Tensions between Safety Cases and STAMP

Where do they disagree and who is right?

Safety Science Innovation Lab

Daniel Grivicic

- Novel, patent pending, level crossing solutions using common off the shelf components.

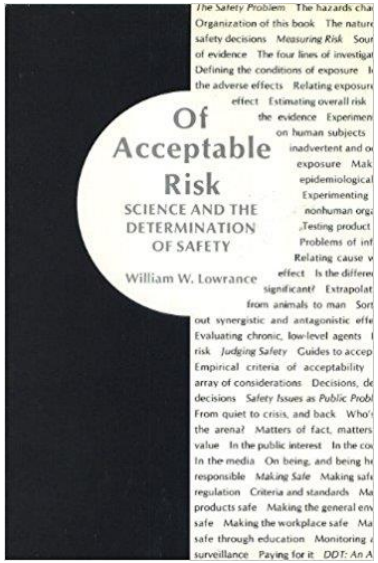
Dr. Drew Rae

- Sincere thanks to my supervisor Dr. Drew Rae from the Safety Science Innovation Lab who provided support.

Safety Engineering

Reducing Harm

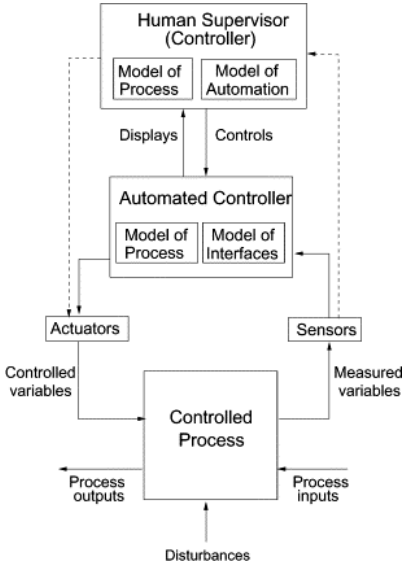
Ensuring Risk is Acceptable



Ways of achieving this?

Safety Case

STAMP



Safety Case

Good

- Structured approach supports safety claims
- Performance based = Flexibility
- Through evidence safety is achieved

Bad

- Retrospectively
- Cognitive bias
- Well publicised catastrophic failures

STAMP

Good

- Safety in design
- Continual improvement
- Feedback & Control

Bad

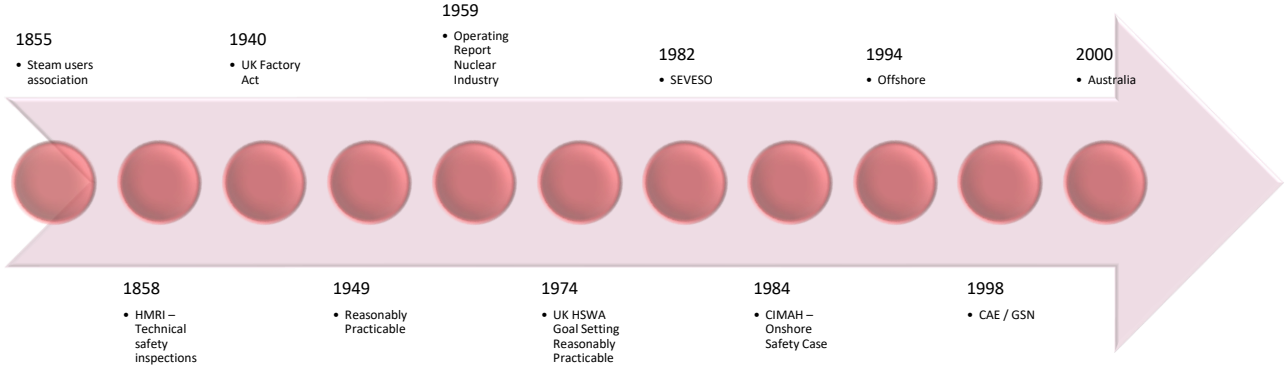
- Brand new
- Limited validation
- Limited guidance

Safety Case

- It's a story
- Clear comprehensible & defensible argument
- Safe operate within context
- In some cases legal requirement
- But – No single safety case format

Source: www.nuclearinst.com

Safety Case Evolution



Safety Cases - Benefits

- Companies
  - Understand safety risk exposure
- Public
  - Provide insight into organisations
- Regulators
  - Use safety case to assist organisations understand and meet safety requirements

Safety Case - Criticisms

Safety Case - Criticisms

…some industries that have adopted a Safety Case and goal-based approaches have experienced much higher accident rates, such as offshore oil exploration and production

Leveson

Safety Case – Cognitive Bias

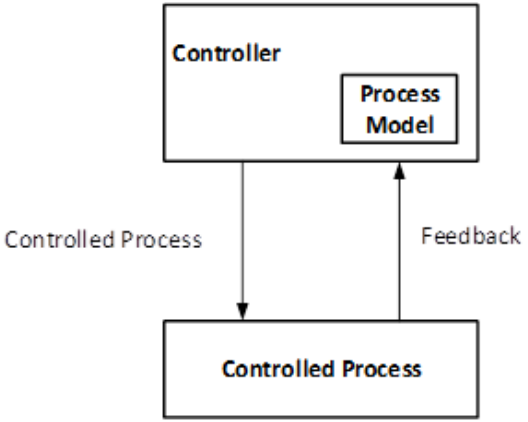
- Safety Case
  - “Safe already”
- EN 50126
  - Structured Safety Case based on the issued standard

Safety Case – Lack of argument

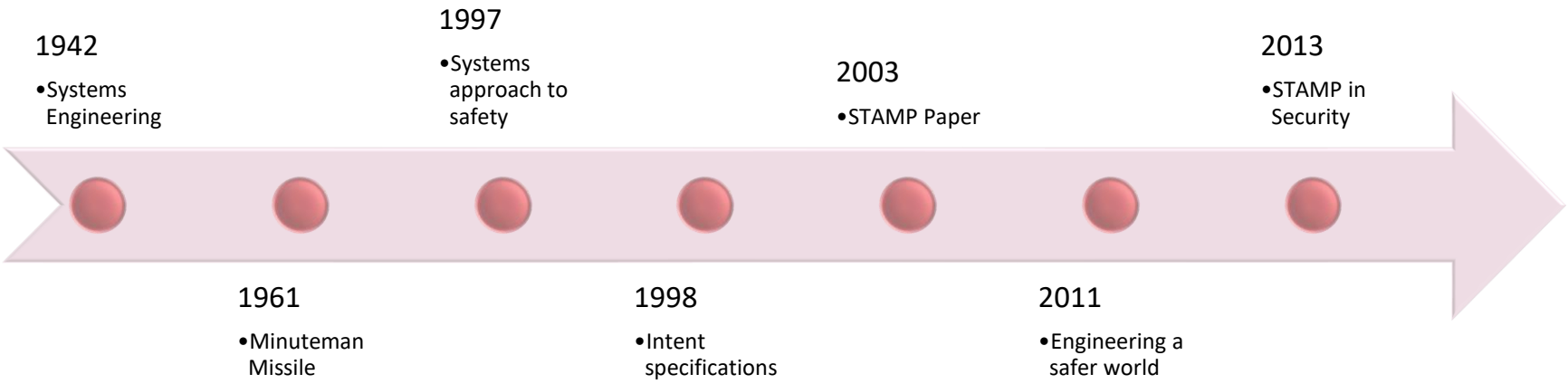
Gerund

STAMP

- Systems-Theoretic Accident Model and Processes
- Feedback and Control
  - Constraints
  - Hierarchical Control
  - Accurate process model
- Used in design not retrospective



STAMP Evolution



STAMP - Benefits

- Companies
  - Helps companies appreciate that single events are not the cause of accidents
- Public
  - STAMP method includes the public
- Regulators
  - Provides regulators with a methodology to understand safety

STAMP - Criticisms

- STAMP is an idea without evidence
- Little guidance in its use
- Unreliable?
- Immature

Debates

Safety Case

- Long history – mature idea
- Process driven welcoming of new ideas
- Spectacular failures

STAMP

- Launched with fanfare
- Directly attacked STAMP
- Still unknown – less unknown than fault tress which is also attacks
- Difficult to implement?

Safety Case Failures?

http://tomtunguz.com/clandestine-statisticians/

Debates

Safety Case

- Legislated
- Quantitative
- Qualitative

STAMP

- Does not create safety
- Qualitative (exclusively)

Debates – Partial Truce?

Safety Case

- Create Safety
- Uses a narrative
- Safety case What and Why

STAMP

- Create Safety
- Uses a narrative
- Intent specifications (What and Why requirements)

Future Considerations

- Improper application of Safety Cases have cased failure
- Safety Cases generally go right
- STAMP is a systems based *model*
- Safety Cases are *processes*
- Safety cases structured to meet legislative requirements
- Safety Cases develop late to ensure application
- STAMP is created early but has not argument

Future Considerations

- STAMP was created
- Safety Cases evolved
- STAMP was marketed by an engineer
- Safety Cases sell themselves

- “Does not imply what previously done is wrong and new approach correct”

Conclusion

- No evidence that Safety Cases are not meeting intended requirements
- Investigate papers that use STAMP
- Extract the safety argument from these papers
- See if these papers present a strong argument or are there areas that are lacking
- Is STAMP an improvement on Safety Cases?