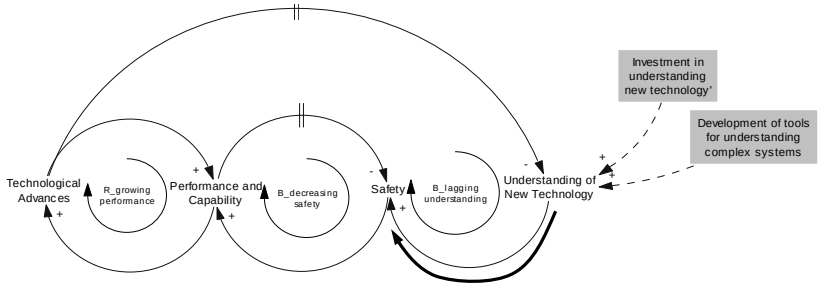


The Safety Archetypes

- Stagnant Safety Practices in the Face of Technological Advances
- Decreasing Safety Consciousness
- Unintended Side Effects of Safety Fixes
- Eroding Safety

Stagnant Safety Practices

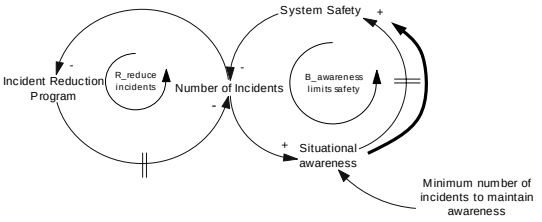
Rapid technological advancement can have a detrimental effect on safety



- Understanding of new technology constrains safety
- We can ameliorate the problem by:
  - Investing more resources in understanding new technologies; and
  - Developing tools for understanding complex systems

Decreasing Safety Consciousness

Continued application of particular safety measures does not always increase safety

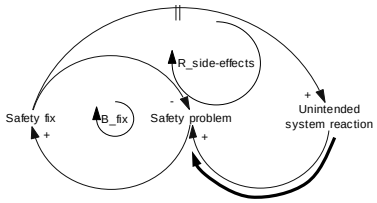


- Over-optimisation numbs adaptive capabilities of systems
- E.g. Working to reduce incidents to zero does not necessarily protect against disastrous accidents
  - Certain number of incidents required to maintain system awareness
  - Zero incidents creates impression that safety problem is solved
  - Attention is diverted to other goals

Unintended Side Effects of Safety Fixes

Unintended consequences of poorly designed problem fixes can worsen the problem

- Well-intentioned, commonplace solutions to safety problems
  - Often fail to help;
  - Have unintended side effects; or
  - Exacerbate problems

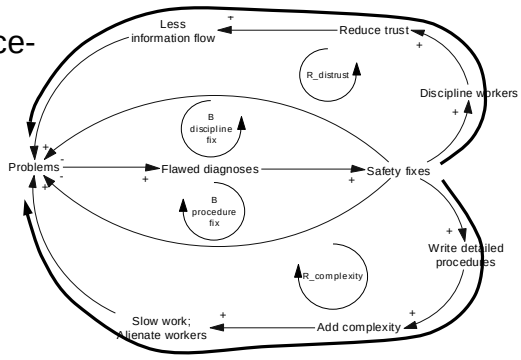


- Must correctly identify the fundamental problem and design appropriate solution strategies, but
  - Identifying the fundamental problem is often difficult; and
  - Designing and implementing solution strategies can be challenging
- Awareness of long-term negative implications that fixes often have can provide the impetus to search for fundamental solutions instead

Unintended Effects: Failed Safety Programs

Disciplining workers and writing more detailed procedures may not increase safety

- Typical fix for maintenance-related problems
- Detailed procedures and closer supervision seen as mistrust and regimentation
- Discourages problem solving



- Blaming individuals encourages all workers to hide problems
- When incidents are concealed, underlying problems stay hidden, often worsen, and may lead to more problems

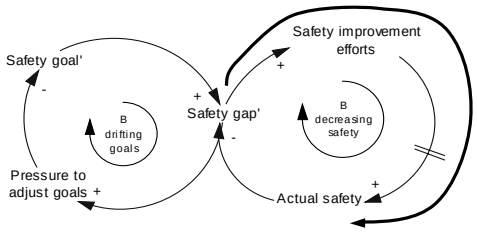
Accident Investigations

Accident investigation recommendations do not always improve safety

- Focus on preventing recurrence of similar accidents, ensuring procedural compliance, and assigning blame
- Attempts to identify the deeper factors or conditions that allowed safety to deteriorate often insufficient
- Symptomatic solutions decrease the pressure to find fundamental solutions
- For long term safety improvement the fundamental problem or structural deficiency must be identified

Eroding Safety

Safety goals may drift, or erode, over time

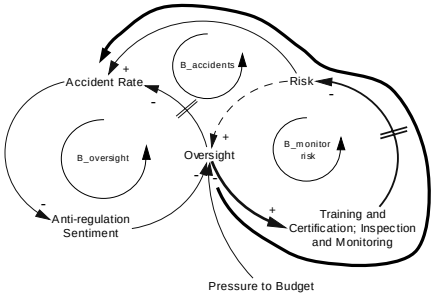


- Temptation to shift goals instead of determining why goals were not met in the first place
- When successive adjustments result in net lowering of goals, safety deteriorates
- Without objective metrics of system safety, difficult to challenge temptation to progressively lower goals
- Often difficult to observe because change is gradual

Eroding Safety: Complacency

History of safe operations encourages growing complacency

- Complacency arises because accident rate usually does not immediately increase following a decrease in oversight
- Problem with complacency is twofold:
  - Difficult not to become complacent when success follows upon success
  - Difficult for an organisation to realise that it is becoming complacent, and often a serious accident is required to shake the complacency

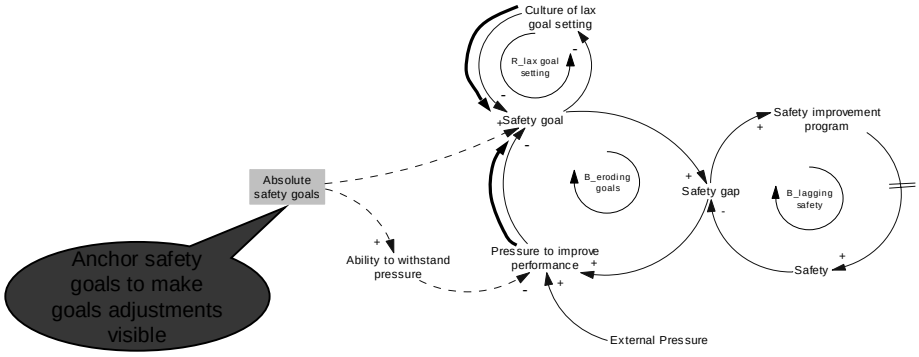


- Must continuously monitor risk and set the level of oversight accordingly
- Must consider long-term trend in risk level

Eroding Safety: Disappointing Safety Programs

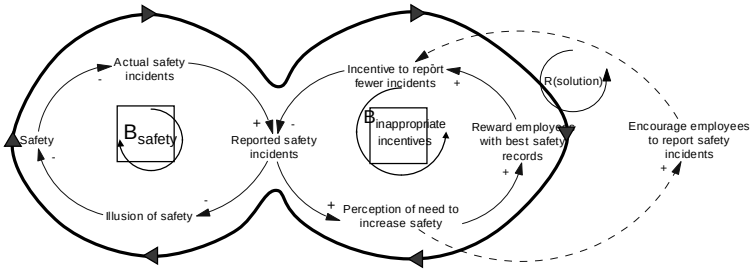
Why do safety programs often disappoint?

- Safety programs can be expensive and show no immediate results
- Immediate cost of safety program subject to external pressures
  - Combination of seeming ineffectiveness and external pressures makes it tempting to adjust the goals of the safety program
  - Adjustment is not necessarily seen as a failure, even seen as improvement



Eroding Safety: Incident Reporting Schemes

Incident reporting schemes may perversely decrease safety



- Incident reporting meant to encourage greater vigilance
- Workers with the fewest (reported) incidents are rewarded
  - Incentive to withhold information about small accidents & near misses
- Illusion that system is becoming safer
- Management becomes less aware of the behaviour of the system, and safety may therefore decrease

Summary

- Archetypes explain why safety-related decisions
  - Do not always result in the desired behaviour; and
  - How decisions elsewhere in an organisation affect safety
- Analysis tools:
  - Used in accident investigations to develop dynamic models that describe system migration towards accident
- Synthesis tools:
  - Highlight potential mechanisms by which system can drift towards unsafe behaviour
  - Post-investigation recommendations; and
  - Risk assessments