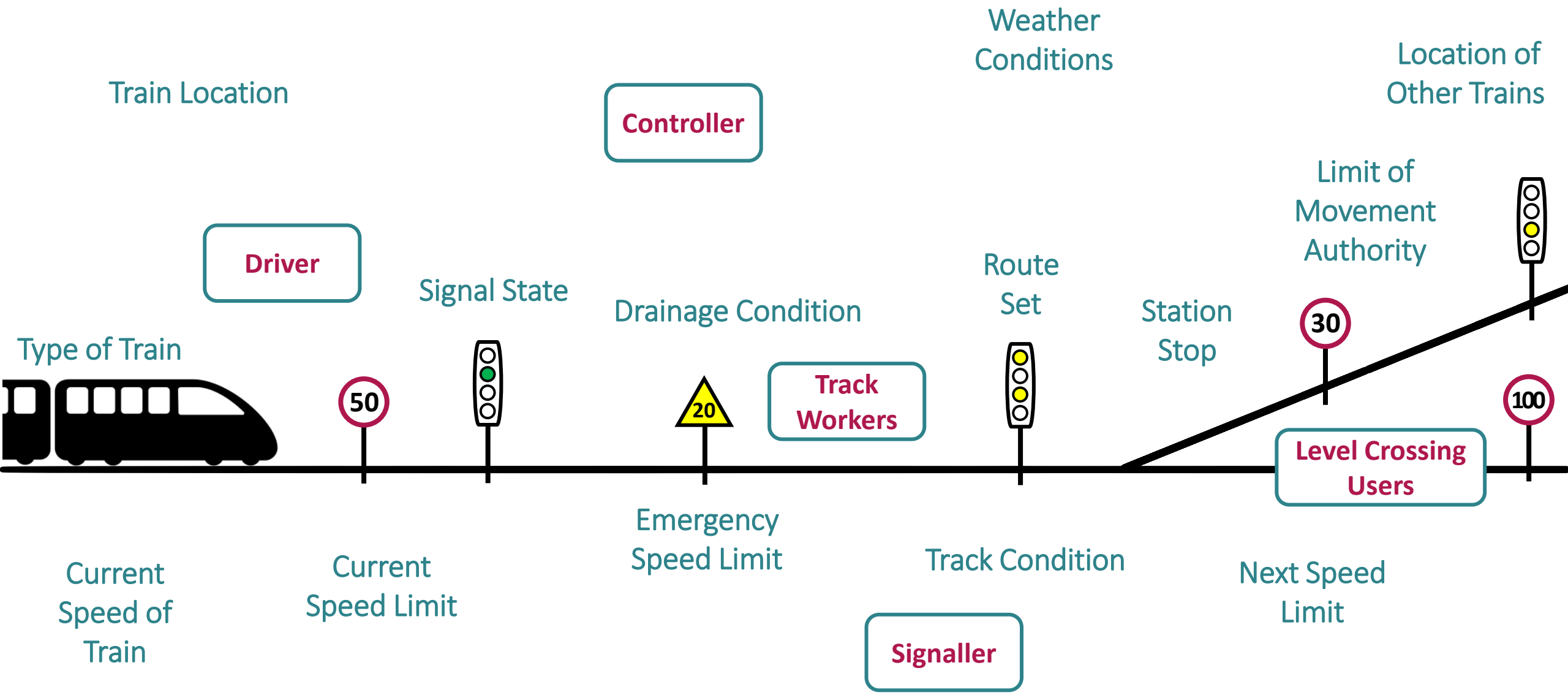
Human Factors in the Control Loop: A Case Study of the Use of STPA for a Rail Innovation Project

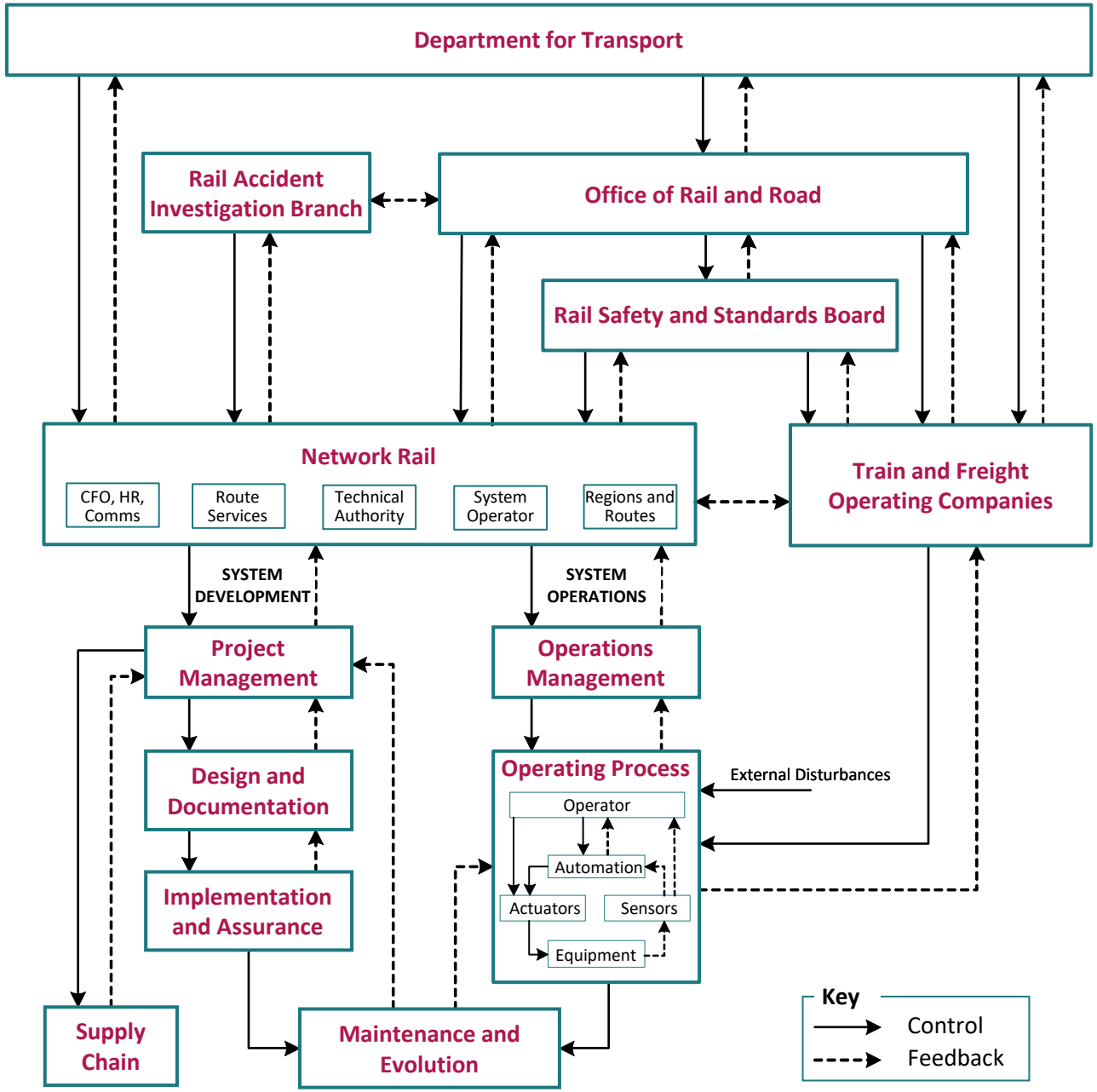
Richard Bye, Network Rail and Meaghan O'Neil, System Design and Strategy Ltd


SIEMENS
GROVE PARK

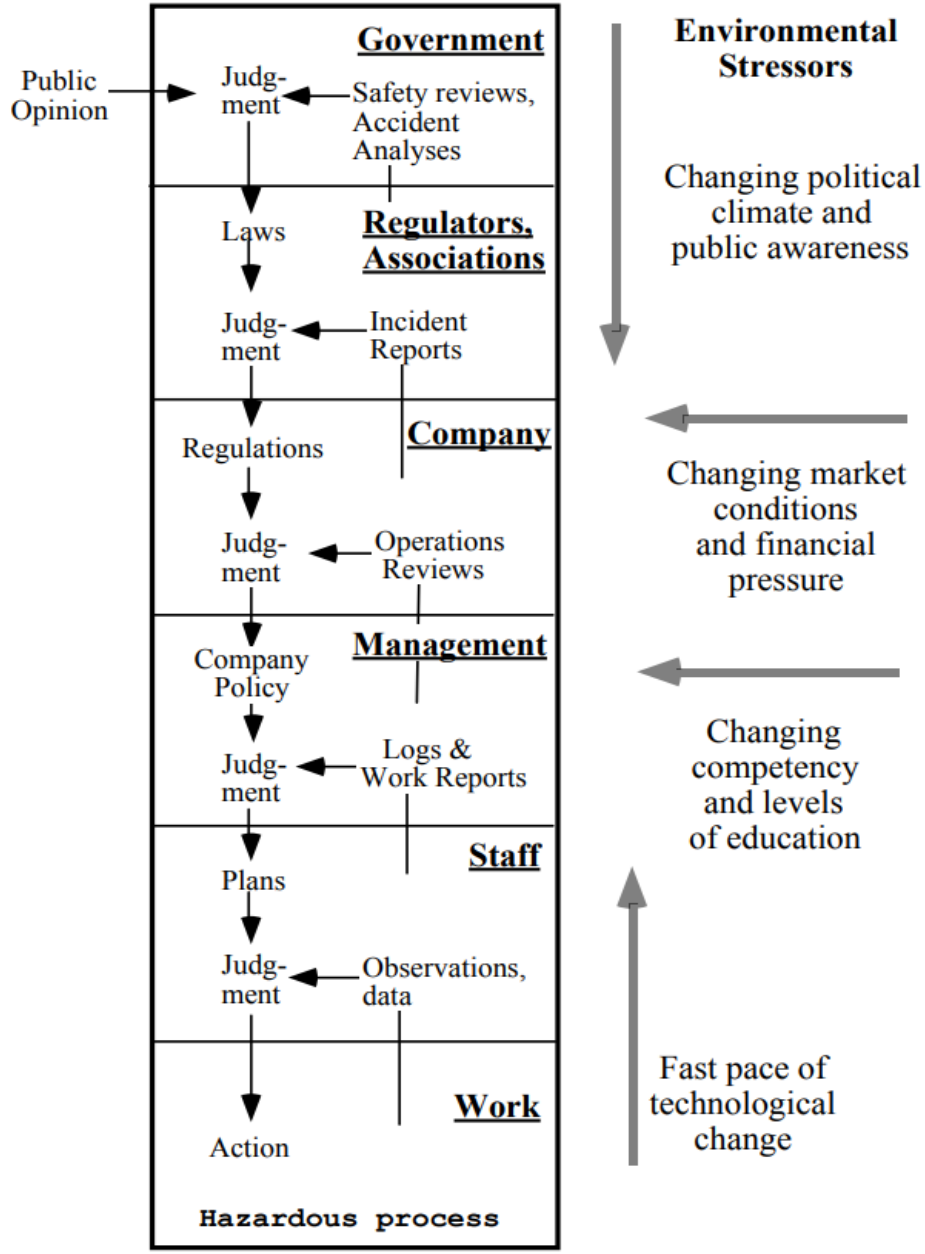
The Railway as a Distributed Cognitive System



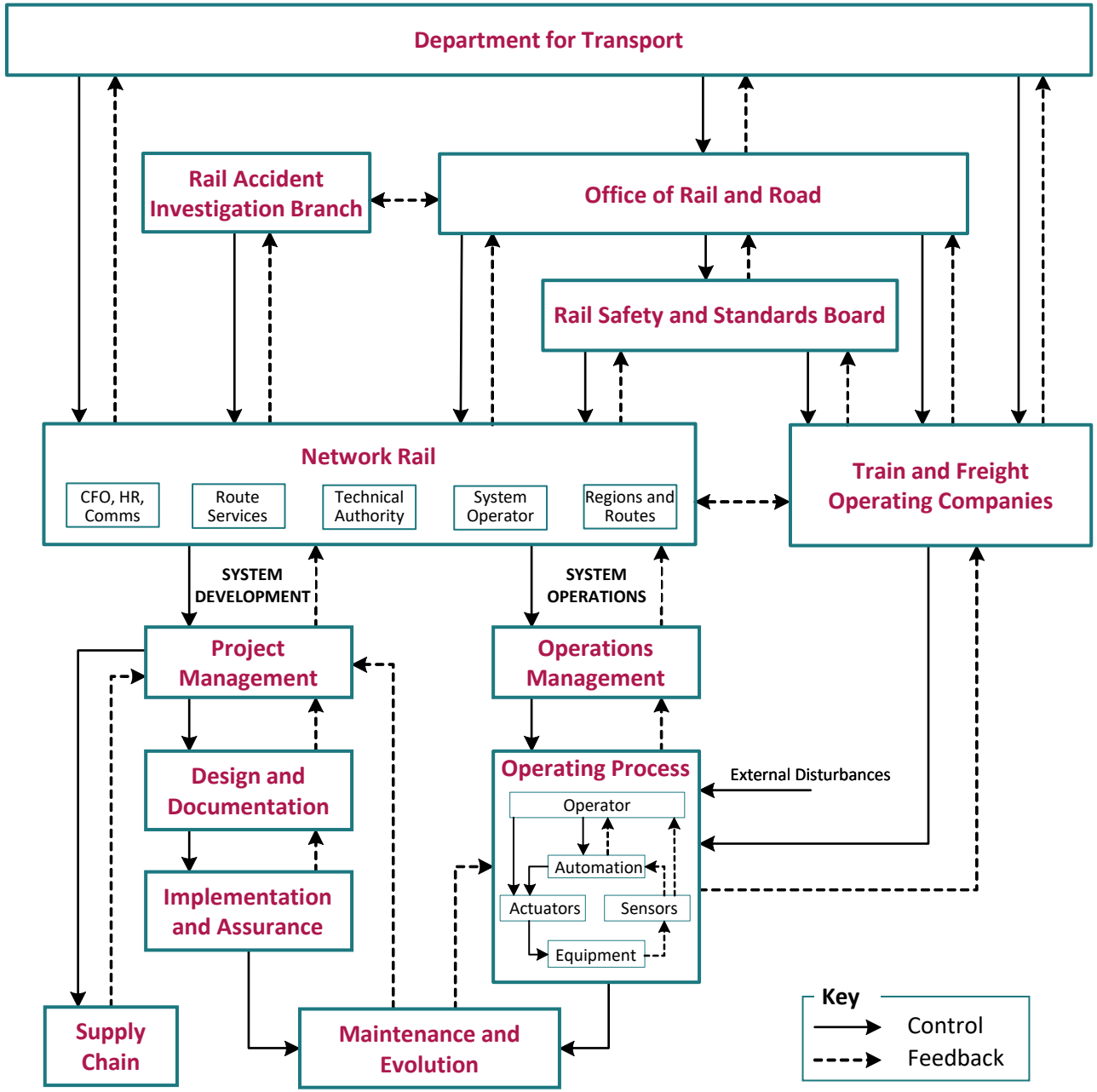
RAIB – Rail Accident Report: Derailment of a passenger train at Carmont, Aberdeenshire, 12 August 2020. Report 02/2022. © Crown copyright 2022.



GB Rail Industry Control Structure



Rasmussen, J. (1997). *Risk management in a dynamic society: a modelling problem*. Safety science, *27*(2-3).



GB Rail Industry Control Structure

L-1

Financial loss

L-2

Loss of life or injury

L-3

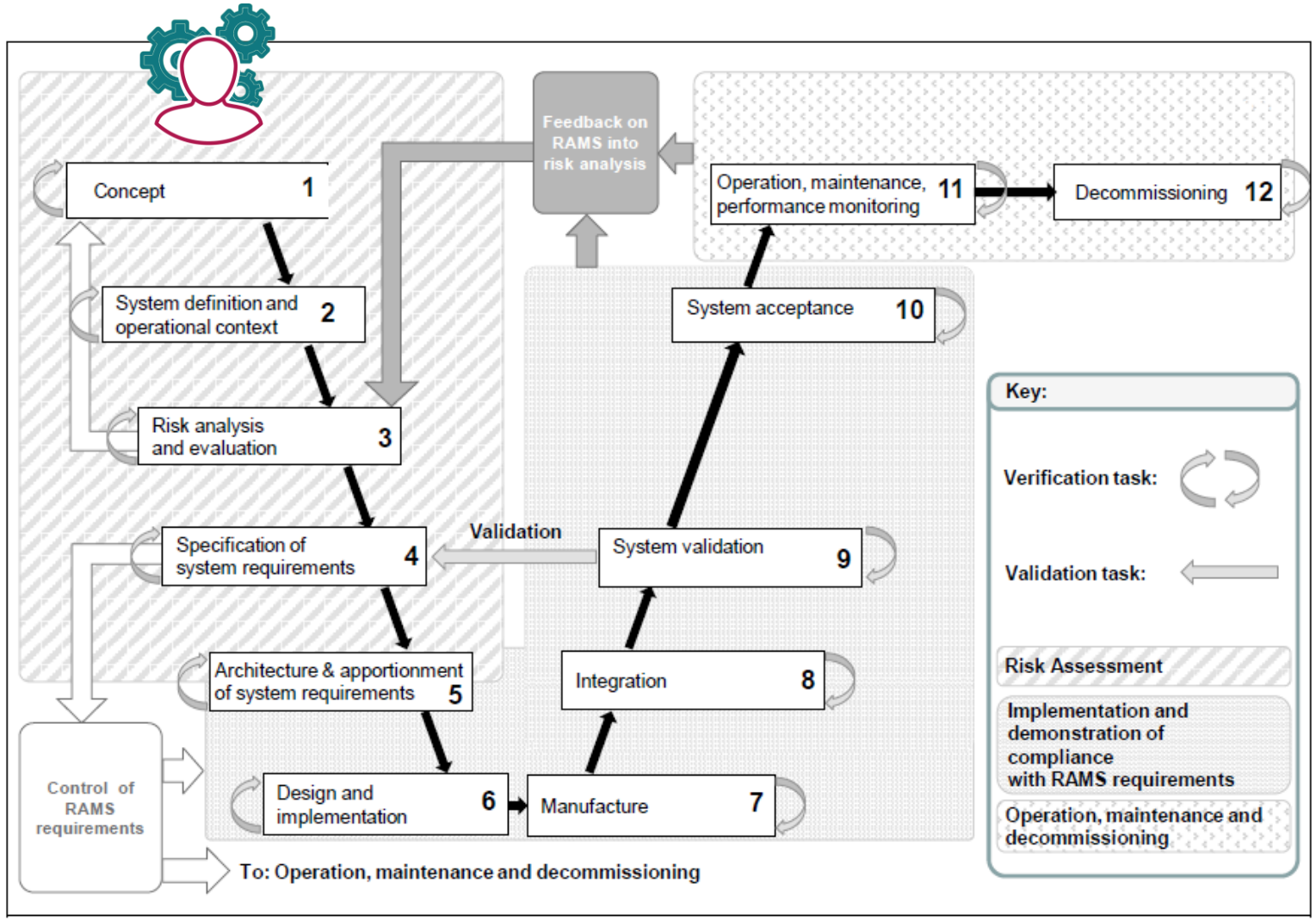
Loss of trust or reputation

L-4

Loss or damage to property or the environment

L-5

Failure to deliver the rail service



Put safety first

Use human-centred design methods

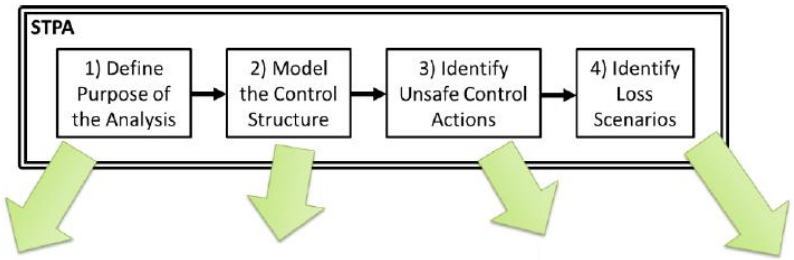
Evoke trust

Reduce risk through digital engineering

Focus on the operational context

BS EN 60126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

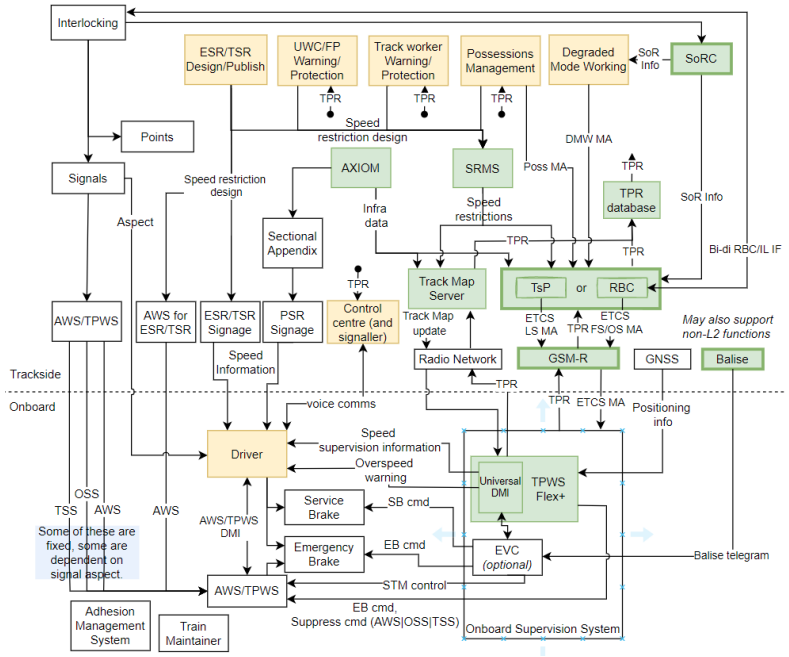
Basic STPA Method



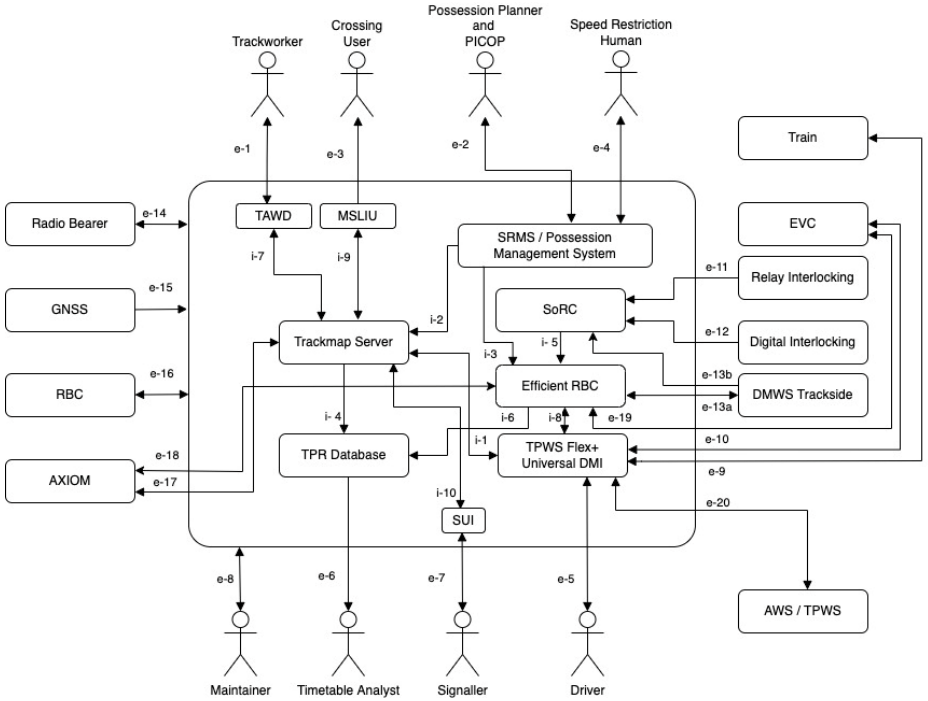
STPA

Safety Guided Design

Design Decisions



Concept Architecture



System Contexts and Interfaces

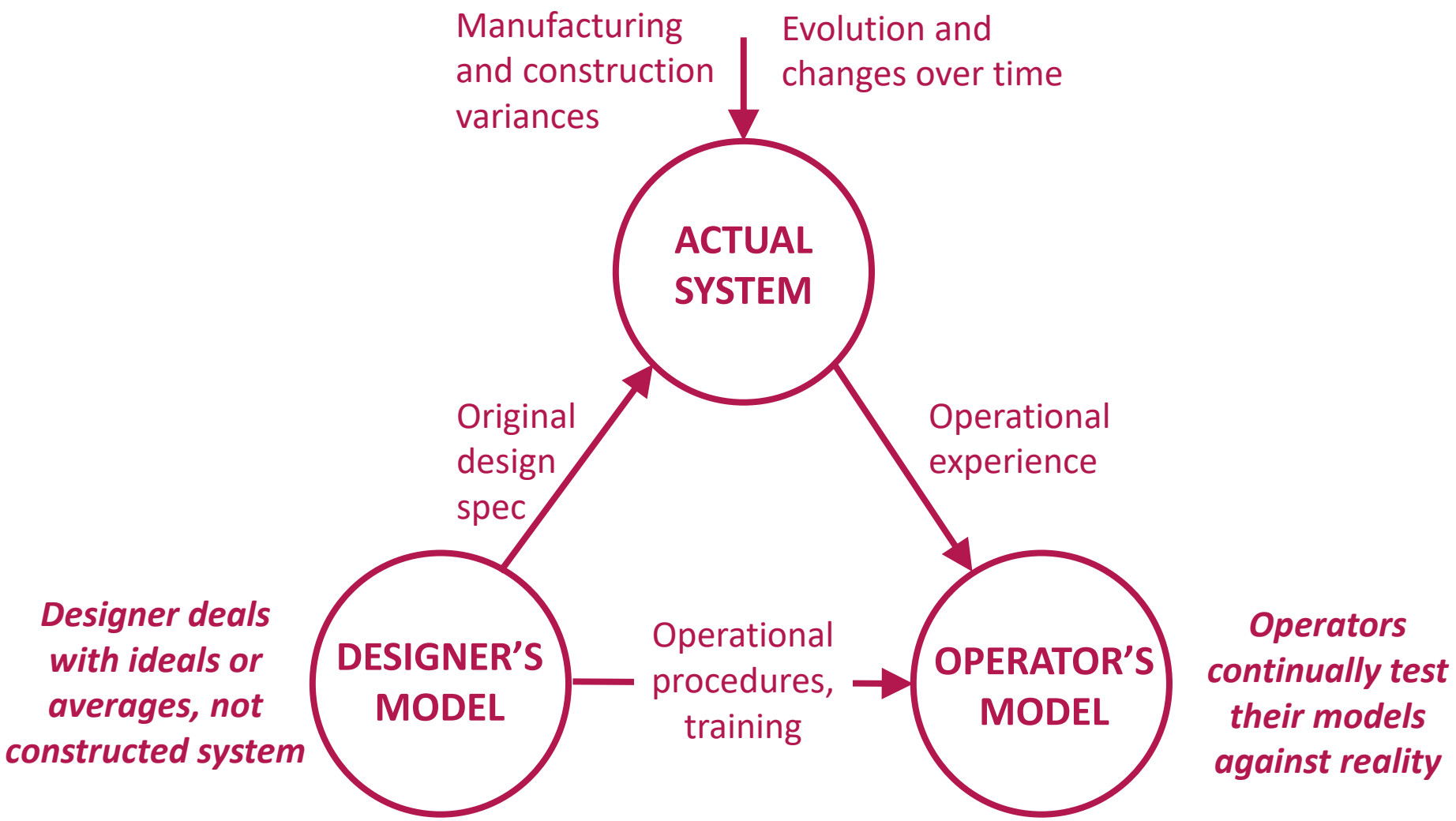
Signal Engineers

Operations Experts

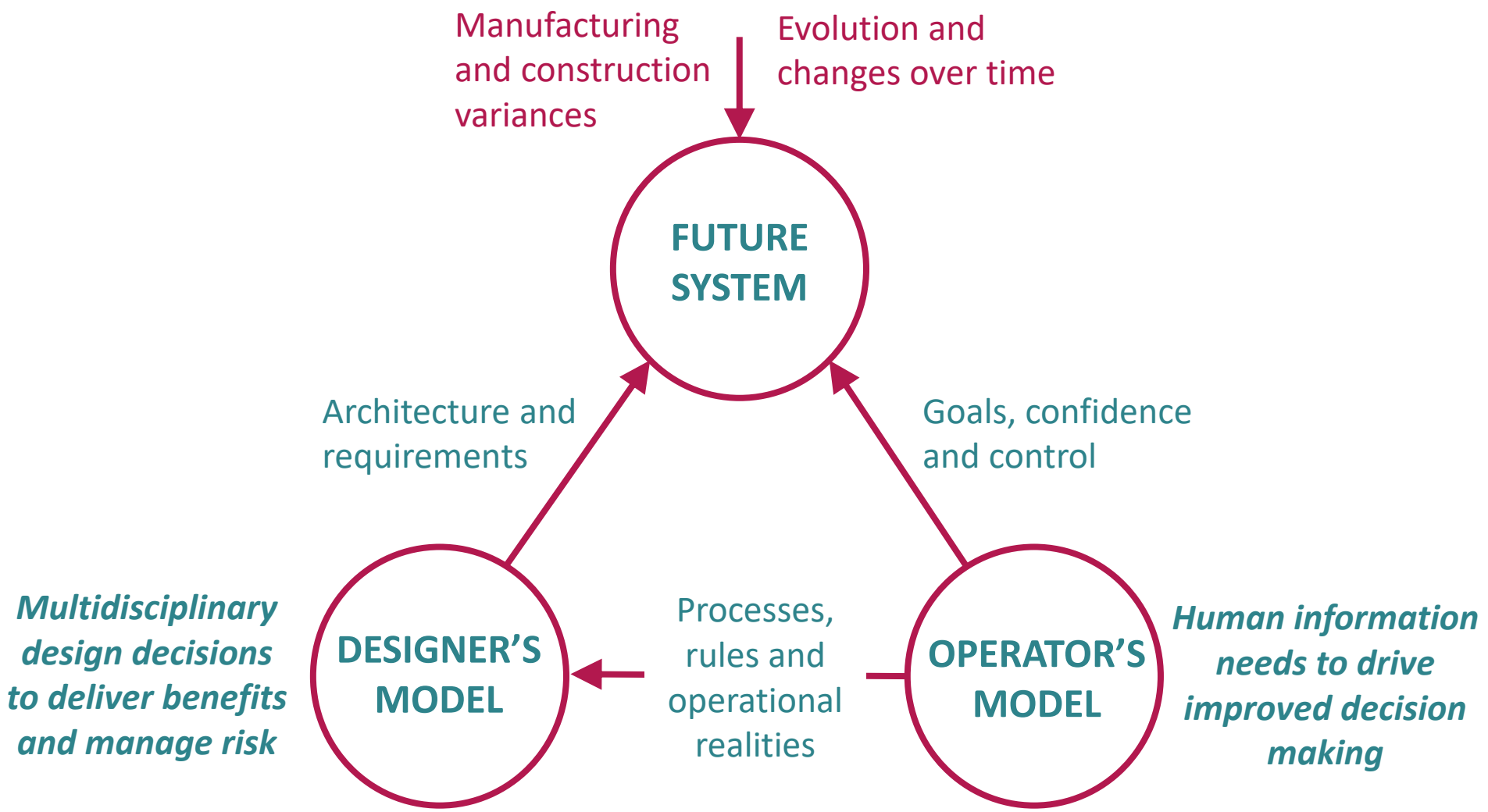
STPA

Human Factors Specialists

Safety Engineers

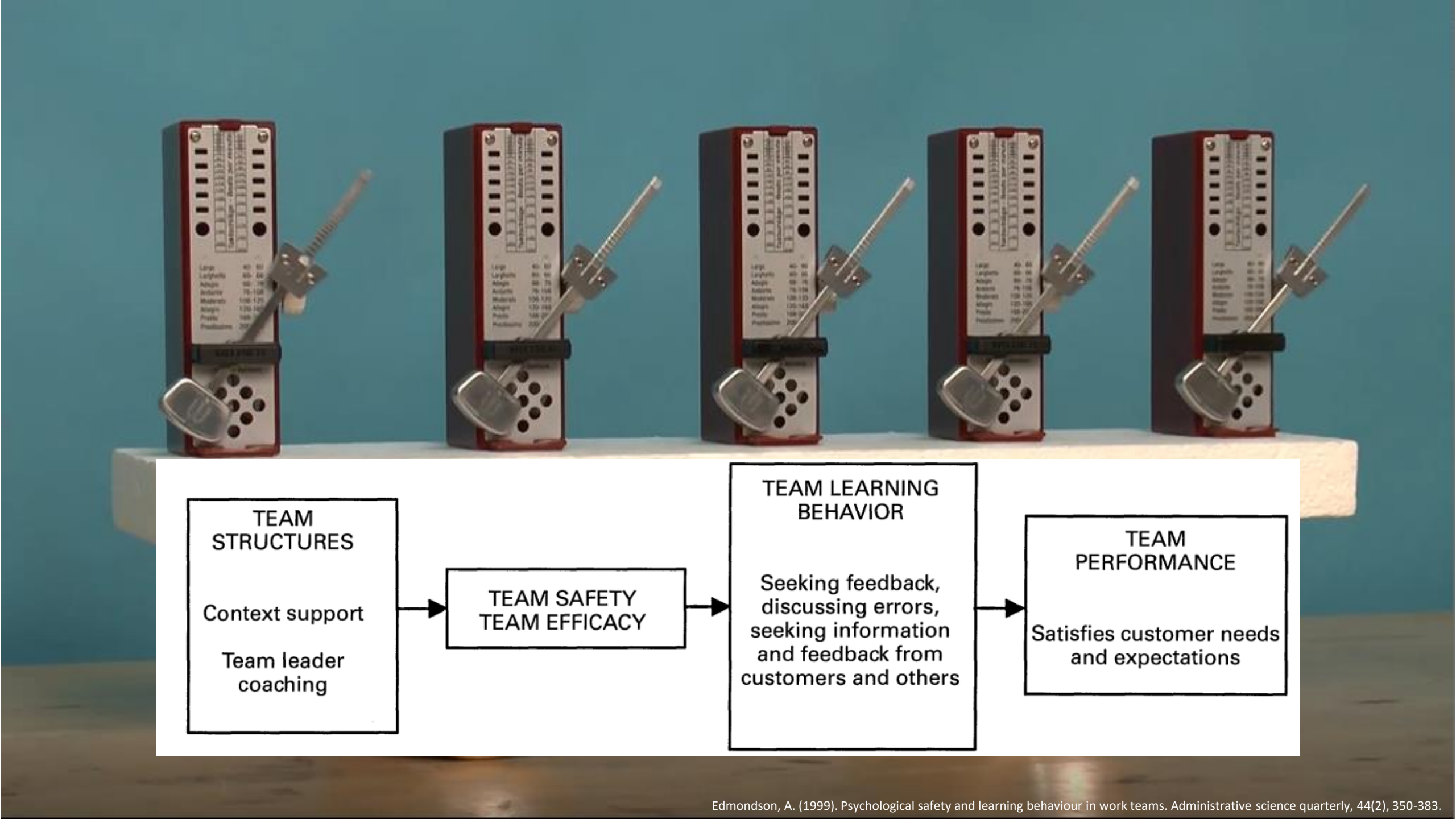


Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.



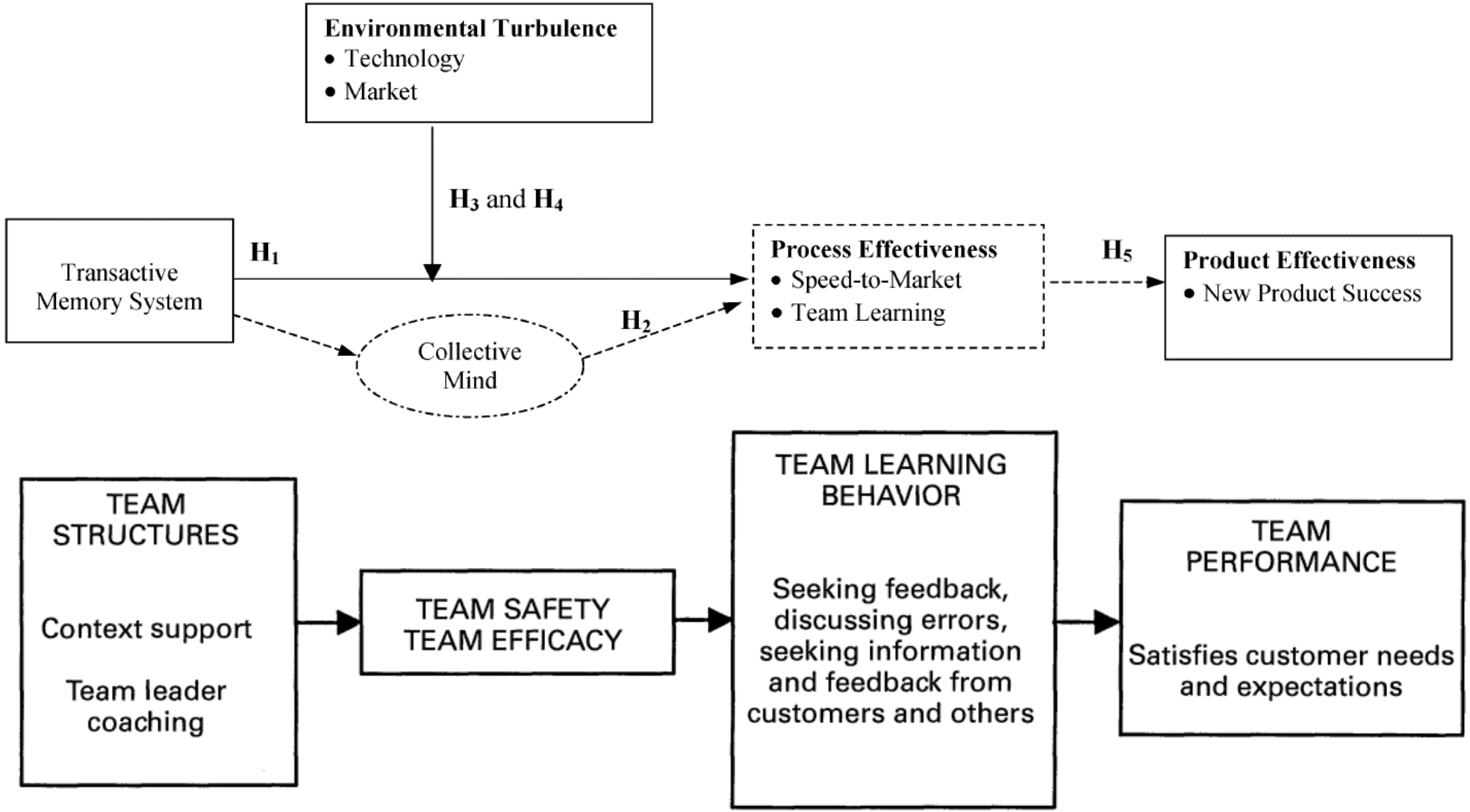
Adapted from Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.

https://www.youtube.com/watch?v=T58lGKREubo



Edmondson, A. (1999). Psychological safety and learning behaviour in work teams. Administrative science quarterly, 44(2), 350-383.

Transactive Memory Systems in Product Development Teams



Akgün, et.al. (2006). Transactive memory system in new product development teams. *IEEE Transactions on Engineering Management, 53*, 95-111.

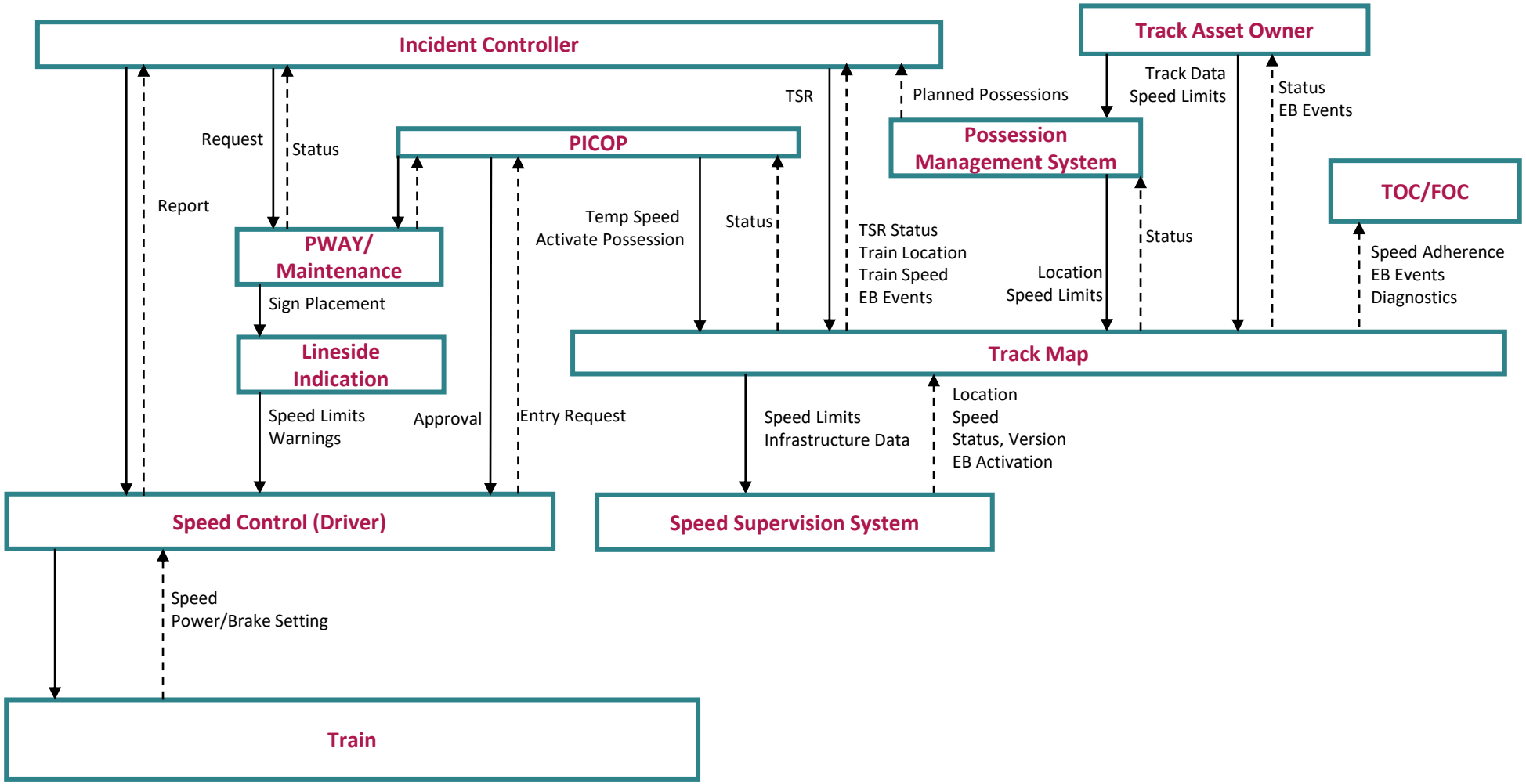
Edmondson, A. (1999). Psychological safety and learning behaviour in work teams. Administrative science quarterly, 44(2), 350-383.

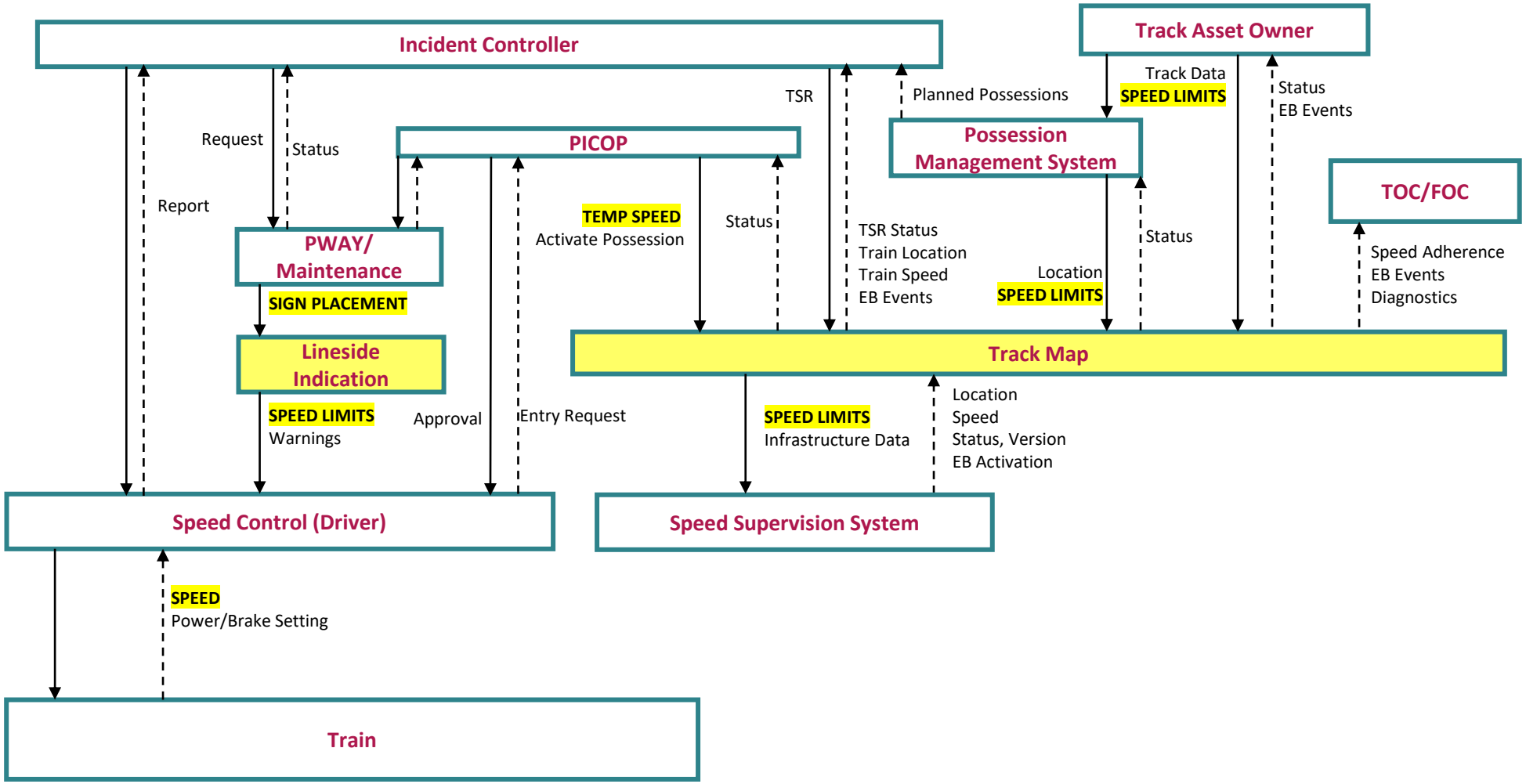
How did using STPA help?

- STPA control structures are useful ***cognitive artifacts*** that offer ***decision making stability*** in the face of ***strategic uncertainty***.

- ***Blending STPA with human factors methods*** can surface ***system vulnerabilities*** and unlock opportunities for ***creative decision making and innovation***.

- STPA provides ***structure and processes*** to consider ***humans and machines as collaborative agents*** during the ***design of complex systems***.

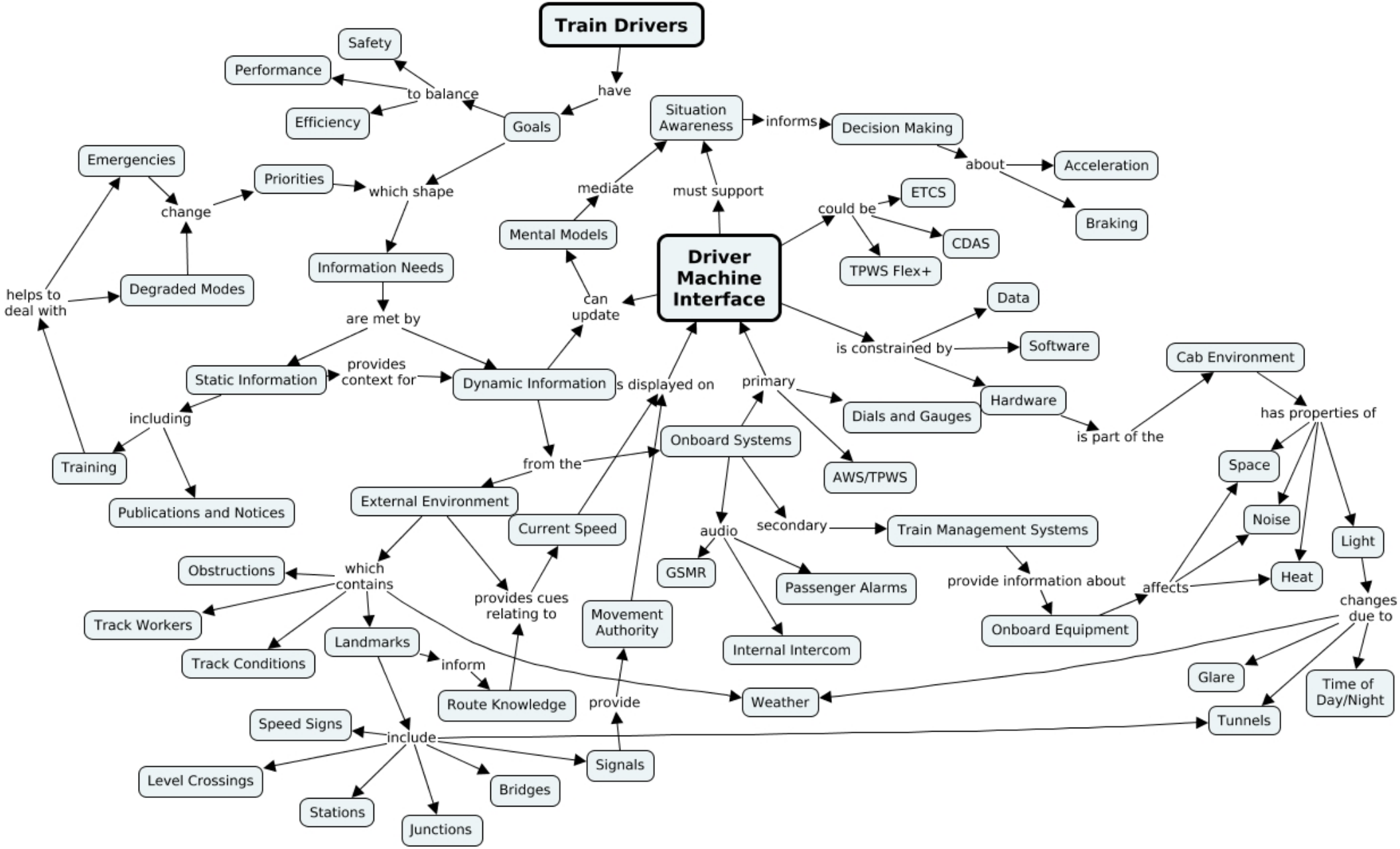

Incident Controller
Track Asset Owner
Request
Status
Report
PICOP
TSR
Planned Possessions
Track Data
Speed Limits
Status
EB Events
Possession Management System
TOC/FOC
PWAY/ Maintenance
Temp Speed
Activate Possession
Status
TSR Status
Train Location
Train Speed
EB Events
Location
Speed Limits
Status
Speed Adherence
EB Events
Diagnostics
Sign Placement
Lineside Indication
Track Map
Speed Limits
Warnings
Approval
Entry Request
Speed Limits
Infrastructure Data
Location
Speed
Status, Version
EB Activation
Speed Control (Driver)
Speed Supervision System
Speed
Power/Brake Setting
Train


Incident Controller
Track Asset Owner
Request
Status
Report
PICOP
TSR
Planned Possessions
Track Data
SPEED LIMITS
Status
EB Events
Possession Management System
TOC/FOC
PWAY/ Maintenance
TEMP SPEED
Activate Possession
Status
TSR Status
Train Location
Train Speed
EB Events
Location
SPEED LIMITS
Status
Speed Adherence
EB Events
Diagnostics
SIGN PLACEMENT
Lineside Indication
Track Map
SPEED LIMITS
Warnings
Approval
Entry Request
SPEED LIMITS
Infrastructure Data
Location
Speed
Status, Version
EB Activation
Speed Control (Driver)
Speed Supervision System
SPEED
Power/Brake Setting
Train

- STPA control structures are useful ***cognitive artifacts*** that offer ***decision making stability*** in the face of ***strategic uncertainty***.

- ***Blending STPA with human factors methods*** can surface ***system vulnerabilities*** and unlock opportunities for ***creative decision making and innovation***.

- STPA provides ***structure and processes*** to consider ***humans and machines as collaborative agents*** during the ***design of complex systems***.


Train Drivers
have
Goals
to balance
Safety
Performance
Efficiency
Emergencies
change
Priorities
which shape
Information Needs
are met by
Static Information
provides context for
Dynamic Information
including
Training
Publications and Notices
helps to deal with
Degraded Modes
Mental Models
mediate
Situation Awareness
informs
Decision Making
about
Acceleration
Braking
must support
Driver Machine Interface
can update
could be
ETCS
CDAS
TPWS Flex+
is constrained by
Data
Software
Hardware
is part of the
Cab Environment
has properties of
Space
Noise
Light
Heat
Glare
Time of Day/Night
changes due to
Tunnels
is displayed on
primary
Dials and Gauges
AWS/TPWS
Onboard Systems
from the
External Environment
Current Speed
audio
GSMR
Passenger Alarms
Internal Intercom
secondary
Train Management Systems
provide information about
Onboard Equipment
affects
Obstructions
which contains
Track Workers
Track Conditions
Landmarks
inform
Route Knowledge
provides cues relating to
Movement Authority
provide
Weather
Speed Signs
include
Level Crossings
Stations
Junctions
Bridges
Signals

Train Drivers

- have
  - Goals
    - to balance
      - Safety
      - Performance
      - Efficiency
    - which shape
      - Priorities
        - change
          - Emergencies
          - Degraded Modes
            - helps to deal with
      - Information Needs
        - are met by
          - Static Information
            - including
              - Training
              - Publications and Notices
            - provides context for
          - Dynamic Information
            - from the
              - External Environment
                - which contains
                  - Obstructions
                  - Track Workers
                  - Track Conditions
                  - Landmarks
                    - inform
                      - Route Knowledge
                        - provide
                          - Movement Authority
                            - provides cues relating to
                              - Current Speed
                                - can update
                                - Driver Machine Interface
                                - must support
                                - mediate
                                - Mental Models
                                - Situation Awareness
                                - informs
                                - Decision Making
                                - about
                                - Acceleration
                                - Braking
                                - could be
                                - ETCS
                                - CDAS
                                - TPWS Flex+
                                - is constrained by
                                - Data
                                - Software
                                - Hardware
                                - is part of the
                                - Cab Environment
                                - has properties of
                                - Space
                                - Noise
                                - Heat
                                - Light
                                - changes due to
                                - Glare
                                - Time of Day/Night
                                - Tunnels
                                - Weather
                                - include
                                - Speed Signs
                                - Level Crossings
                                - Stations
                                - Junctions
                                - Bridges
                                - Signals
                              - is displayed on
                                - Onboard Systems
                                - primary
                                - Dials and Gauges
                                - AWS/TPWS
                                - audio
                                - GSMR
                                - Passenger Alarms
                                - Internal Intercom
                                - secondary
                                - Train Management Systems
                                - provide information about
                                - Onboard Equipment
                                - affects

- STPA control structures are useful ***cognitive artifacts*** that offer ***decision making stability*** in the face of ***strategic uncertainty***.

- ***Blending STPA with human factors methods*** can surface ***system vulnerabilities*** and unlock opportunities for ***creative decision making and innovation***.

- STPA provides ***structure and processes*** to consider ***humans and machines as collaborative agents*** during the ***design of complex systems***.

Competency

Experience

Situation Awareness

Distributed Cognition

Decision Making

Fatigue

Mode Confusion

Usability

Mental Workload

Expertise

Cognitive Tunnelling

Vigilance

Physical Ergonomics

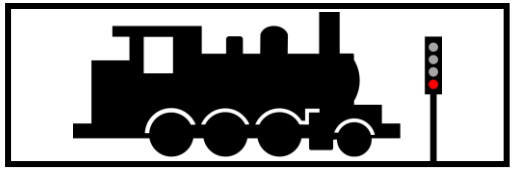
Divided Attention

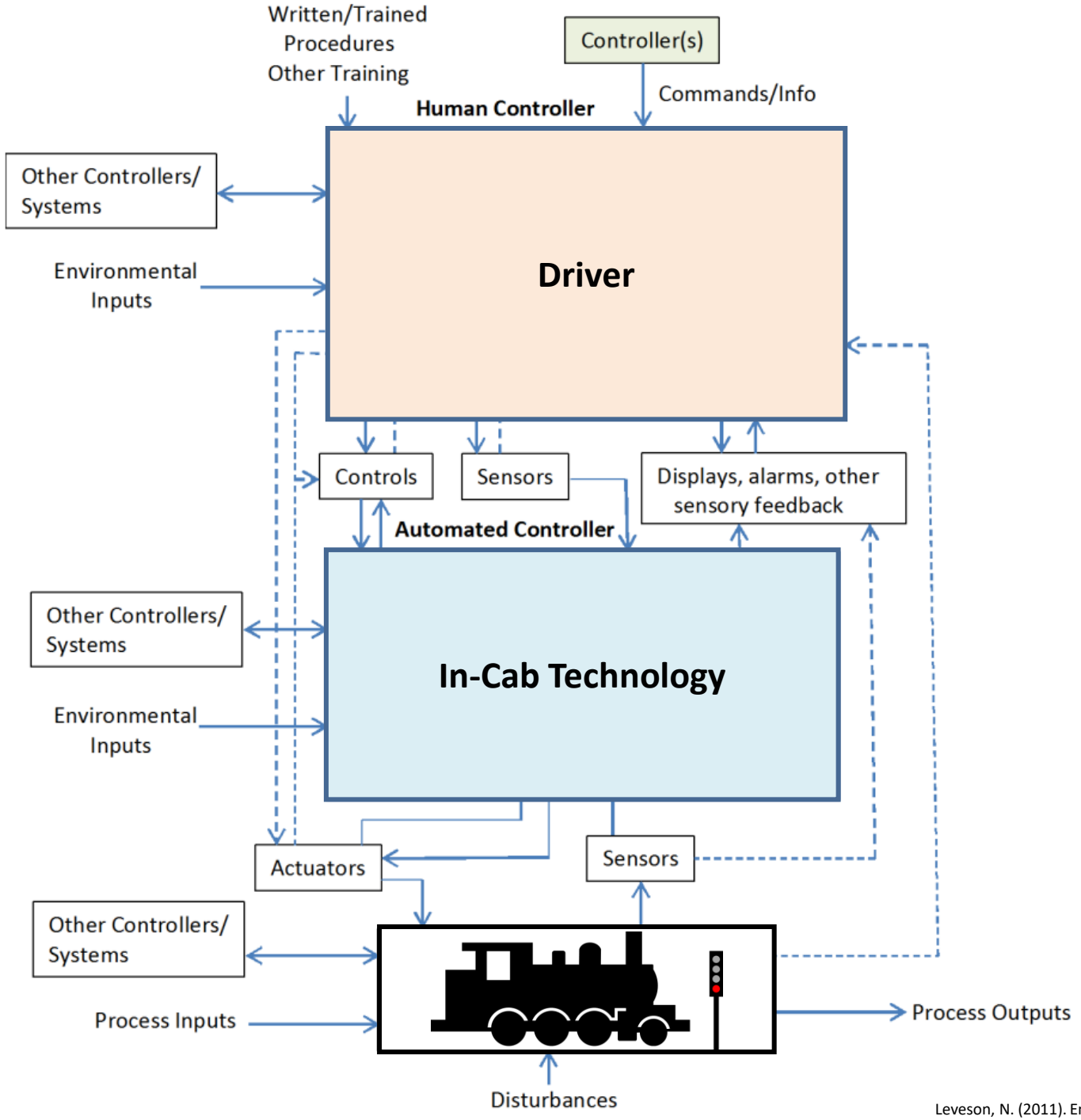
Cognitive Complexity

Stress

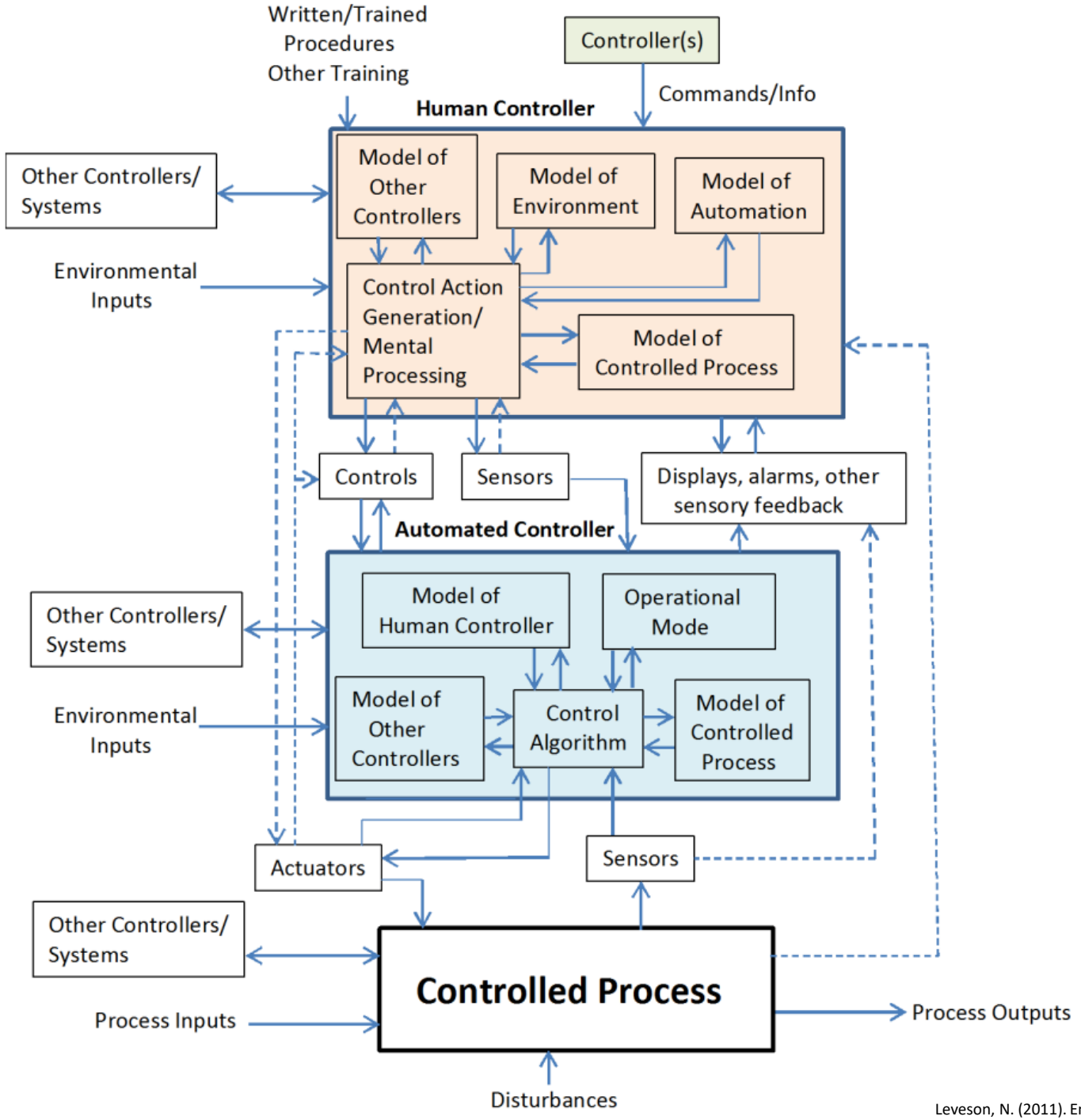
Driver

In-Cab Technology





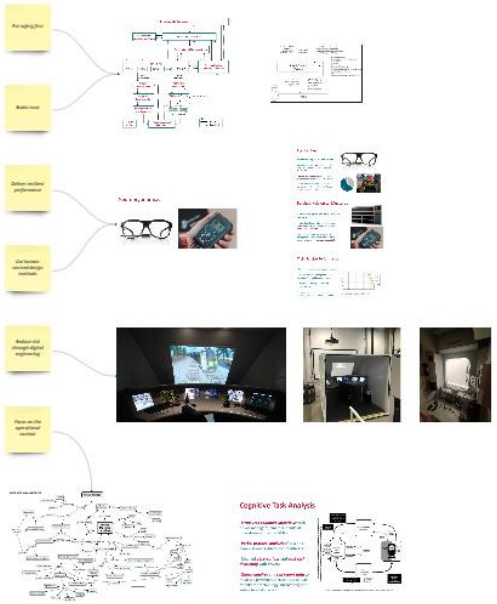
Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.



Leveson, N. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.

Human Factors Design Scope - Train Drivers

DMI Principles
- Consider the evidence
- Deliver the requirements



PROJECT

HUMAN FACTORS INTEGRATION 1

GOVERNANCE	CONTEXT OF USE	PEOPLE & PROCESSES	HARDWARE & ENVIRONMENTS	SOFTWARE & DATA	PERFORMANCE	ACCEPTANCE
Structured human factors integration processes shall be followed. 2	User requirements shall be developed and refined. 3	Human needs and capabilities shall inform the system design. 4	Hardware and environments shall be safe and fit for purpose. 5	System functionality shall be effective, and optimised for human use. 6	The system shall be efficient, effective and resistant to human error. 7	Suitable evidence for human factors acceptance shall be provided. 8

Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO)

TOC & FOC Org Factors

Target Audience Description

Lessons Learned

Scenarios

Cab Designs

Existing DMIs

Software Design Patterns

DMI: Human Factors RAIDO
- Analysis baseline of reference documentation
- Considerations register

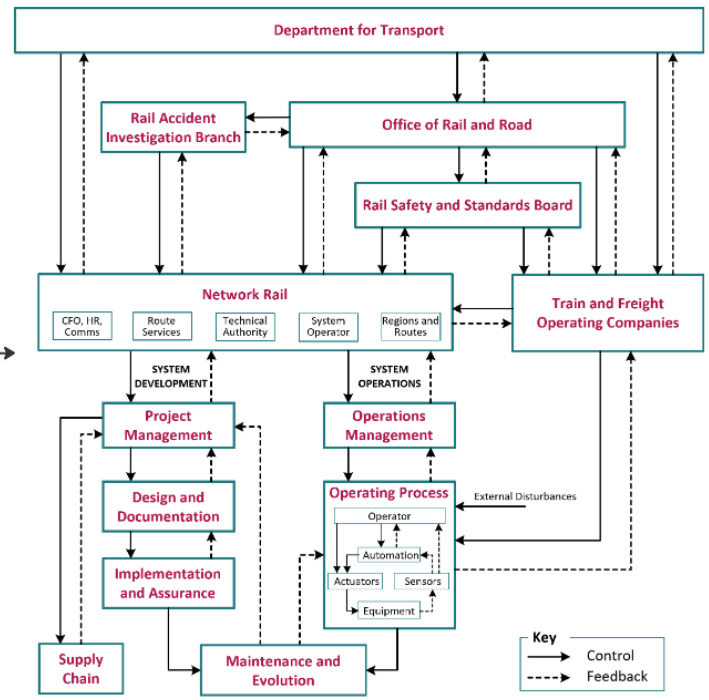
Cab Design Survey
- Volumes
- Types
- Variables
- Edge cases

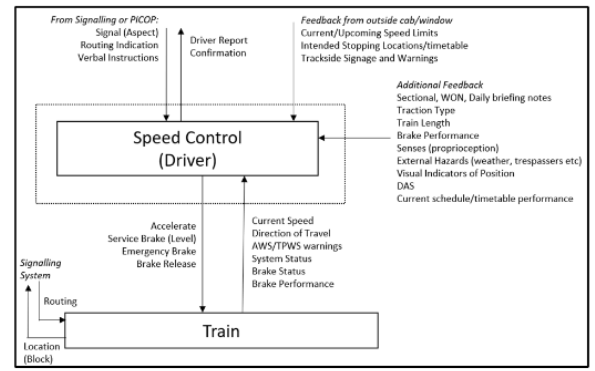
Operational Scenarios
- Goals
- Scenarios
- Tasks
- Decisions

DMI Market Scan
- Functionality
- Hardware
- Software

Put safety first

Evoke trust





Deliver resilient performance

Use human-centred design methods

Reduce risk through digital engineering

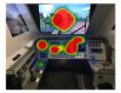
Neuroergonomics

Eye Tracking

Understanding where drivers look

-Allocation of ***visual attention*** through the analysis of fixations, saccades and dwell time

-***Mental workload*** evaluation through analysis of blink rate and pupil dilation



-Assessment of correlates of ***situation awareness*** such as 'look but fail to see' and cognitive tunnelling

Psychophysiological Measures

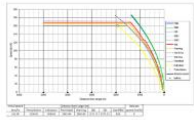
Understanding the biological markers of emotion

-Evaluation of uncertainty, time pressure, strain and workload through analysis of ***heart rate variability***

-Tracking attention, startle response, anticipation and moments of realisation using measures of ***electrodermal activity***

Train Service Performance

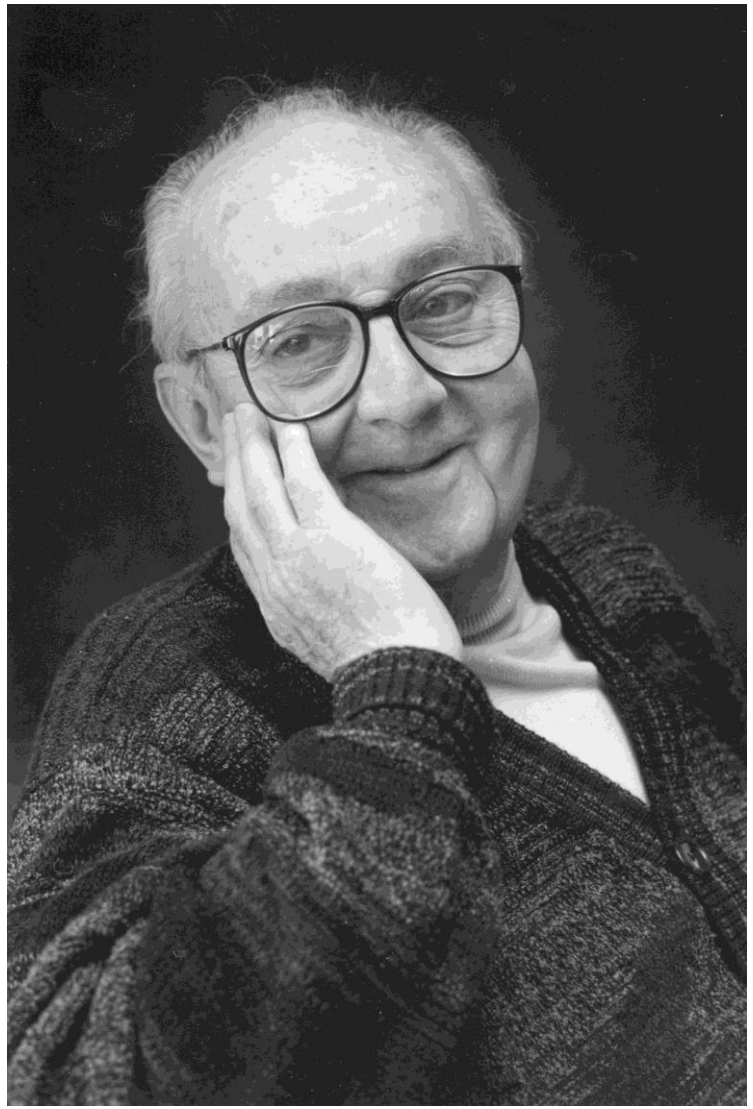
-Detailed measures of train performance



-Detailed distance-time graphs with speed profiles and braking curves

-Analysis of warning and braking interventions

-Comparisons between drivers and between levels of automation support



“The only way to know how a complex system will behave—after you modify it—is to modify it and see how it behaves.”

George E. P. Box

Network Rail Ergonomics

Human Factors-Centred Innovation

linkedin.com/in/richardbye