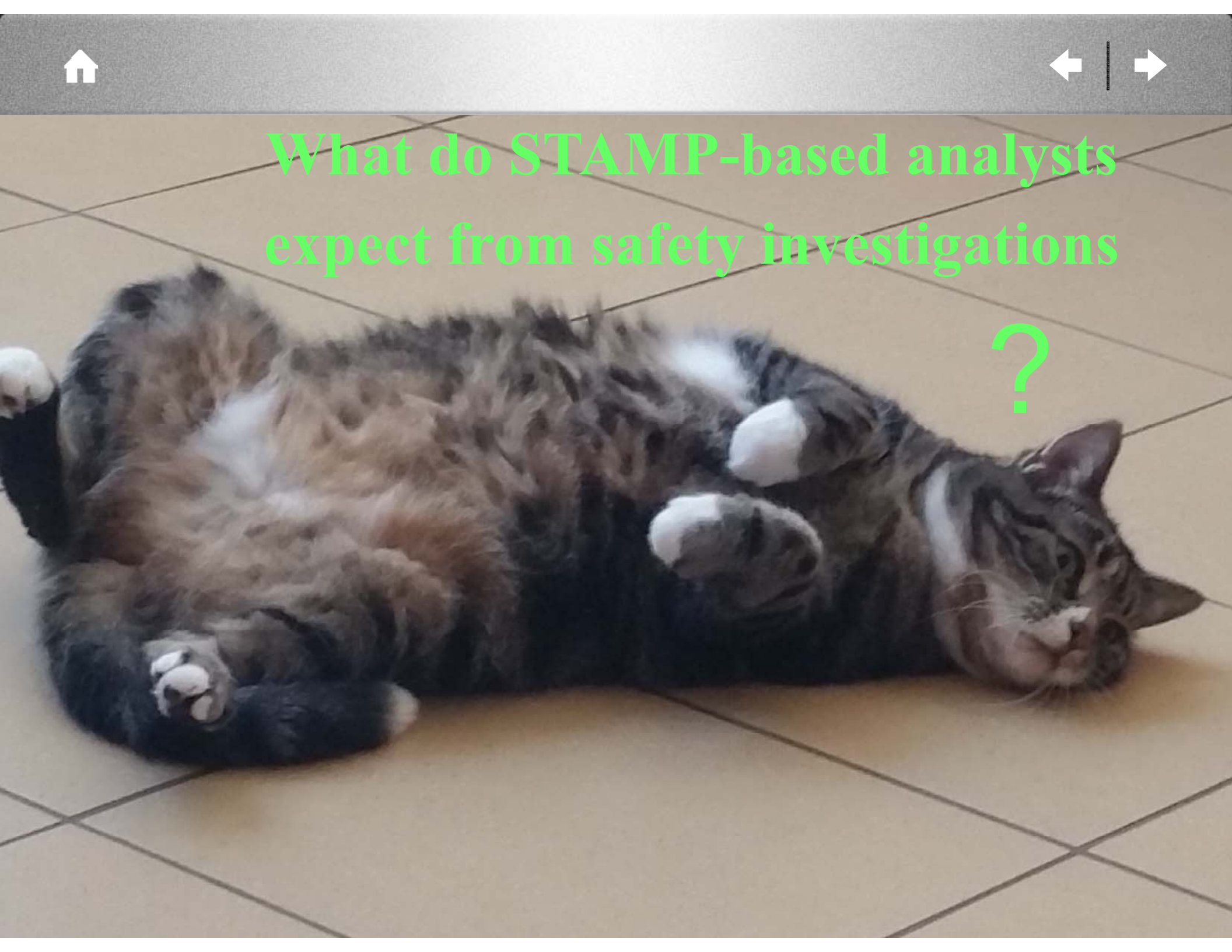

What do STAMP-based analysts expect from safety investigations
?


John Stoop
Ludwig Benner Jr
OLD

STAMP...

- is a new accident causation model
- an analysis but not investigation model
- provides CAST process to analyze accidents
- CAST needs several kinds of input data


CAST…

- Based on STAMP system control model
- Uses nine-step analysis process
- Steps not necessarily performed in sequence
- No formalized case selection criteria

CAST data needs...

- accident investigation data
- system safety controls/constraints structure
- safety control structure performance over time

CAST analyses need...

1. the proximate event chain
2. conditions that allowed events to occur
3. direct factors critical to understanding why accident occurred

Accident investigations...

- At least 28 investigation methods used
- Each produces different reported results
- Resultant data variability affects CAST
- CAST / STAMP do not specify a preferred investigation method

Differences in methods affect...

- investigation scope
- input data selected
- input data documentation
- input data integration
- integrated data use
- cause attribution
- data integration rigor
- terminology used
- form of reports
- quality assurance
- decision transparency


CAST data sources...

- Event data
  - accident reports
  - if not in accident reports, then
  - system description


CAST data sources...

- System data
  - system definition
  - system control network model
  - social control dynamics

CAST data sources...

- Analysts' proficiency
  - roles
  - resources
  - decision process and rules


Expanding data sources…

- Options:
  - Refer to safety audits
  - Refer to system safety analyses
  - Other reports of same accident
  - Build STAMP system control library
  - Pre-emptive modeling of events

Expanding data sources...

- Options:
  - develop case selection criteria
  - harmonize investigation methods
  - use “best fit” investigation method(s)
  - focus on systemic inherent properties

Three systemic control levels

The operator level: inherent properties

- Tayloristic model
- Rational utility, ETTO trade-offs

Require:

- A new view on human error
- Separating event from system

Three systemic control levels

The network level: principles, properties, performance

- concept: size, source variation, connectivity, integration, architectural control
- categories: disconnected, hybrid or spider
- technological control: R&D costs, knowledge hubs, coupling, platform leadership, hierarchical control
- social control: empowerment distribution and mechanisms, roles, control agents, aspects, coping capacities, resources, means, scope, impact level

Three systemic control levels

The systems business model: control agents

- Transport systems are inherently unstable: open architecture, interoperable, interconnective, 24/7 operational, free accessible, global configuration, heterarchically organized, delegated and distributed responsibilities, flexible, absorp crises and perturbations, continuously changing and adapting
- Institutional arrangements create illusion of stability: gradual changes, damping oscillations, drift into failure
- Innovations provoke oscillation: time, cost, efficiency

Inherent systemic failures

- Operational erosion: prospective expectations of performance and profit optimization
- Incremental erosion: speculative expectations, validity of apparent stability, unnoticed erosion, drift into operating margins, masking inherent unstable properties
- Conceptual erosion: wilfull interventions and changing properties, eliminating barriers, structural reduction of damping arrangements, investments and knowledge, feedback loops, power relations

Conclusions

- Investigation data is necessary but insufficient for CAST analyses
- Investigation report contents differ widely
- All reported accident descriptions differ from dynamic safety control analyses
- Analysts should recognize distinction between episodic investigations and dynamic system performance analyses for data sourcing decisions


Questions, any questions?

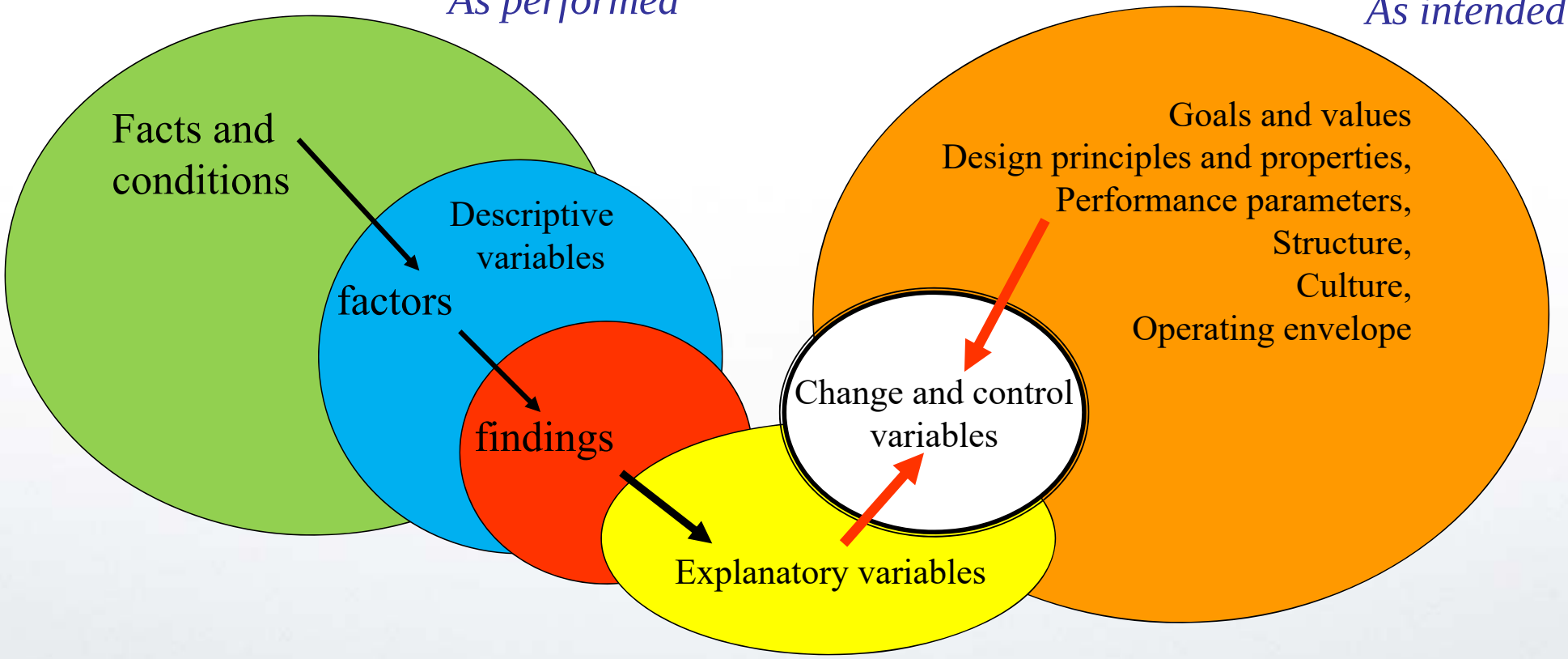
Transition from explanatory to control/change variables

Accident investigation process:

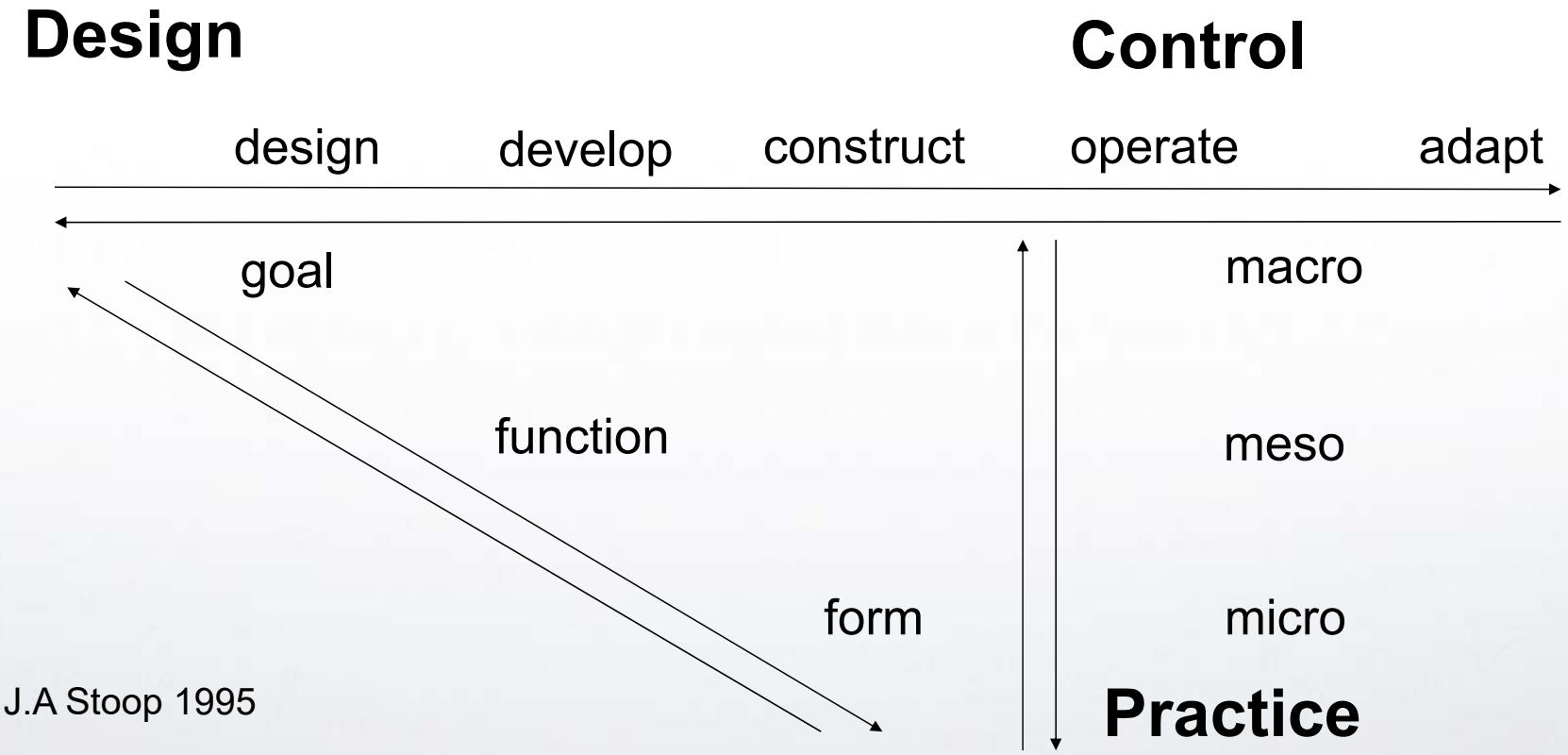
As performed

Systems design and operations:

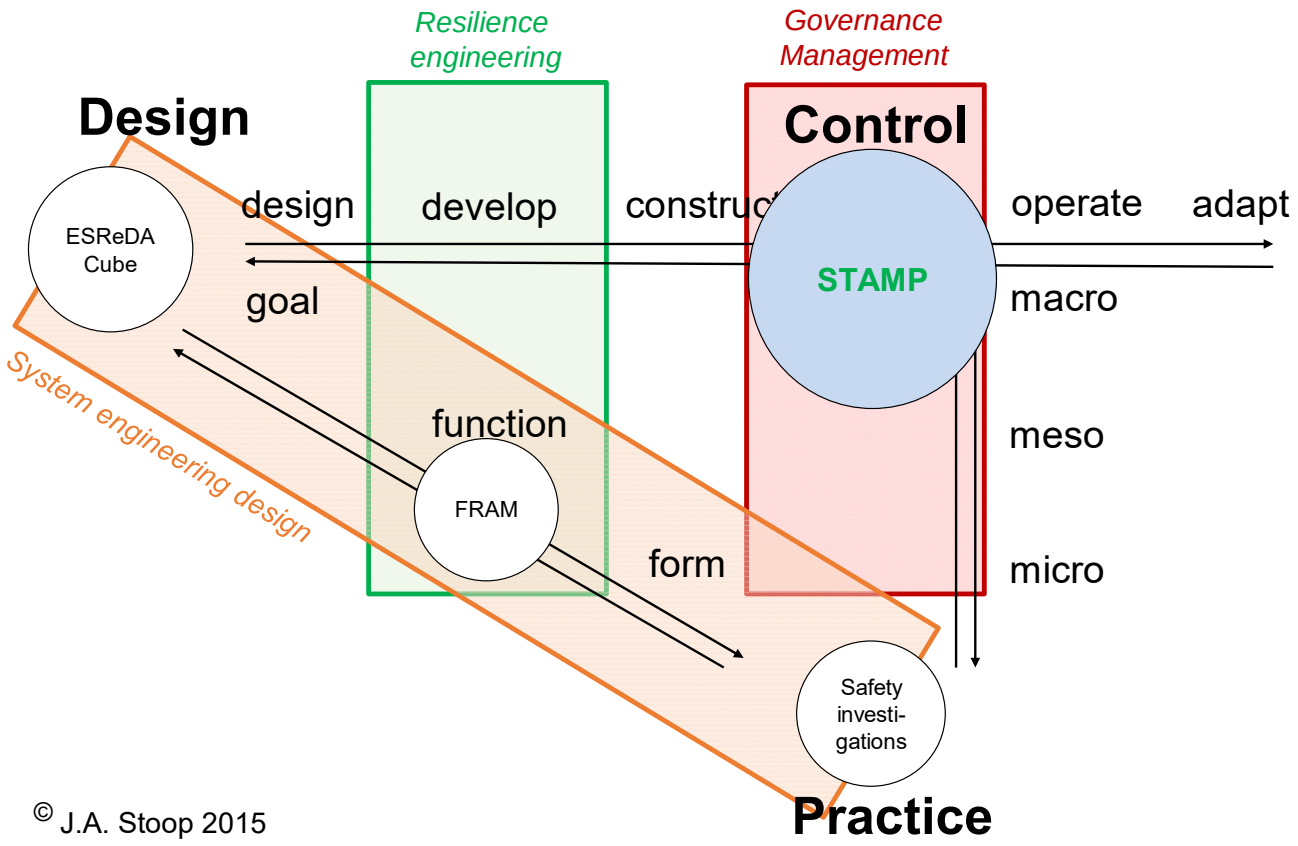
As intended



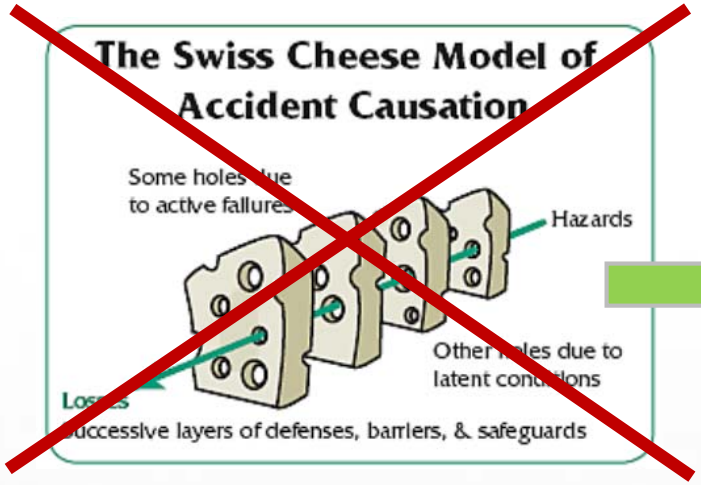
The DCP diagram
a multi-perspective landscape

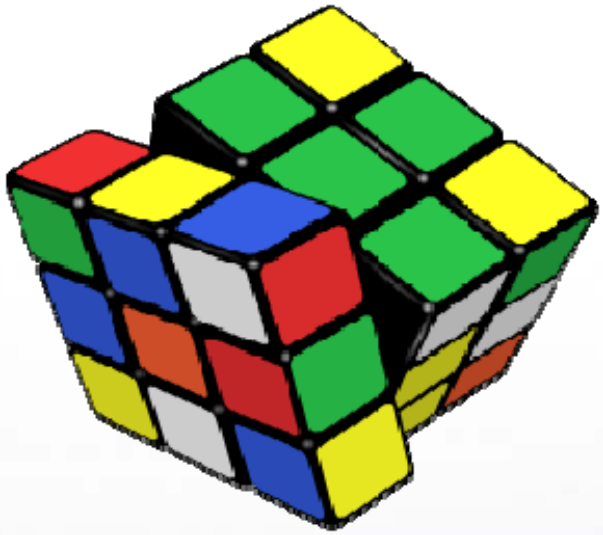


The DCP diagram: positioning safety methods



New communication metaphors





Metaphors?

- Reason Swiss Cheese metaphor
- Heinrich Iceberg principle
- Dekkers' Bad Apples
- Domino stones
- Simplistic methods: Tripod

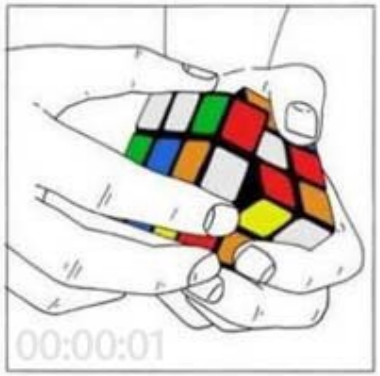
Linear models?

Taylorism: just time and money

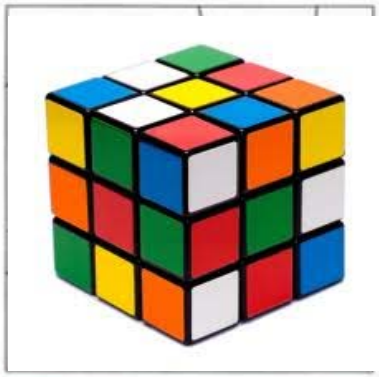
Accident investigation: blame, single cause

How to reduce complex problems

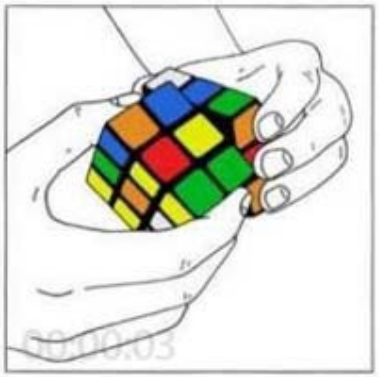
Collect facts

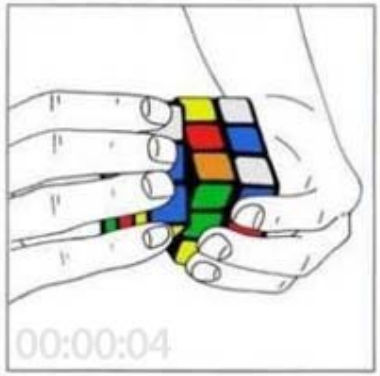


Compose event



Identify system variables





Synchronize variables

Using algorithms

To create transparency

The Safety Intervention Cube
Design, Control and Practice

Introduce information feedback across levels aspects and dimensions