Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

INTRODUCTION TO STAMP

Dr. Robert J. de Boer
Aviation Academy, Amsterdam

Euro Stamp Workshop
Reykjavik, September 13th, 2017

Presentation based on:
- STPA Primer, Version 1.0; Leveson N. (2015). STAMP Tutorial, March 2015, MIT, Boston
- Masterclass Risk Assessment, N. Karanikas (2017), Aviation Academy, Amsterdam
- Masterclass Human Factors & Safety, RJ de Boer & S. Dekker (2017), Aviation Academy, Amsterdam
- Graduate thesis of Patrick van der Spek

OUR OBJECTIVES TODAY

- Comprehend fundamentals (and therefore the advantages) of Systems Thinking and STAMP model.
- Applying the systems theory and the STAMP concept in some short cases

"All models are wrong but some are useful."

-George EP Box

(Statistician)

IS IT PRACTICAL?

- STAMP has been or is being used in a large variety of industries (more than 160 published studies):
  - Spacecraft
  - Aircraft
  - Air Traffic Control
  - UAVs (RPAs)
  - Defense
  - Automobiles (GM, Ford, Nissan)
  - Medical Devices and Hospital Safety
  - Chemical plants
  - Oil and Gas
  - Nuclear and Electrical Power
  - $C0_2$ Capture, Transport, and Storage
  - Finance

DOES IT WORK?

- In all cases where a comparison was made (to FTA, HAZOP, FMEA, ETA, etc.)
  - STPA found the same hazard causes as the old methods
  - Plus it found more causes than traditional methods
  - In some evaluations, found accidents that had occurred that other methods missed.
  - Cost was orders of magnitude less than the traditional hazard analysis methods.

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

ACCIDENT CAUSALITY AND MODELS

www.international.hva.nl

ACCIDENT CAUSALITY MODEL. WHY?

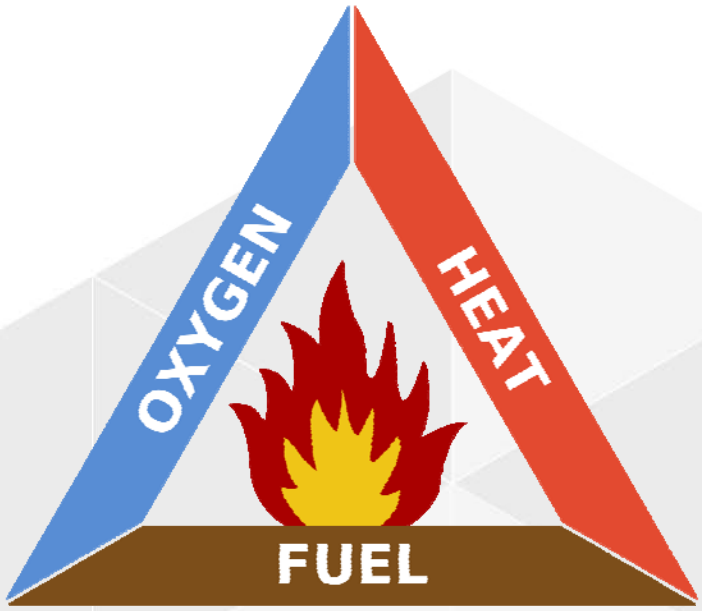
- The underlying accident causality model or assumptions determine the success of our efforts to understand what happened
- We always use an accident model, even unconsciously.

WHAT ACCIDENT CAUSALITY MODEL DO YOU USE?

- Approaches to accidents:
  - Unfortunate but unavoidable results of random events.
  - Results of individual component failures.
  - Results of simultaneously or consecutively failing protections
  - Results of dysfunctional interactions and inadequately controlled processes in the system.

WHAT IS A CAUSE?

- Let's examine the example of a fire:
  - What are the conditions?
  - Are all necessary?
  - Is their existence in isolation sufficient to start a fire?
- Causes: Sets of necessary conditions, named causal scenarios.

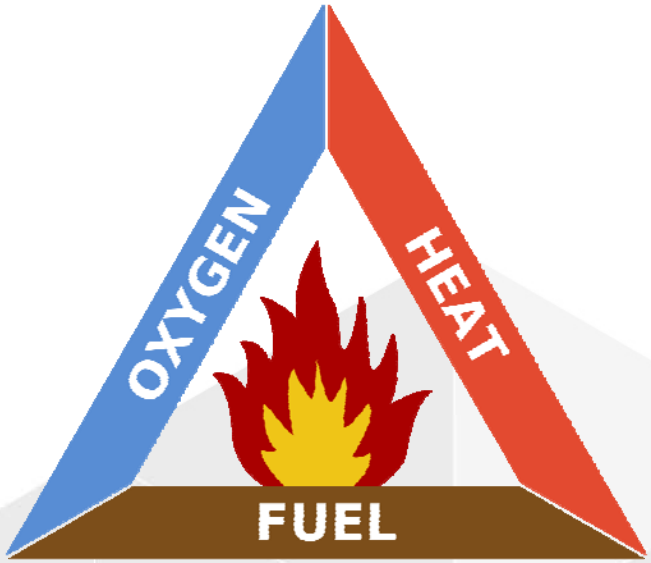


CAUSALITY

- The relation among the fire conditions imply:
  - Linear relationship
  - Causality

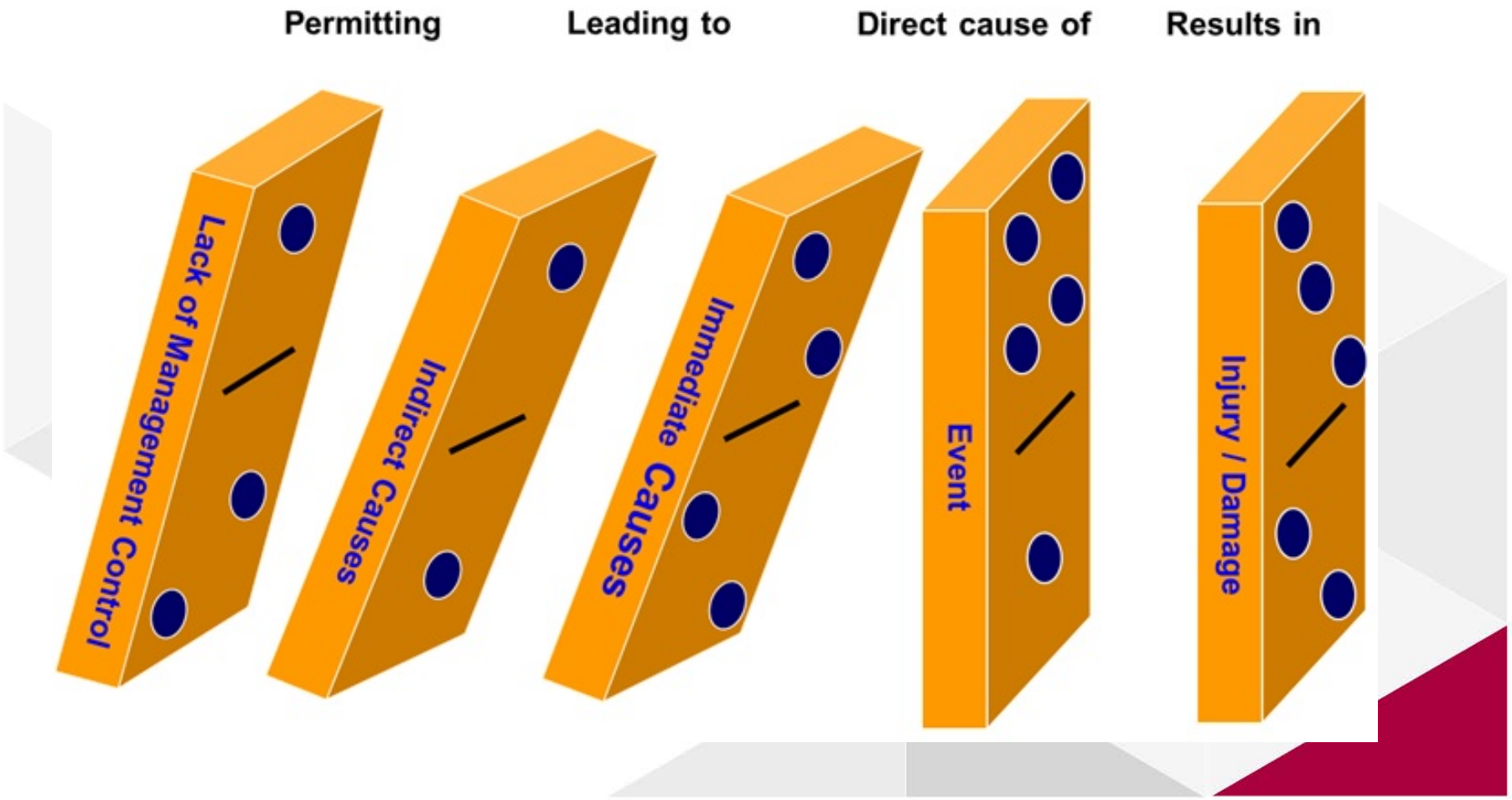
If “A” occurs while “B” and “C” → Then “D” occurs

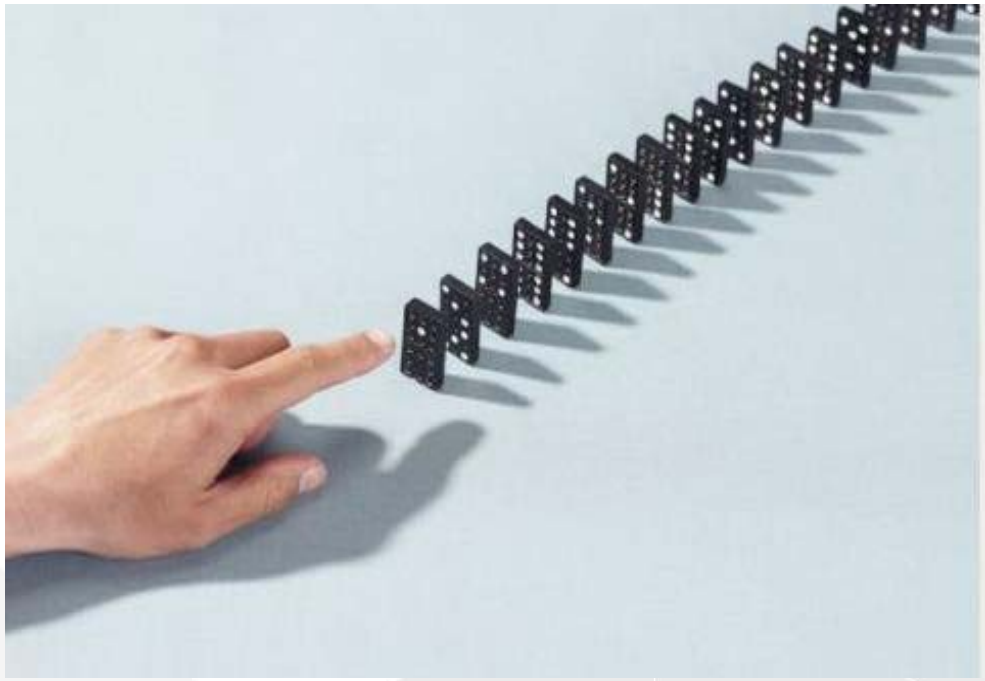
If “D” occurred while “B” and “C” → Then “A” has occurred



Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

HEINRICH'S DOMINO MODEL OF ACCIDENT CAUSATION (1932)



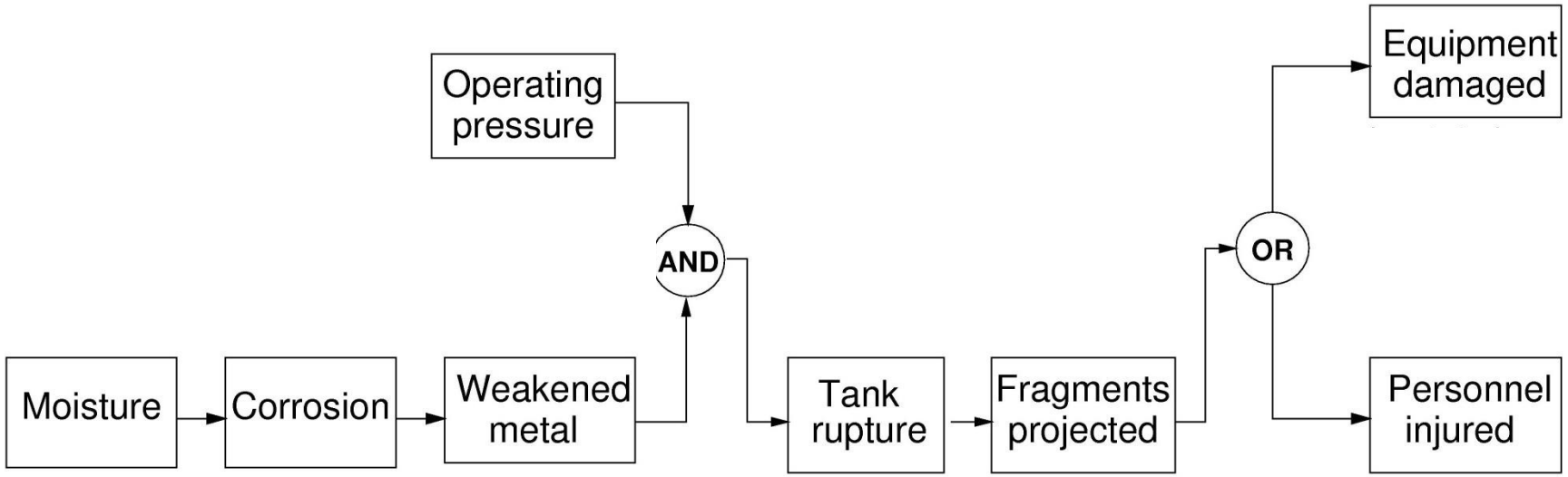


DC-10:

Cargo door fails → Causes → Floor collapses → Causes → Hydraulics fail → Causes → Airplane crashes

Chain of Failure Events

CHAIN-OF-EVENTS EXAMPLE



THE CASE OF THE MISTAKEN TAKE-OFF

- On Feb 10th 2010, a KLM 737 took off from a taxiway

THE CASE OF THE MISTAKEN TAKE-OFF

- Aircraft had been de-iced on an apron
- Light snow on taxiways.
- ATC instructed to taxi to the departure runway 36C via taxiway ‘A’
  - Was against prescribed direction of travel
  - There are two parallel taxiways adjacent to runway 36C
- High workload
- During taxi ATC suggested W8 entry and this was accepted.
- Whilst on W8 received ‘line up and wait’ and take off clearances in quick succession.
- Neither green taxiway lighting nor yellow taxi lines nor blue markers visible at turn off although the airport complies to ICAO standards.
- Plane turned right again onto taxiway ‘B’ and began a standing start take off.
- Aircraft was not monitored by ATC between clearance and take-off.
- Air traffic control informed the crew of the incident during climb.

CAL5420
PH-BDP
-transfer PH-BDP
-entry becomes W8
-line up and wait
(36C W8)
-line up permitted?
+ confirmation line up
-transfer CAL5420
- problems CAL5420
dedicated route
takeoff clearance
W8
W9
W10
W11
W12
Image © 2011 Aerodata International Surveys

SKYbrary

The single point reference for aviation safety knowledge

Google™ Custom Search

navigation
- Home page
- Operational issues
- Human performance
- Enhancing safety
- Safety regulations
- Accidents and incidents
- Aircraft Types
- Airport Directory
- Toolkits
- Bookshelf
- Publications
- OGHFA

information
- About SKYbrary
- Contact us
- Help
- Who is who
- Glossary
- Promotion

tools
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information
- Browse properties

If you wish to contribute or participate in the discussions about articles you are invited to ***join*** *SKYbrary as a registered user*

Operational Issues | **Human Performance** | **Enhancing Safety** | **Safety Regulations**


Air Ground Communication


Airspace Infringement


Bird Strike


Controlled Flight Into Terrain


Fire Smoke & Fumes


Ground Operations


Airworthiness


Level Bust


Loss of Control


Loss of Separation


Runway Excursion


Runway Incursion


Wake Vortex Turbulence


Weather


Emergency and Contingency

Highlighted Article

The importance of visually checking the runway for obstructions as you approach touchdown…

posted 6 July 2015 in Category:Accidents and Incidents

On 26 July 2014, the crew of an aircraft which had just touched down at Perth saw the rear of a stationary vehicle on the runway centreline approximately 1180 metres from the landing threshold. An immediate go around was called and made and the aircraft cleared the vehicle by about 150 feet. The same experienced controller who had issued the landing clearance was found to have earlier given runway occupancy clearance to the vehicle.

Read more >>

2015 Safety Forum Automation and Safety

One Safety Issue - One Coordinated

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

THE CASE OF THE MISTAKEN TAKE-OFF

- Skybrary summary of the incident:

> On 10 February 2010 a KLM Boeing 737-300 unintentionally made a night take off from Amsterdam in good visibility from the taxiway parallel to the runway for which take off clearance had been given. Because of the available distance and the absence of obstructions, the take off was otherwise uneventful. The Investigation noted the familiarity of the crew with the airport and identified apparent complacency.

http://www.skybrary.aero/index.php/B733,_Amsterdam_Netherlands,_2010; accessed April 22nd, 2016

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

THE CASE OF THE MISTAKEN TAKE-OFF: DISCUSSION (1)

- Do you agree with “the familiarity of the crew with the airport and […] apparent complacency” as the main cause of this incident?
- What do we learn from such an analysis, and what can we change?

IS OUR PERCEPTION OF LINEAR CAUSES ALWAYS VALID?

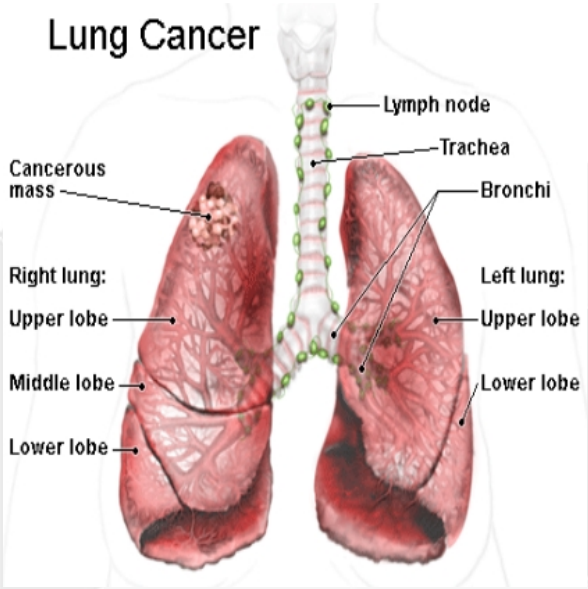
IF -> THEN (?)

????

IS OUR PERCEPTION OF LINEAR CAUSES ALWAYS VALID?

IF -> THEN (?)

????

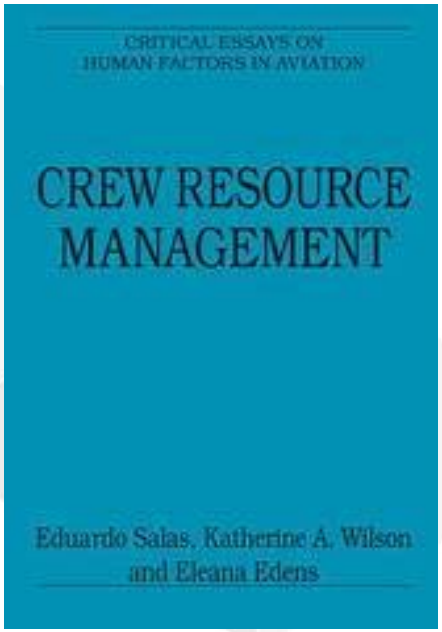


IS OUR PERCEPTION OF LINEAR CAUSES ALWAYS VALID?

IF -> THEN (?)

????

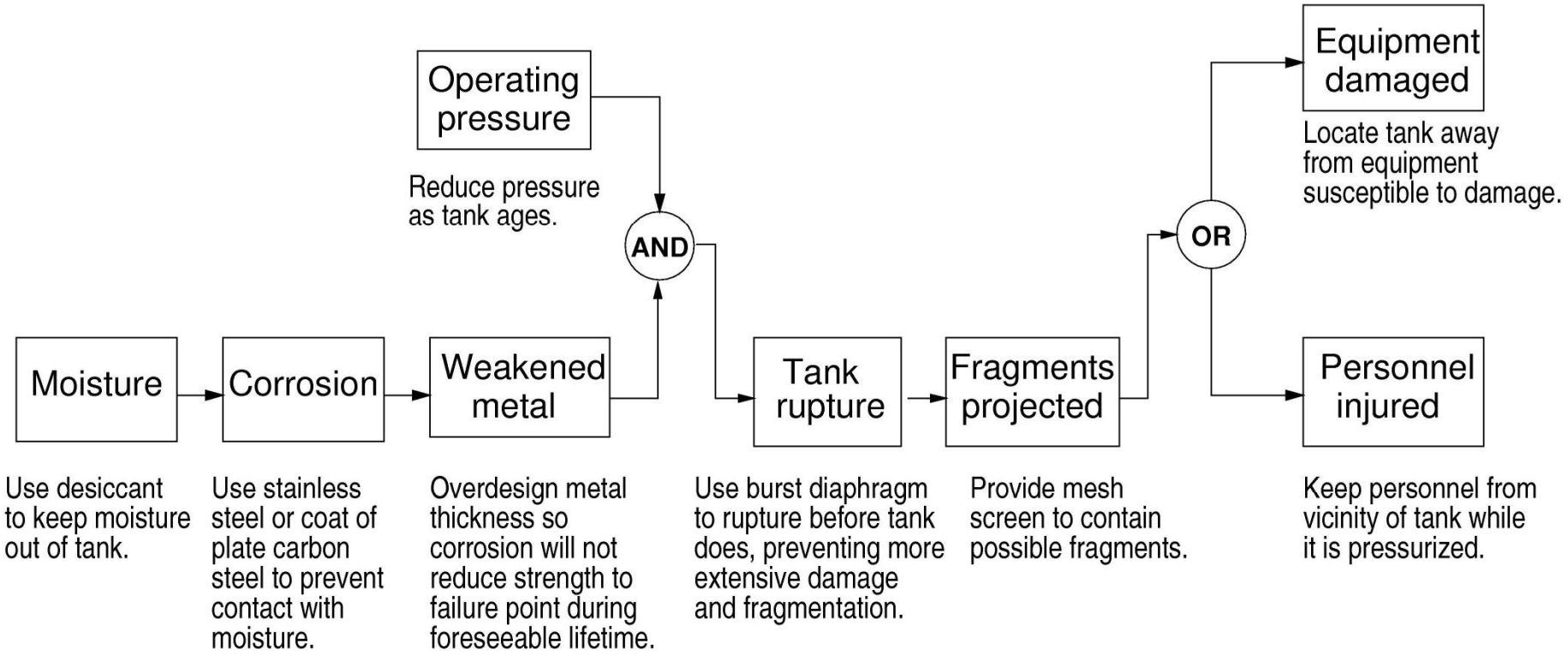
IS OUR PERCEPTION OF LINEAR CAUSES ALWAYS VALID?



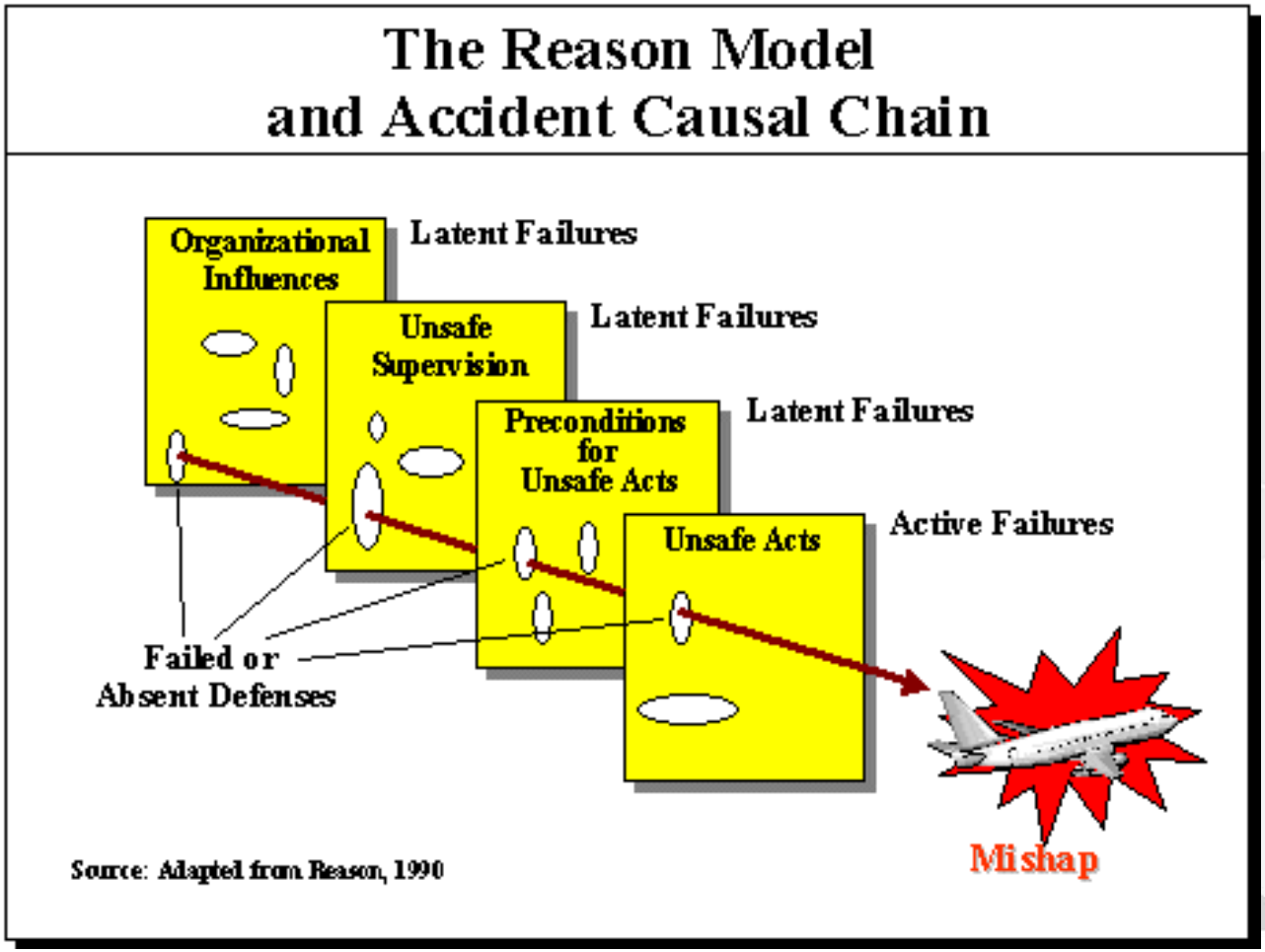
IF -> THEN (?)

????

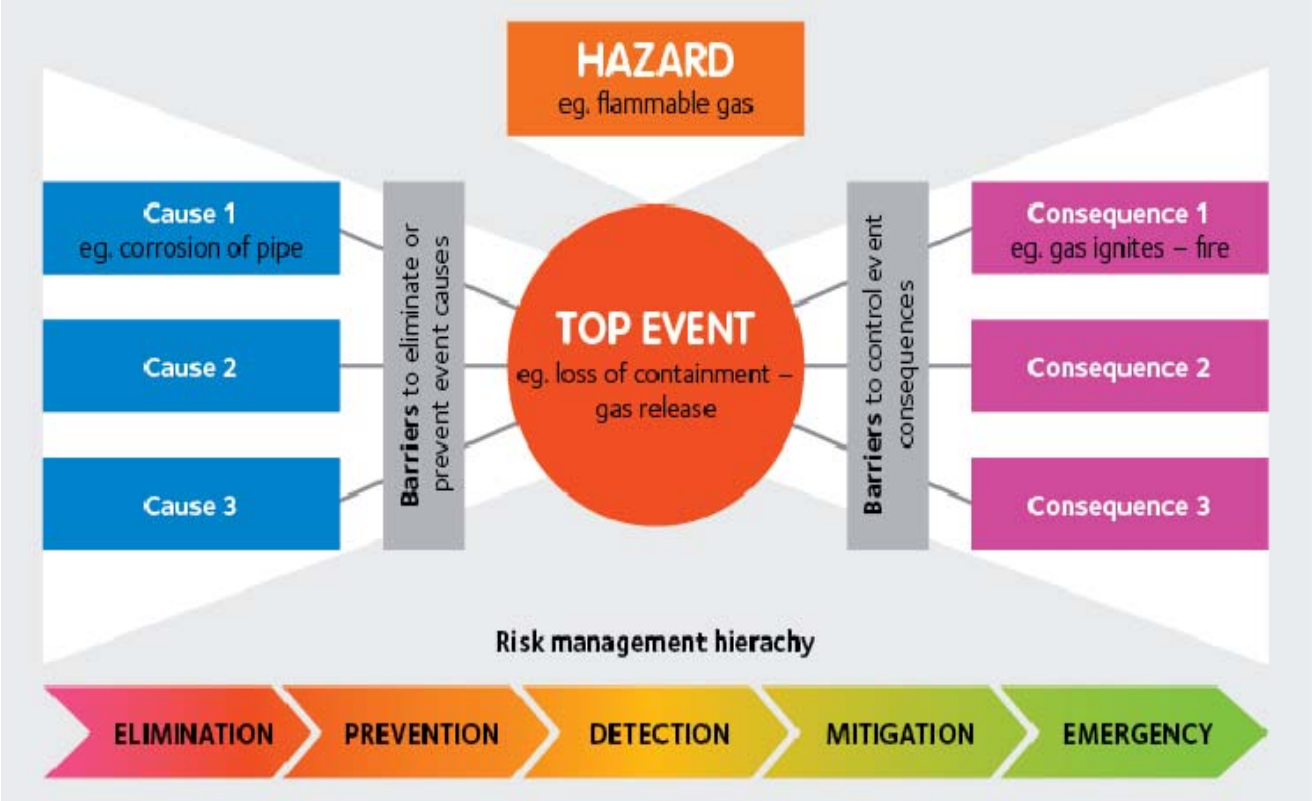
CHAIN-OF-EVENTS AND BARRIERS EXAMPLE



CHAIN-OF-EVENTS AND BARRIERS INTO LAYERS



SETTING MORE BARRIERS



Typical causal factors:
Hardware
Software
Human errors
Unleashed energy

Solutions:
More barriers
More reliability

EPIDEMIOLOGY (CHAIN-OF-EVENTS)

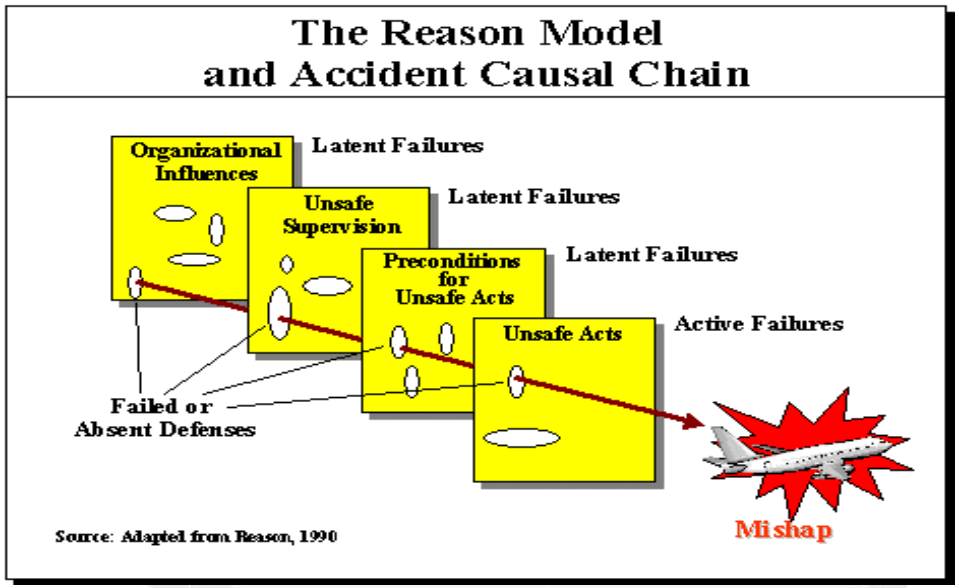
- Descriptive epidemiology: rates associated with characteristics (e.g., age, sex, experience).
- Investigative epidemiology: specific causes of injuries and deaths are collected in order to devise feasible countermeasures.
  - Assumes common factors in accidents, but those can only be determined by statistical evaluation of accident data.
  - Can be used proactively to identify potential causes for accidents in specific system designs.

THE CASE OF THE MISTAKEN TAKE-OFF (2)

- Using the ‘Swiss cheese’ model, identify which barriers failed in the case of the mistaken take-off.
- What can we learn from these?

== 10 minutes ==

- Present your results to the rest of the group



POSSIBLE FAILING “BARRIERS” IN THE CASE OF THE MISTAKEN TAKE-OFF

- Unusual taxiway direction
- Green centerline lights missing
- No ATC monitoring of airplane
- Pilot missed visual cues
- Pilot did not use ground movement chart

DUTCH SAFETY BOARD CAUSES

- "The serious incident occurred because of the flight crew's lack of awareness of the aircraft's position […]".
- Contributing factors:
  - Flight crew had less time to check aircraft position due to having to enter changes in flight management computer after accepting shorter route ("workload")
  - ✓ The crew was not using a ground movement chart "as they felt they were sufficiently familiar with their home base".
  - The pilot in command was "distracted" by radio traffic with another aircraft
  - The air traffic controller was forced to shift his attention and assumed that the flight crew would follow his instructions correctly
  - ✓ Aircraft was not monitored by ATC between clearance and take-off.
- Also discussed, but not listed as a contributing factor:
  - ✓ Lack of green centerline lights on taxiway
  - ✓ Taxiing against prescribed direction
  - ✓ ATC monitoring and guidance
  - Production pressure

OVV 2011

IN SUMMARY: TWO TRADITIONAL FAMILIES OF SAFETY MODELS

- Single (root) cause models, such as the “Domino” model:
  - Suggest that a triggering event sets a causal sequence in motion that leads to a harmful event (e.g., Underwood & Waterson, 2013).
- Epidemiological (multiple causes) models, such as the “Swiss cheese” model (Reason, 1990):
  - Differentiates between active failures (i.e. actions and inactions) and latent conditions (i.e. individual, interpersonal, environmental, supervisory and organisational factors present before the accident)
  - The use of defences to counteract for possible failures is common across those types of models, such as the bow-tie (e.g., Boishu, 2014), Threat & Error Management (e.g., Maurino, 2005) and Tripod (e.g., Kjellen, 2000).

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

THE NEW REALITY: COMPLEX SYSTEMS

www.international.hva.nl

MODERN SYSTEMS

- Human role has shifted: complex decision making, variable cognitive workload, monitoring vs operating etc.
- Nature of human error has changed: mode confusion, complacency etc.

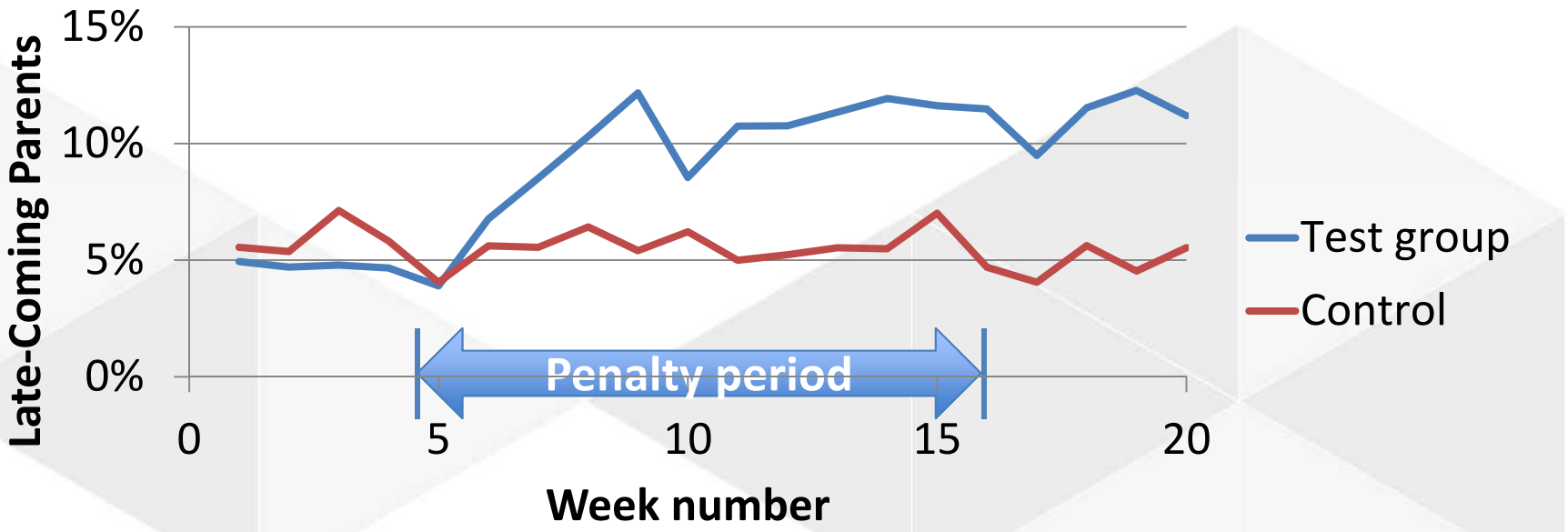
RULE VIOLATION IN DAY CARE

- 10 day-care centers in Israel
- Operate 07:30 - 16:00
- Frequent late parents (1~2 daily)
  - Teacher has to stay
  - No consequences for parents
  - Parents rarely came after 16:30
- Solution: introduce small $ penalty for delay > 10 minutes

➔ What was the net effect?

Gneezy and Rustichini 2000

INTRODUCTION OF $ PENALTIES LED TO A UNYIELDING INCREASE IN RULE VIOLATION



Gneezy and Rustichini 2000


Video

THE CASE OF THE MISTAKEN TAKE-OFF (3)

- Recently, so called ‘systemic’ models have been introduced that focus on ‘faulty’ interactions between elements, rather than faults in the elements themselves.
  - Which interactions were relevant in the current case?
  - Which of these can be judged as ‘flawed’?
- What can we learn from these?

== 10 minutes ==

- Present your conclusions to the rest of the group

THE CASE OF THE MISTAKEN TAKE-OFF

Relevant 'flawed' interactions

- ATC ⇔ Pilots : unusual taxiway direction, late change of runway entry, early take-off clearance
- Pilots ⇔ aircraft: high work pressure
- Pilot ⇔ taxiway: unusual taxiway, position not monitored
- ATC ⇔ aircraft: position was not monitored
- Pilots ⇔ management: punctuality
- ATC ⇔ management: capacity
- Pilots, ATC ⇔ other traffic: was blocking the way
- Pilots ⇔ environment: light snow, dusk lighting, lights in the distance,
- Pilots ⇔ airport: no green center line
- ICAO ⇔ airport: green centerline not compulsory

Newtonian-Cartesian

System behavior can be reduced to component behavior

Effects have proportional causes

Harm is foreseeable

Time is reversible

Complete knowledge is possible

Foreseeability

Current state known?

Laws by which system operates known?

Then all other states can be predicted/postdicted

Griffith UNIVERSITY

Complexity

System behavior cannot be reduced to component behavior:

- emergence, relationships

Cause-effect asymmetry

Only probabilities are foreseeable

Time is irreversible

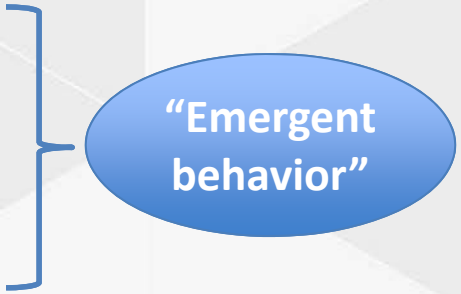
Complete knowledge is impossible:

- open systems
- multiple legitimate descriptions, always out of date

MOST ENGINEERED SYSTEMS ARE "COMPLEX"

Complex system characteristics

- Are open to influences from the environment and vice-versa
- Components are ignorant of system behavior and effects of own actions on it
- Interaction is complex, not necessarily the components
- **Complex systems not in static equilibrium: feedback loops required**
- **History or path dependence (non-Markov)**
- **Non-linear interactions ("Butterfly effect")**
- **New structures are generated "internally"**



Dekker , Cilliers, Hofmeyr 2013; Cilliers 1998; Dekker, 2011, cited in Salmon, McClure, Stanton 2012

EMERGENT BEHAVIOR IS..

- A result of interactions of system components
- Therefore not predictable beforehand …
- But … comprehendable in retrospect

Griffith UNIVERSITY

When things fail

Have no coherent theory for how such complexity develops

Apply linear, componential explanations for when it fails

- Our technologies have got ahead of our theories

Newton

organization as machine

order through hierarchy, control

focus on local part

develop one best method for it

work describable, predictable

compliance

Complexity

organization as living system

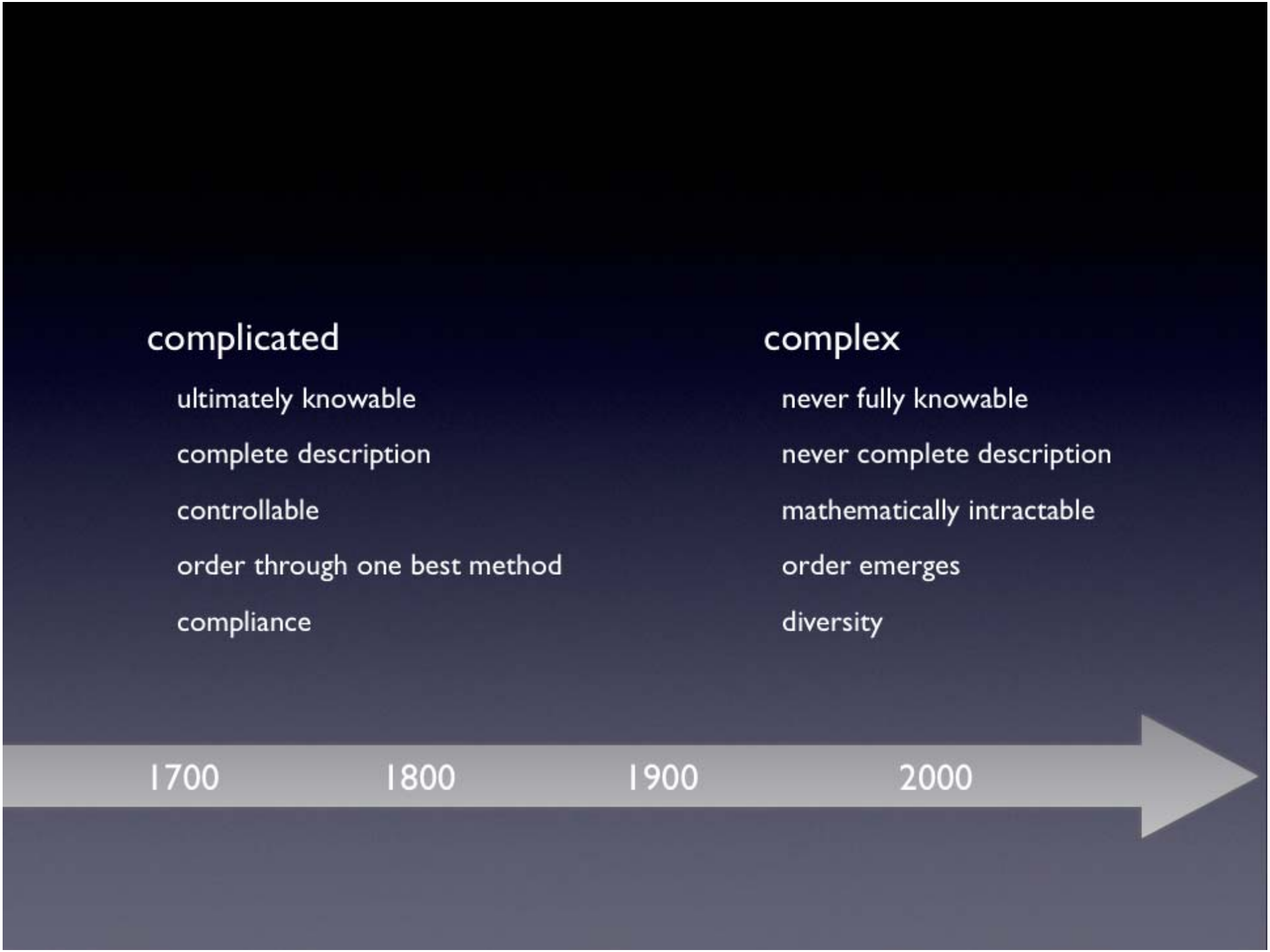
order emerges

local decisions, global influence

balance exploration/exploitation

never complete description

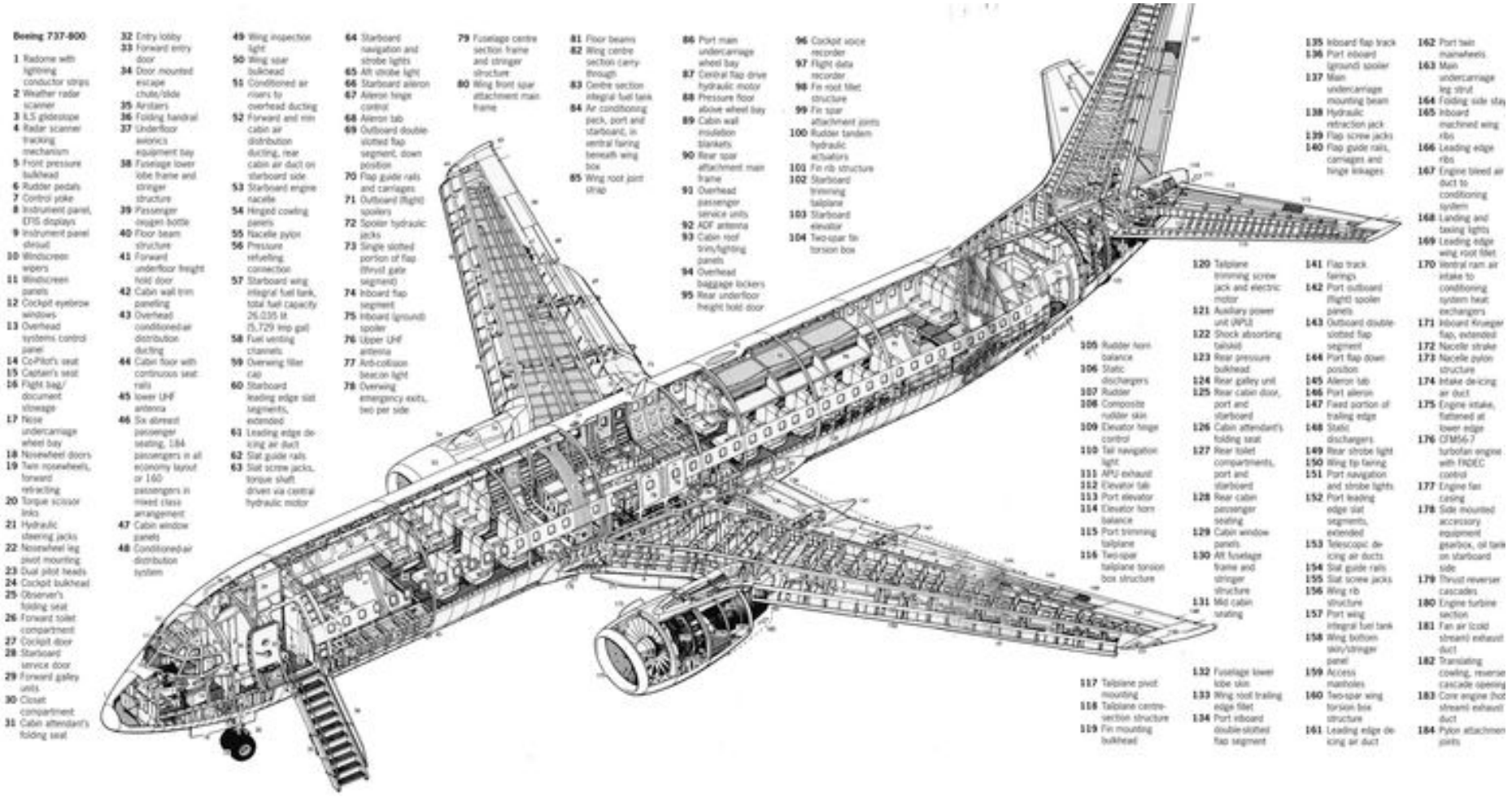
diversity


complicated
ultimately knowable
complete description
controllable
order through one best method
compliance
complex
never fully knowable
never complete description
mathematically intractable
order emerges
diversity
1700
1800
1900
2000

Complicated or complex?

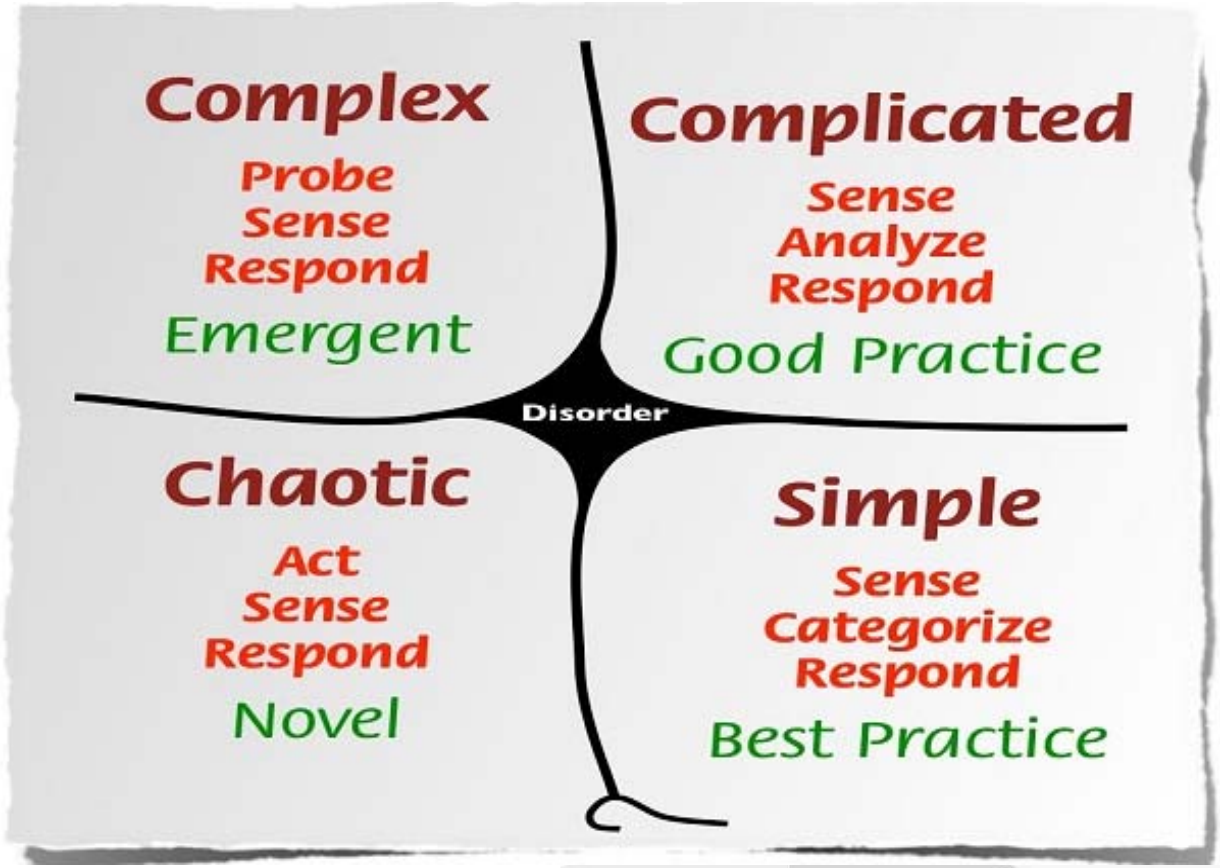
sidneydekker.com

Complicated or complex?



video

THE CYNEFIN FRAMEWORK

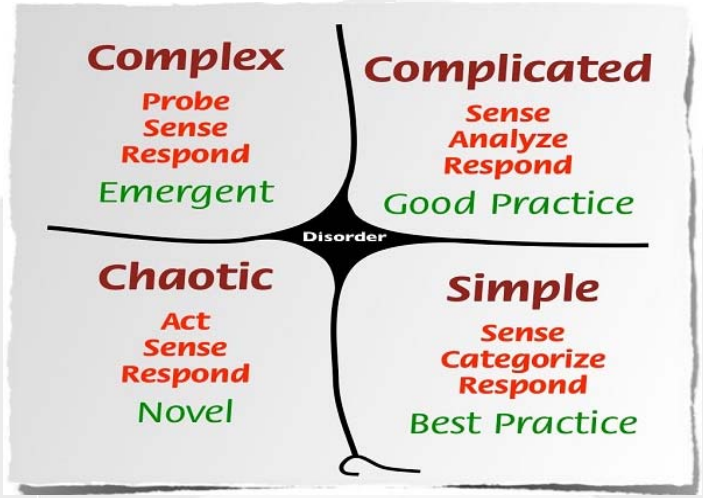


Snowden & Boone 2007

EMERGENT PROPERTIES IN YOUR SYSTEMS

- What examples of complicated and complex (sub-)systems can you identify in your organization?
- What emergent behavior is apparent in the complex (sub-)systems in your own organization?

The Cynefin framework



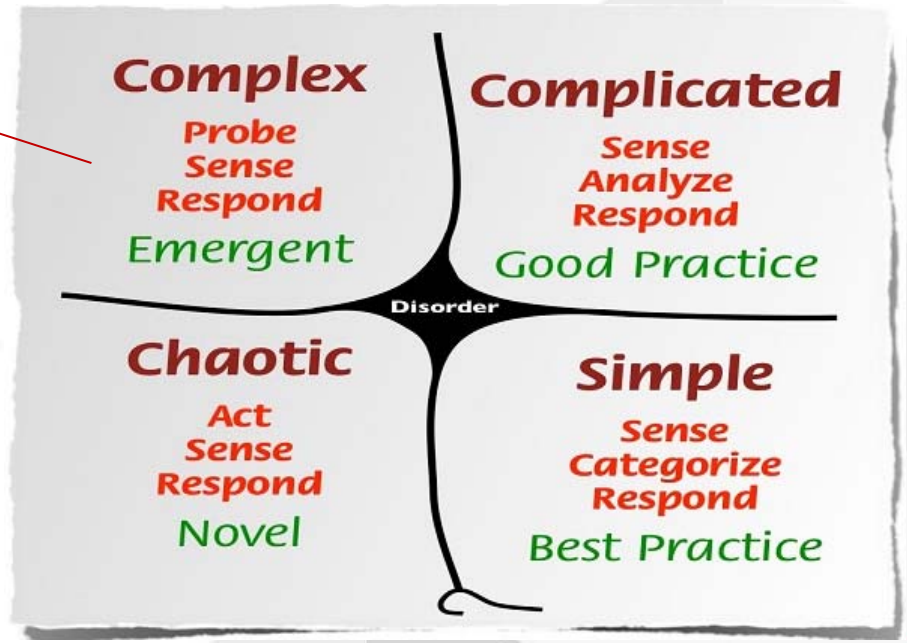
PROBING AND SENSING IS ESSENTIAL IN THE COMPLEX DOMAIN

Probe by safe to fail experiments

Sense emerging patterns

Respond by amplifying or dampening

The Cynefin framework



Snowden & Boone 2007

COMPLICATED VERSUS COMPLEX

- **Complicated system**
- Interactions governed by fixed relationships
- Reliable prediction of technical, time and costs issues
- E.g. an automobile or even an airplane
- Understanding by breaking it down
- “Good practice”

- **Complex systems**
- Self-organization
- Managerial independence
- Local interactions give rise to novel, nonlocal emergent patterns
- Geographical distribution
- Evolutionary development
- Always the case for a System of Systems (SoS)
- E.g. air transport system
- Understanding by iterative exploration and adaption
- Holistic approach

Hogeschool van Amsterdam
Techniek

DECISIONS IN COMPLEX CONTEXTS

Characteristics

- Flux and unpredictability
- No right answers, emergent instructive patterns
- Unknown unknowns
- Many competing ideas
- A need for creative and innovative approaches
- Pattern-based leadership

Danger Signals

- Temptation to fall back into habitual, command-and-control mode
- Temptation to look for facts rather than allowing patterns to emerge
- Desire for accelerated resolution of problems or exploitation of opportunities

Response to Danger Signals

- Be patient and allow time for reflection
- Use approaches that encourage interaction so patterns can emerge

The Leader's Job

- Probe, sense, respond
- Create experiments for patterns
- Increase levels of interaction
- Generate ideas

$$\Delta u_n = K_P \cdot \left[(eP_n - eP_{n-1}) + \left(\frac{T_s}{T_i} \cdot e_n \right) + \frac{T_d}{T_s} \cdot (eDf_n - 2 \cdot eDf_{n-1} + eDf_{n-2}) \right]$$

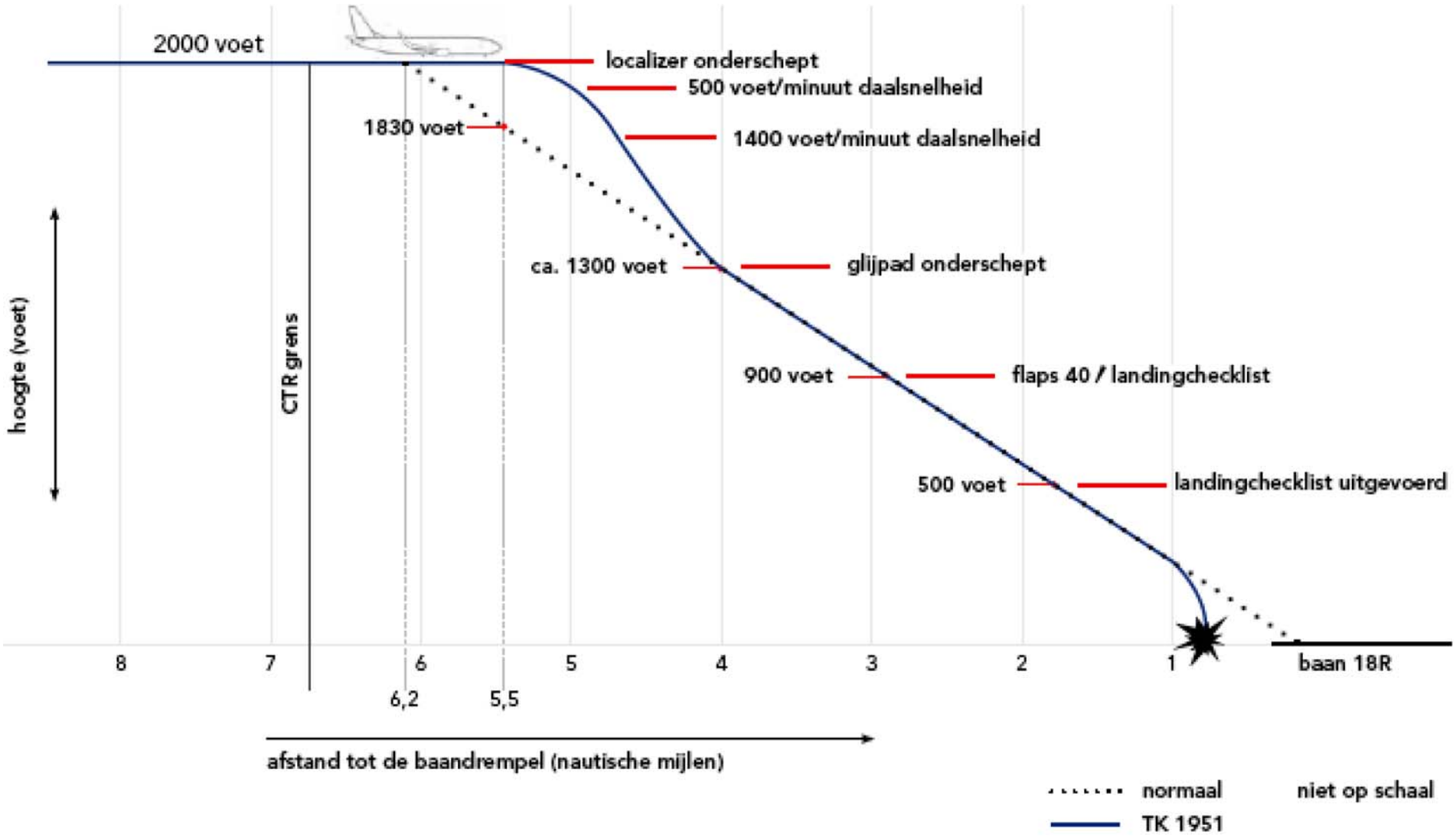
Variable	Description
Δu_n	The incremental output
K_P	Proportional gain
eP	Proportional error with reference weighing
	$eP = \beta \cdot r_n - y_n$
	where:
	β: Weighing factor
	r_n: Reference (setpoint)
	y_n: Process value, measured
e_n	Error, $e_n = r_n - y_n$
T_s	Sampling interval (i.e. Δt)
T_i	Integrator time
T_d	Derivator time
eDf	Derivate error with reference weighing and filtering
	$eDf_n = eDf_{n-1} / (\frac{T_s}{T_f} + 1) + eD_n \cdot \frac{T_s}{T_f} / (\frac{T_s}{T_f} + 1)$
	where:
	T_f: Filter time
	$T_f = \alpha \cdot T_d$ where α usually is set to 0.1
	eD: Unfiltered derivate error with reference weighing
	$eD = \gamma \cdot r_n - y_n$
	where:
	γ: Weighing factor
u_n	absolute output

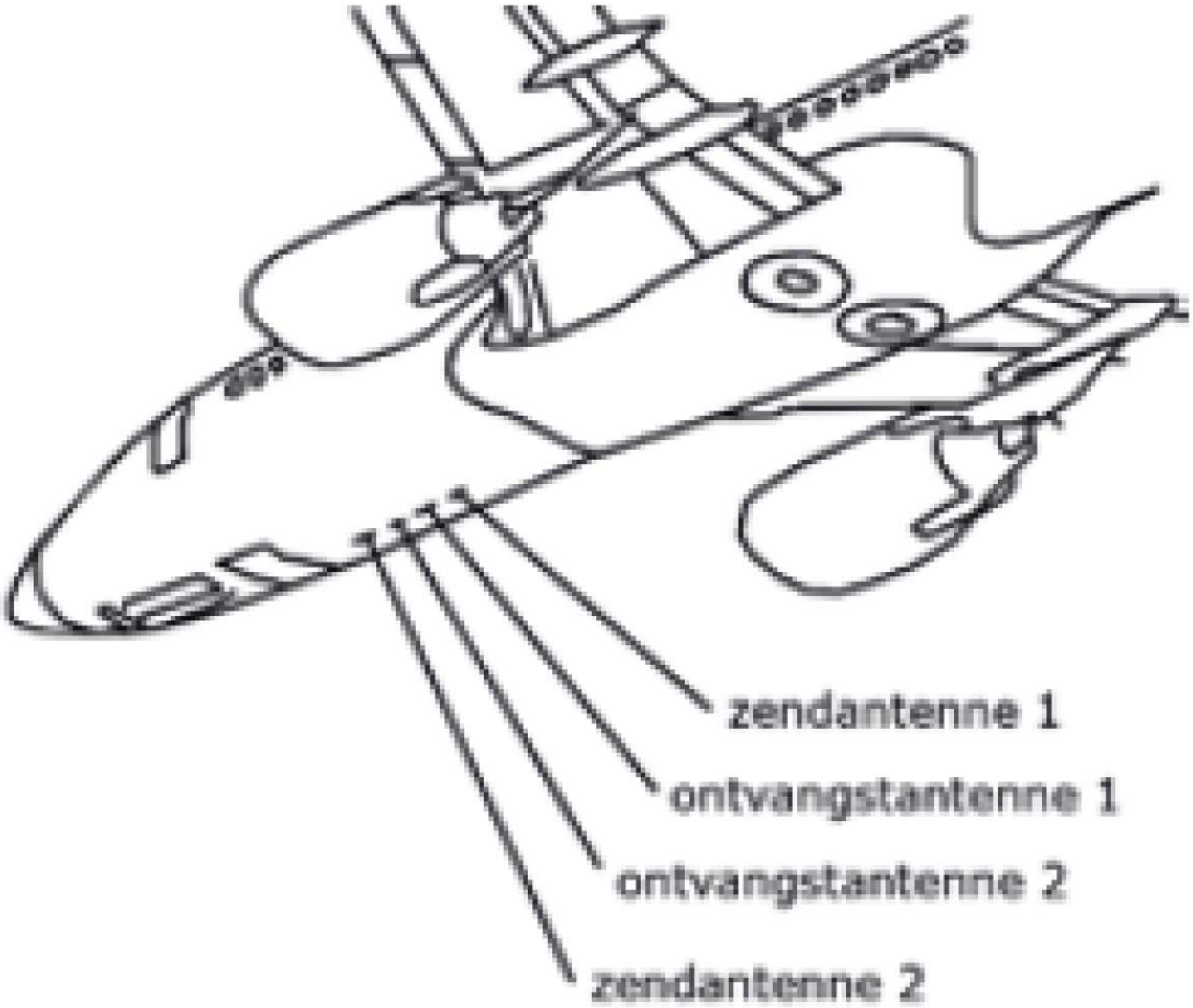
$$\Delta u_n = K_P \cdot \left[(eP_n - eP_{n-1}) + \left(\frac{T_s}{T_i} \cdot e_n \right) + \frac{T_d}{T_s} \cdot (eDf_n - 2 \cdot eDf_{n-1} + eDf_{n-2}) \right]$$

Variable	Description
Δu_n	The incremental output
K_P	Proportional gain
eP	Proportional error with reference weighing
	$eP = \beta \cdot r_n - y_n$
	where:
	β: Weighing factor
	r_n: Reference (setpoint)
	y_n: Process value, measured
e_n	Error, $e_n = r_n - y_n$
T_s	Sampling interval (i.e. Δt)
T_i	Integrator time
T_d	Derivator time
eDf	Derivate error with reference weighing and filtering
	$eDf_n = eDf_{n-1}/(\frac{T_s}{T_f} + 1) + eD_n \cdot \frac{T_s}{T_f}/(\frac{T_s}{T_f} + 1)$
	where:
	T_f: Filter time
	$T_f = \alpha \cdot T_d$ where α usually is set to 0.1
	eD: Unfiltered derivate error with reference weighing
	$eD = \gamma \cdot r_n - y_n$
	where:
	γ: Weighing factor
u_n	absolute output

Other automated control systems?

Flight crew?


2000 voet
localizer onderschept
500 voet/minuut daalsnelheid
1830 voet
1400 voet/minuut daalsnelheid
ca. 1300 voet
glijpad onderschept
900 voet
flaps 40 / landingchecklist
500 voet
landingchecklist uitgevoerd
hoogte (voet)
CTR grens
8
7
6
5
4
3
2
1
baan 18R
6,2
5,5
afstand tot de baandrempel (nautische mijlen)
normaal
niet op schaal
TK 1951


zendantenne 1
ontvangstantenne 1
ontvangstantenne 2
zendantenne 2

Anatomy of the TK1951 Automation Surprise

What is trained:

"One of the FCC's is specified as the master FCC."

"Each FCC continues to calculate thrust, pitch and roll commands"
"The autothrottle adjusts the thrust levers with commands from the FCC."

"Two independent radio altimeters provide radio altitude to the respective FCC's."

"FCC A controls autopilot A and FCC B controls autopilot B"

(source: Boeing 737 FCOM and Computer Based Training for pilots)

What a crew could have concluded:

We select FCC B as Master

FCC B calculates thrust commands;
FCC B is giving the autothrottle its commands

FCC B has its own independent radio altimeter.
An inoperative RA on the left has no impact, as the left RA goes to FCC A

We fly this approach on autopilot B, which gets its input from FCC B.

What is actually going on:

FCC B controls autopilot B.
Autopilot B is following the glideslope

The autothrottle gets its height information directly from the left radio altimeter, independent of which FCC has been selected Master.

Flying the approach on FCC B does not protect you from a left RA anomaly.

(source: Boeing 737 technical documentation that pilots do not have access to)

complicated

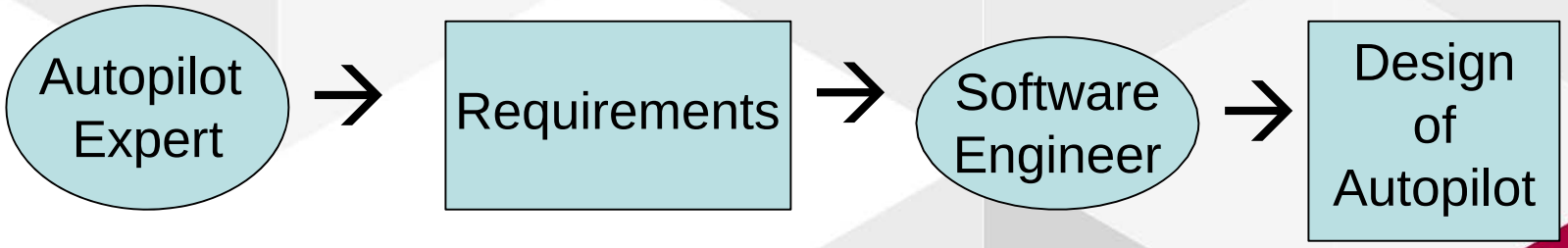
- fully describable
- closed system
- train to one best method
- determinate linear relationships
- closed-loop learning

complex

- not fully describable
- open to unforeseen interactions
- "best" method varies with context
- small change—large event
- open to societal demands

MODERN SYSTEMS

- Computers and new technology have led to complex designs. Complexity is the new challenge.
- Inability to conduct exhaustive testing of modern systems.
- Critical design errors become visible during operations: we test for what we designed (i.e. identified requirements), not what could happen (exhaustive list of requirements).



Introduction of new technology is a theory or hypothesis about how work is done

Hypothesis almost always based on componential, Newtonian view of work

complicated

- better results with substitution
- offloads human work
- focuses human attention
- less expertise needed
- fewer errors

complex

- new roles, transformed relationships
- new kinds of human work
- becomes additional partner
- new kinds of expertise
- new pathways to failure

system in design → system in operation

Complexity

Open systems

Locality principle

Optimized at edge of chaos

Path dependence

Non-linear interactions

Open systems

Fuzzy, permeable boundaries

Not clear what is in, what is out

Influences through local connections with outside

"Environment is folded in—everywhere"

(Paul Cilliers)

Locality principle

Each component largely ignorant of behavior of system as whole

Doesn't know full reverberations of local actions

> *"What you do controls almost nothing, but influences almost everything."* (Paul Cilliers)

Components respond with local inputs to local outputs

No component has full model of complex system

(either would have to be as complex as the system itself, or the system is actually not complex)

Complex system held together by local relationships

Griffith UNIVERSITY

Relationships

Complexity is feature of system, not components

Knowledge of each component local

No component possesses capacity to represent whole complex system

Behavior of system can not be reduced to components

Only characterized, temporarily, by multitude of ever-changing relationships between components (and their environment).

Optimized at edge of chaos

Operate at conditions far from equilibrium (i.e. if stop giving inputs …)

Dynamic stability: requires inputs all the time

Best performance extracted at edge of chaos (e.g. coffin corner)

Large changes possible as result of small inputs: as transgression into chaos is near

Path dependency

Past is co-responsible for behavior in present

Need to take history into account in explaining behavior

Non-linear interactions

Asymmetry between input/output

Small changes create large events

Feedback loops, amplifications, multipliers (creating more or less)

(e.g. melting polar ice: black water heats much faster)

the butterfly effect

change one thing. change everything.

It has been said that something as small as the flutter of a butterfly's wing can ultimately cause a typhoon halfway around the world.

- Chaos Theory

Studying failure, success

System behavior not reducable to parts

- Failure and success emerge from same relationships
- Model relationships, not component behavior

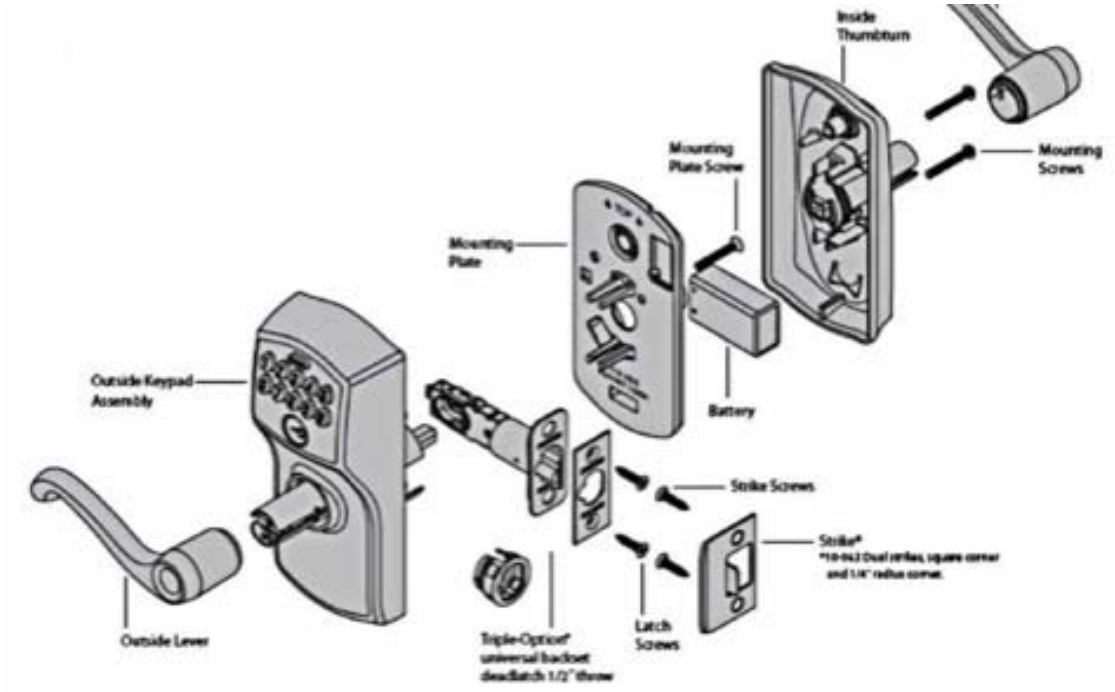
Locality principle: all postconditions of interventions not foreseeable

No definitive description of system

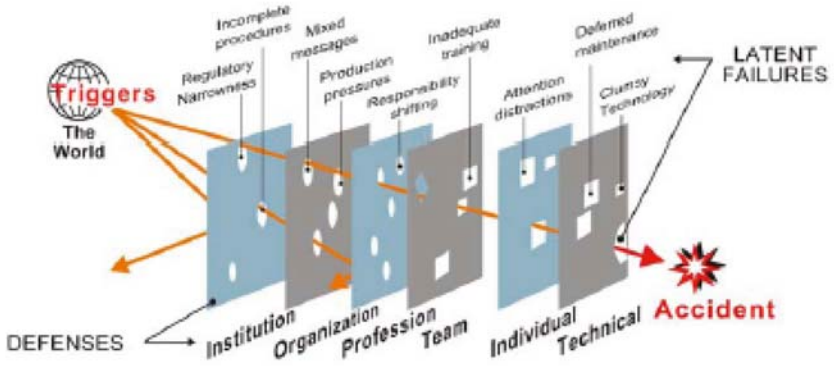
- Multiple legitimate accounts, not reducable to one another
- System post-accident not the same as pre
- All perspectives make analytic sacrifices

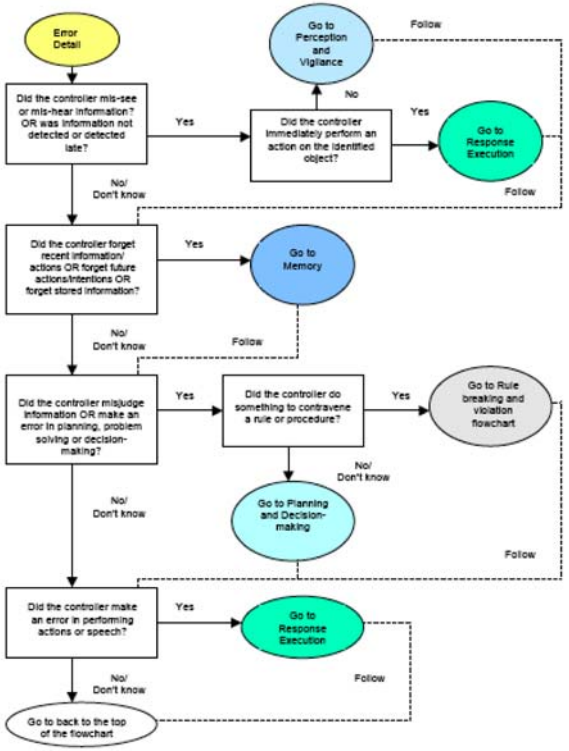
Machine metaphor

Reductionism: Functioning or malfunctioning of part can explain behavior of whole system



Complexity only apparent

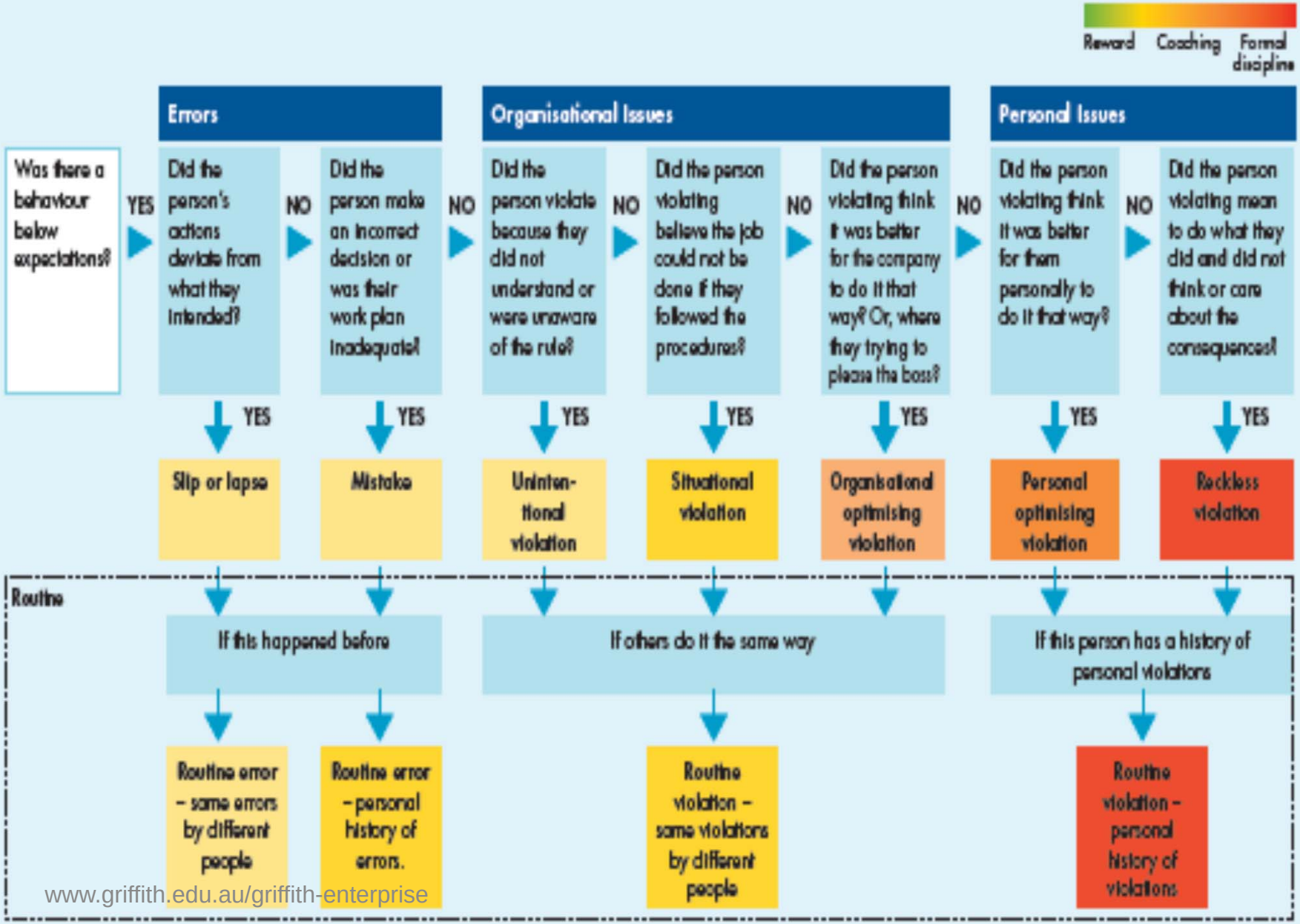




Decompose into smaller parts, becomes simple

sidneydekker.com

The Human Error and Violation Decision Flowchart




the aviation co.
ARE YOU A
LINK IN THE
ERROR CHAIN ?

Failure and success are the joint product of many related factors, all necessary and only jointly sufficient

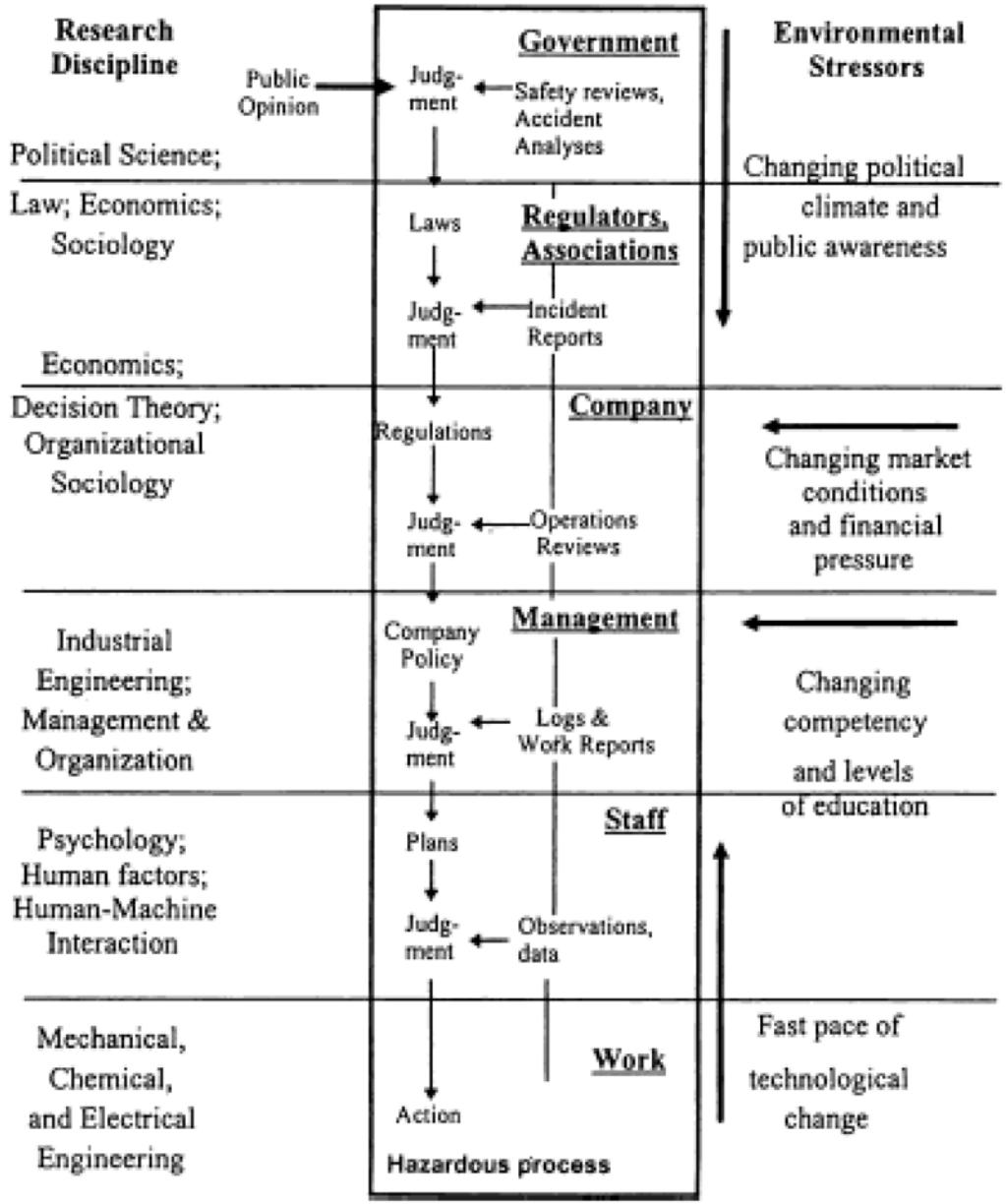
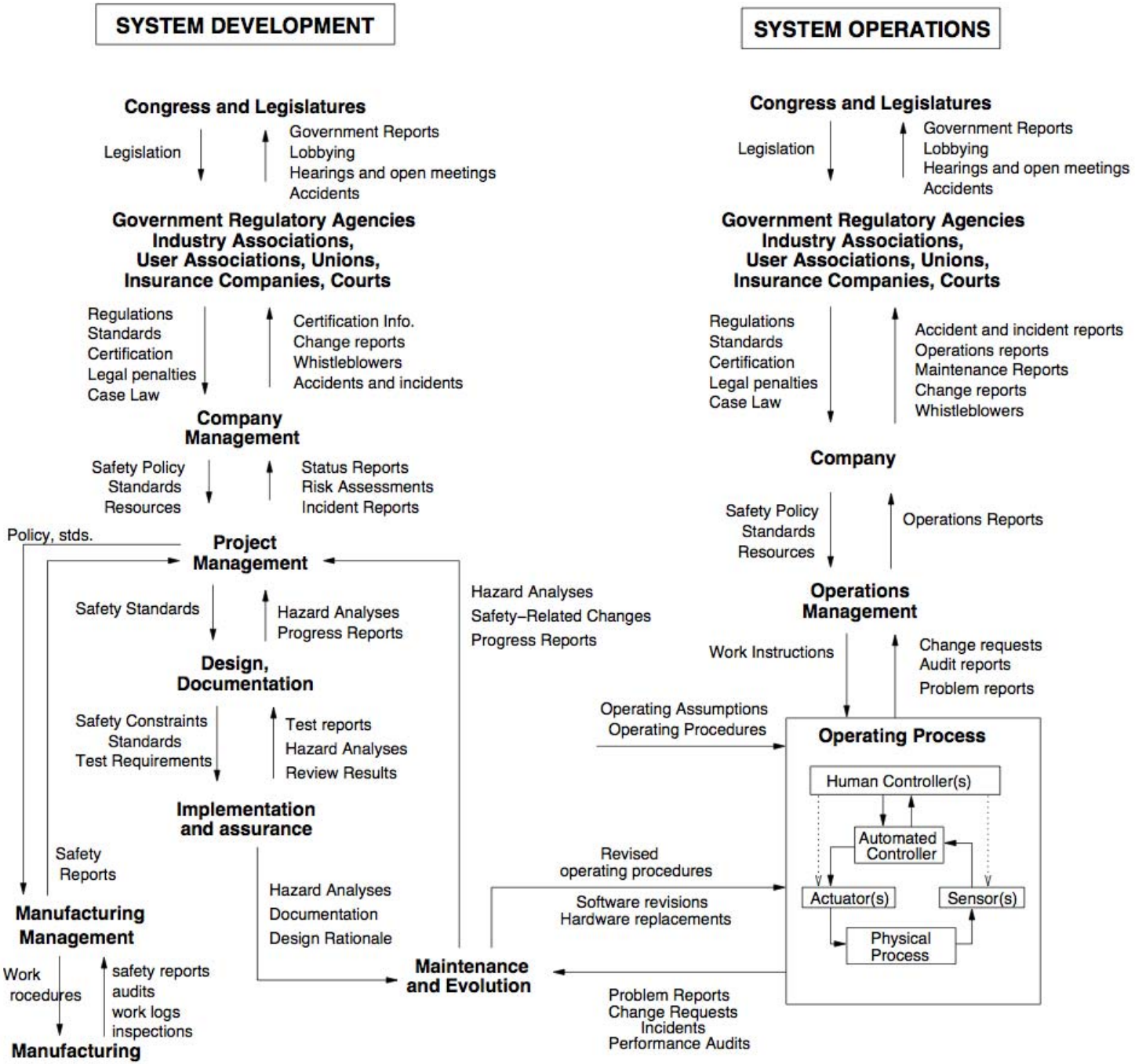


Fig. 2. Hierarchy of decision-making levels in risk management (Rasmussen, 1998).


SYSTEM DEVELOPMENT
SYSTEM OPERATIONS
Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Legal penalties
Case Law
Certification Info.
Change reports
Whistleblowers
Accidents and incidents
Company
Management
Safety Policy
Standards
Resources
Status Reports
Risk Assessments
Incident Reports
Policy, stds.
Project
Management
Safety Standards
Hazard Analyses
Progress Reports
Design,
Documentation
Safety Constraints
Standards
Test Requirements
Test reports
Hazard Analyses
Review Results
Implementation
and assurance
Safety
Reports
Manufacturing
Management
Work
rocedures
safety reports
audits
work logs
inspections
Manufacturing
Hazard Analyses
Documentation
Design Rationale
Maintenance
and Evolution
Hazard Analyses
Safety–Related Changes
Progress Reports
Revised
operating procedures
Software revisions
Hardware replacements
Problem Reports
Change Requests
Incidents
Performance Audits
Company
Safety Policy
Standards
Resources
Operations Reports
Operations
Management
Work Instructions
Change requests
Audit reports
Problem reports
Operating Assumptions
Operating Procedures
Operating Process
Human Controller(s)
Automated
Controller
Actuator(s)
Sensor(s)
Physical
Process

IN SUMMARY: A NEW SAFETY MODEL IS NEEDED

- Single (root) cause models, such as the “Domino” model:
  - Suggest that a triggering event sets a causal sequence in motion that leads to a harmful event (e.g., Underwood & Waterson, 2013).
- Epidemiological (multiple causes) models, such as the “Swiss cheese” model (Reason, 1990):
  - Differentiates between active failures (i.e. actions and inactions) and latent conditions (i.e. individual, interpersonal, environmental, supervisory and organisational factors present before the accident)
  - The use of defences to counteract for possible failures is common across those types of models, such as the bow-tie (e.g., Boishu, 2014), Threat & Error Management (e.g., Maurino, 2005) and Tripod (e.g., Kjellen, 2000).
- Systemic models such as STAMP (Leveson, 2011), FRAM (Hollnagel, 2010) and Accimap (e.g., Rasmussen,1997) that focus on component interactions rather than single component failures in a dynamic, variable and interactive operational context.

Steffen Kaspers, Nektarios Karanikas, Alfred Roelen, Selma Piric, Robert J. de Boer (2016): Review of Existing Aviation Safety Metrics, Aviation Academy, Amsterdam

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

INTRODUCING STAMP

www.international.hva.nl

SYSTEMS THEORY (1)

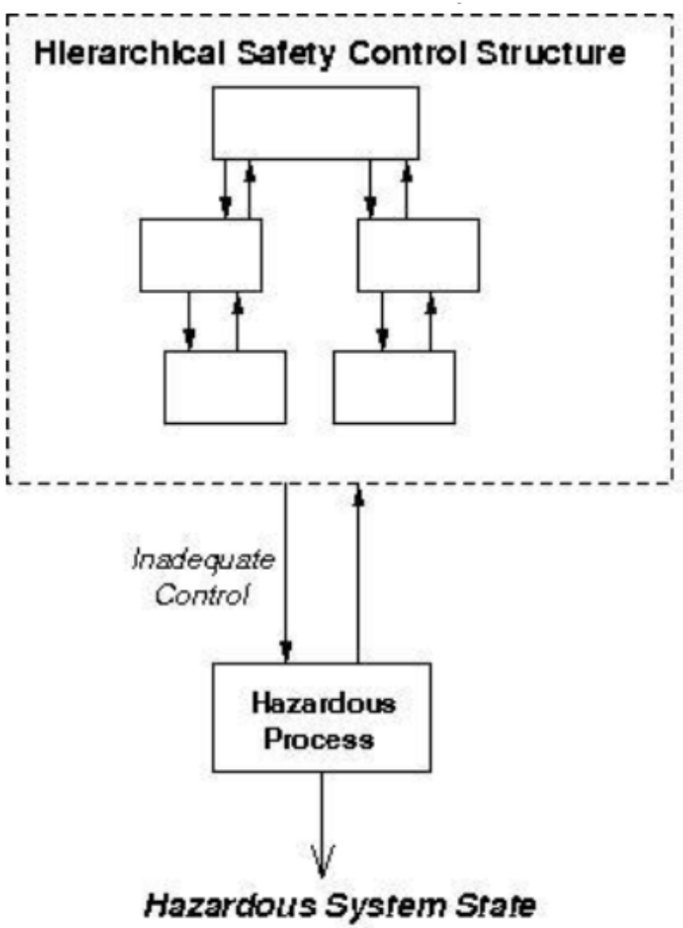
- Developed for systems that are
  - Too complex for complete analysis
    - Separation into (interacting) subsystems distorts the results
    - The most important properties are emergent
  - Too organized for statistics
    - Too much underlying structure that distorts the statistics
    - New technology and designs have no historical information
- First used on ICBM systems of 1950s/1960s
- Basis for system engineering and system safety

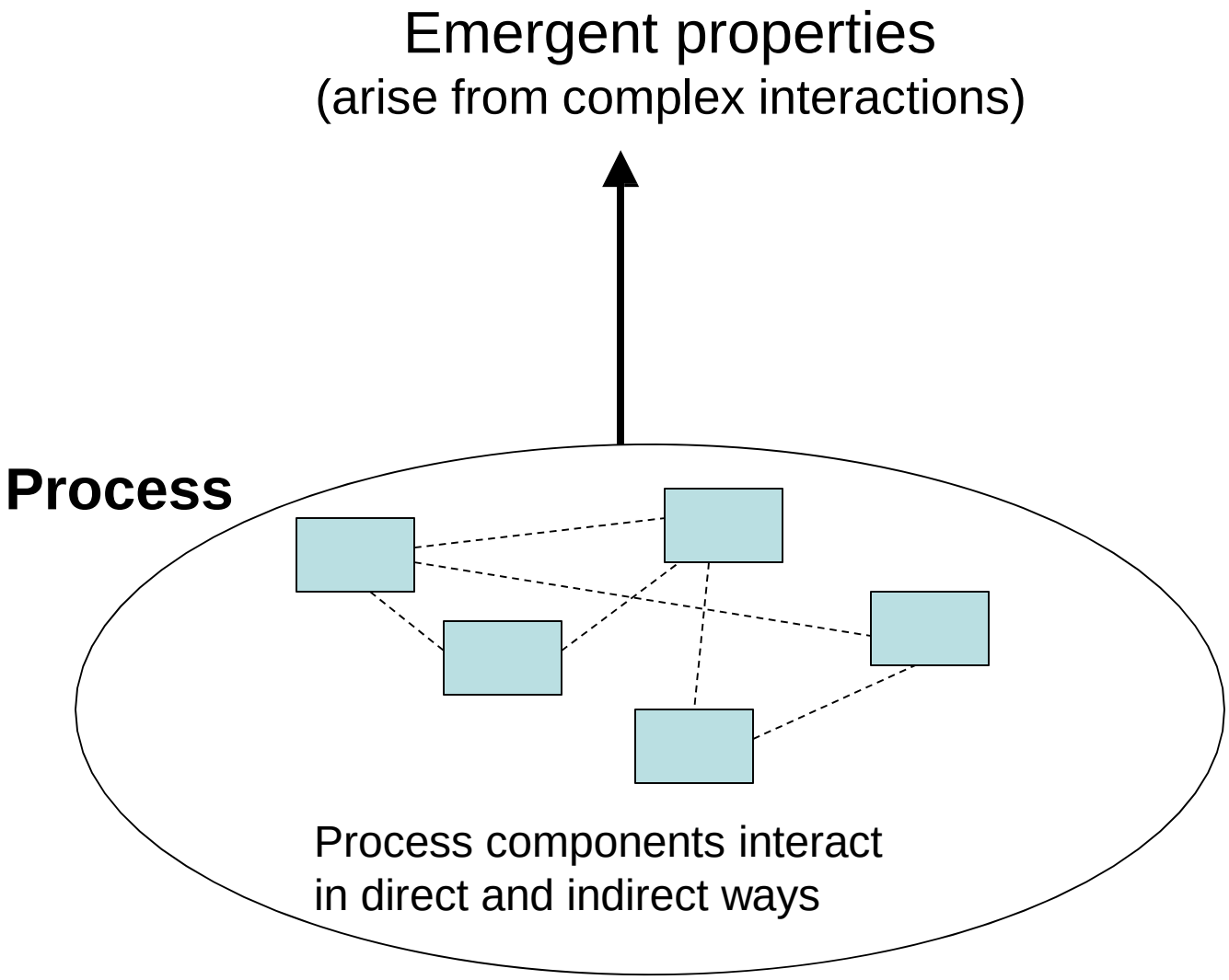
SYSTEMS THEORY (2)

- Focuses on systems taken as a whole, not on parts taken separately
- Emergent properties
  - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects
- “The whole is greater than the sum of the parts”
  - These properties arise from relationships among the parts of the system
- How they interact and fit together

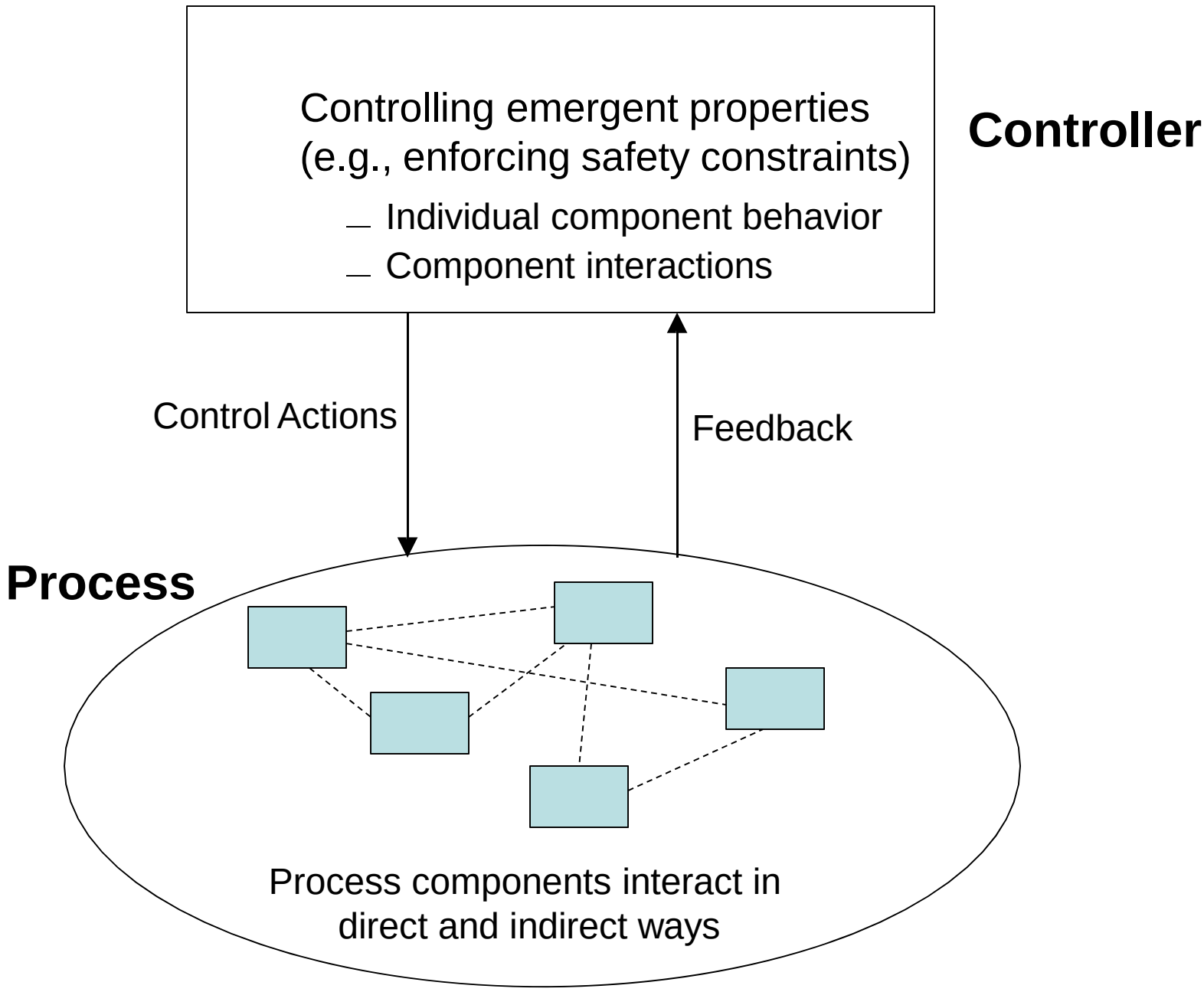
BASICS OF SYSTEMS THEORY

- The whole is not the sum of its parts. It is greater than that.
- Considers relations and interactions among system components.
- Systems are viewed as hierarchy of organizational levels.
- The levels have properties that are not visible in the properties of individual components.
- Each hierarchical level of a system controls the relationships between the components at the next lower level.

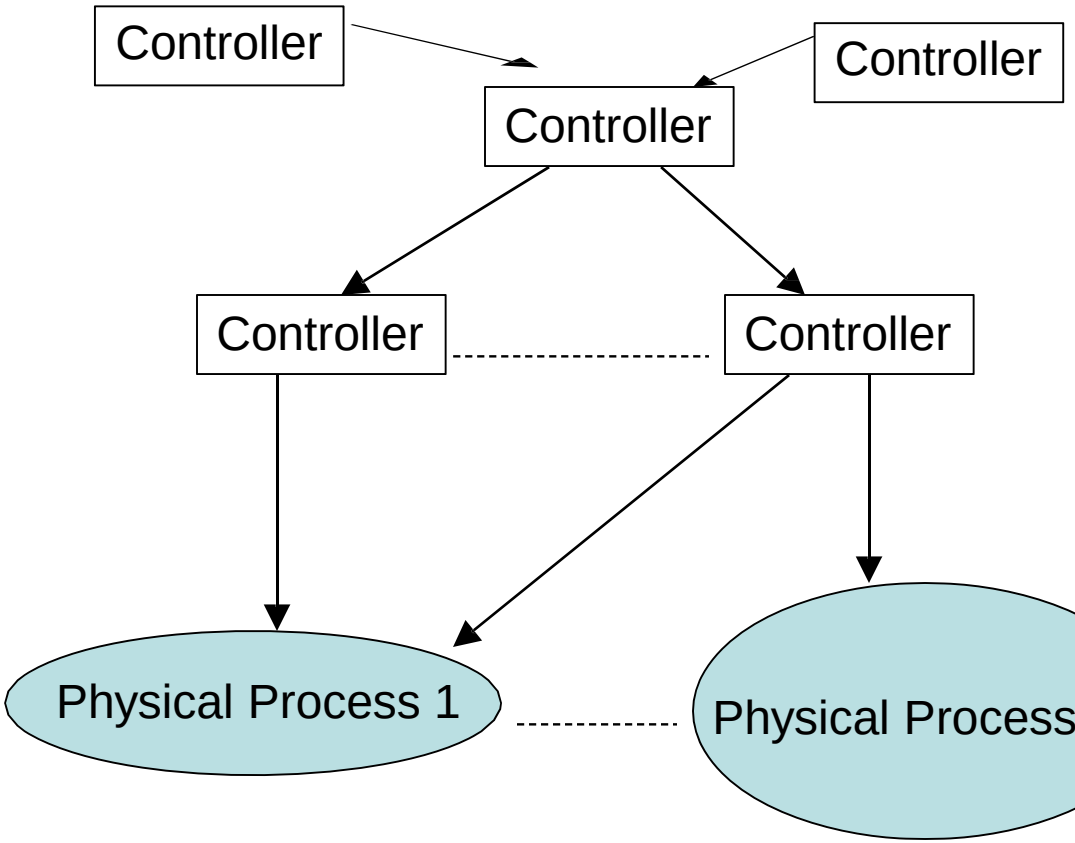




Safety is an emergent property


Controlling emergent properties
(e.g., enforcing safety constraints)
Individual component behavior
Component interactions
Controller
Control Actions
Feedback
Process
Process components interact in
direct and indirect ways

multiple controllers, processes, and levels of control

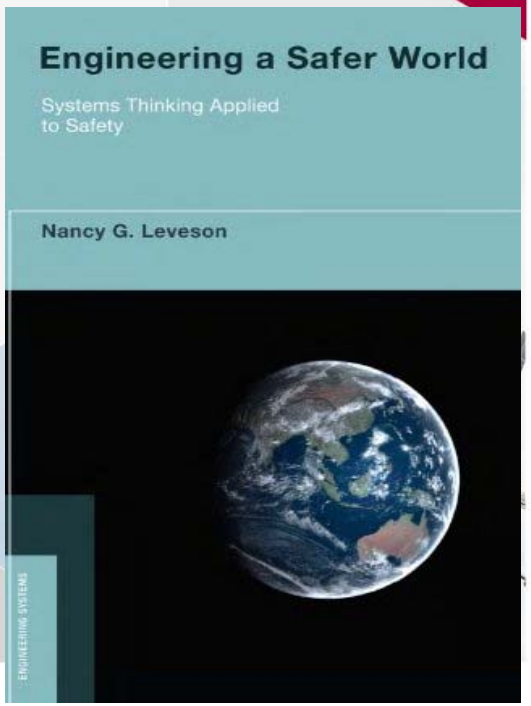


Each controller enforces specific constraints, which together enforce the system level constraints (emergent properties)

(with various types of communication between them)

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

A SYSTEMIC APPROACH TO SAFETY: THE STAMP MODEL



www.international.hva.nl

STAMP (SYSTEM-THEORETIC ACCIDENT MODEL AND PROCESSES)

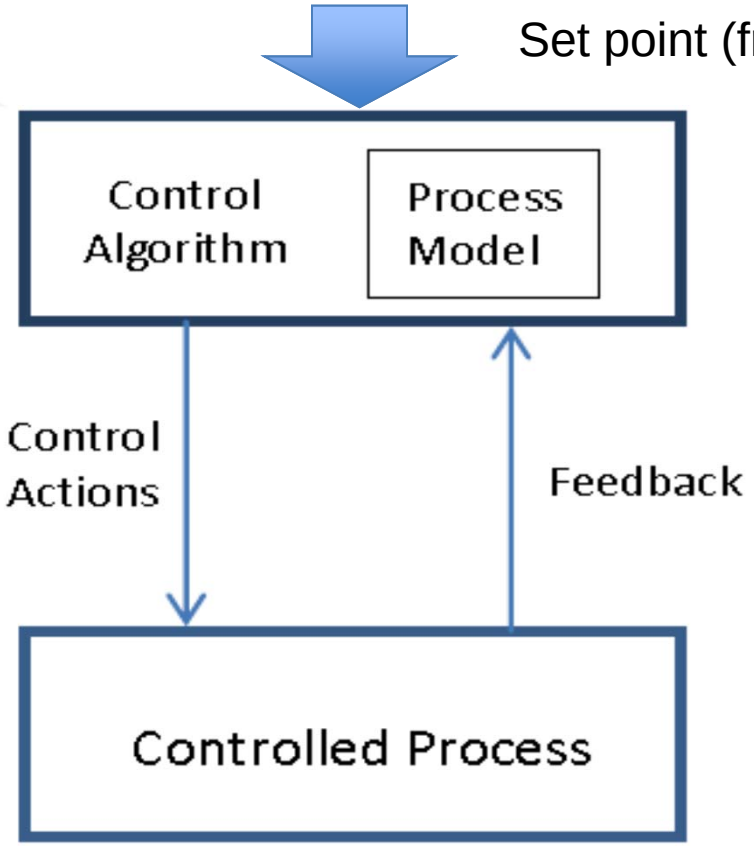
- Defines safety as a control problem (vs. failure problem)
- Applies to very complex systems
- Includes software, humans, new technology
- Based on systems theory and systems engineering
- Expands the traditional model of the accident causation (cause of losses)
  - Not just a chain of directly related failure events
  - Losses are complex processes

STAMP: SAFETY AS A DYNAMIC CONTROL PROBLEM

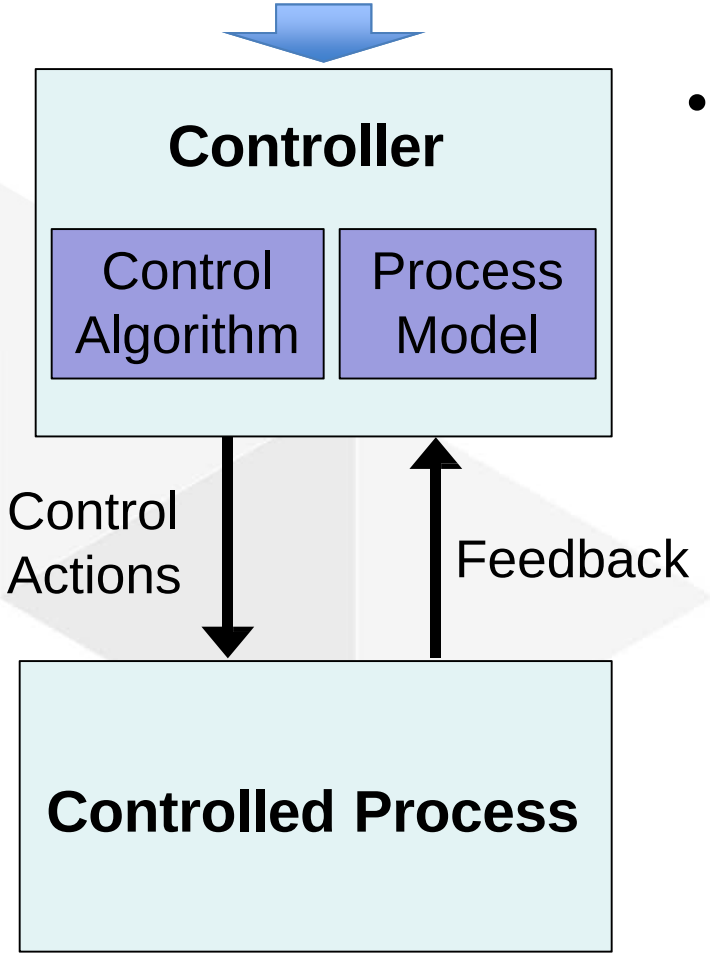
- Events result from lack of enforcement of safety constraints in system design and operations.
- Goal is to control the behavior of the components and systems as a whole to ensure safety constraints are enforced in the operating system
- A change in emphasis:
  - “prevent failures at system level”

“enforce safety/security constraints on system behavior”

THE CORE OF STAMP: CONTROL LOOPS

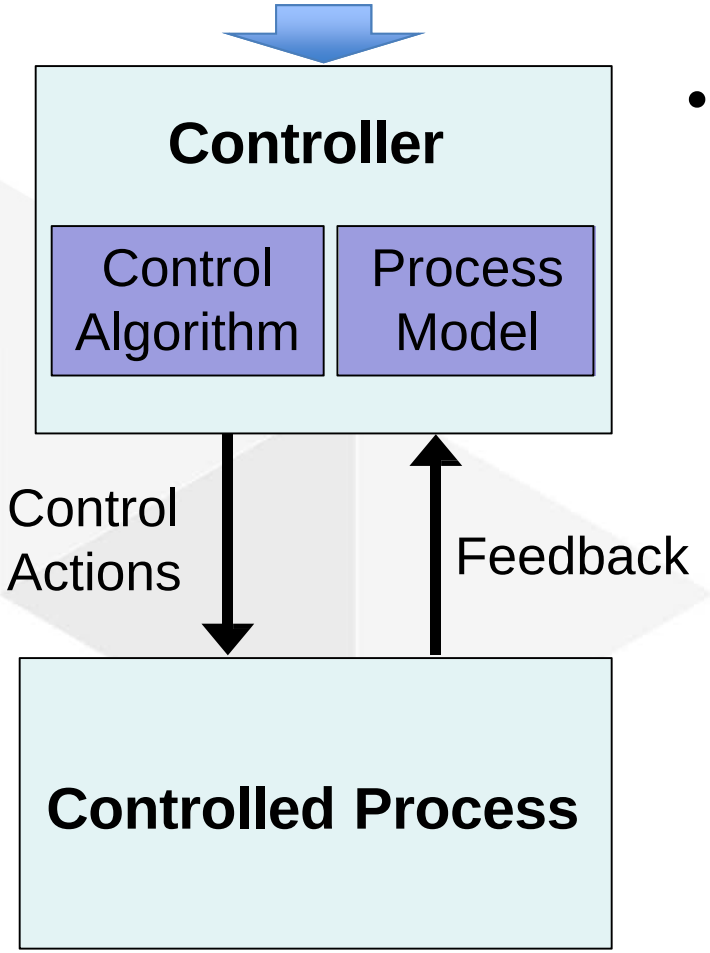


COMPONENTS OF THE CONTROL STRUCTURE



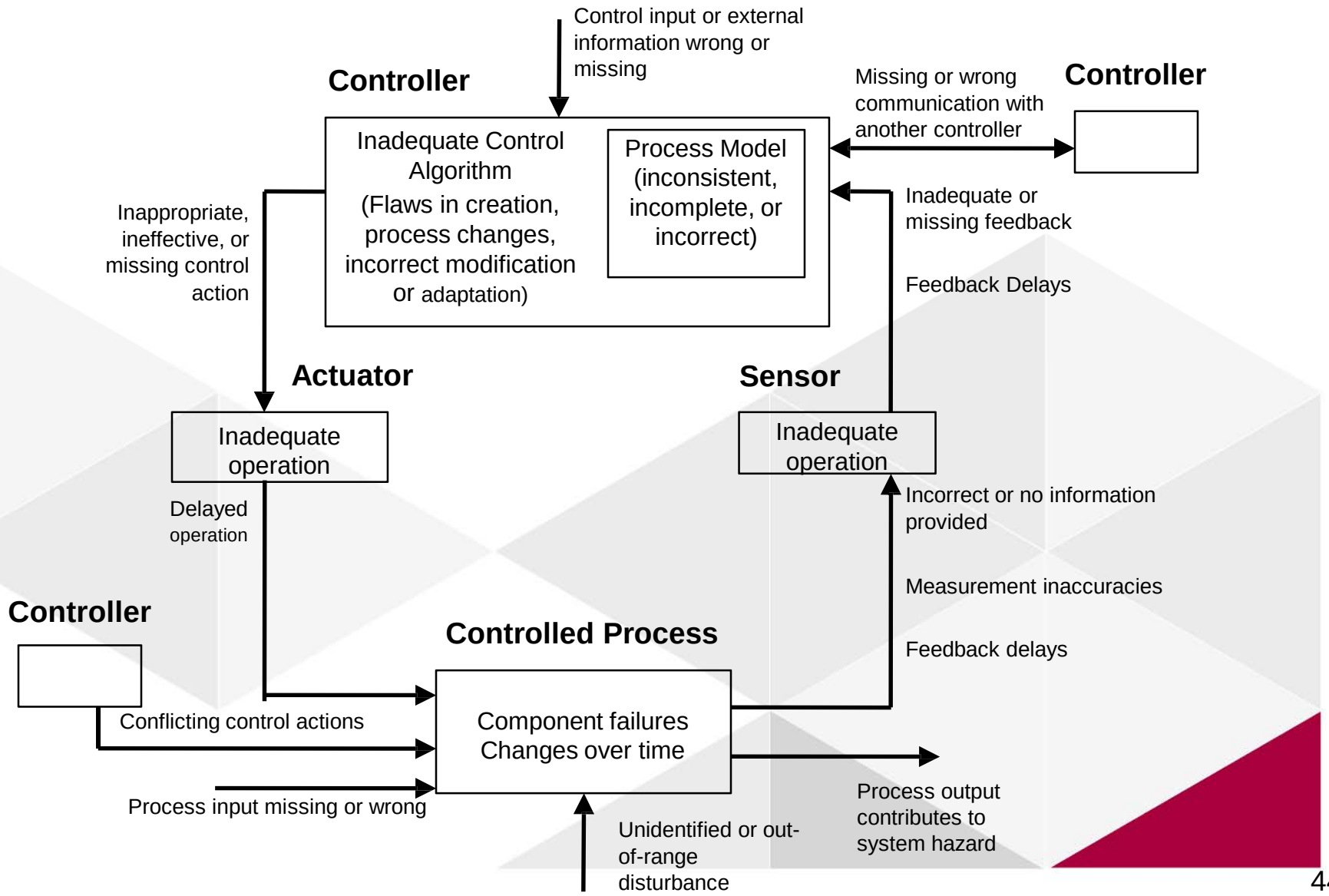
- Controllers (humans & computers) aim to keep the controlled process at target (set by superior controller) by:
  - **Process model** and feedback to determine process state
  - **Control algorithm** devises the appropriate control actions

COMPONENTS OF THE CONTROL STRUCTURE



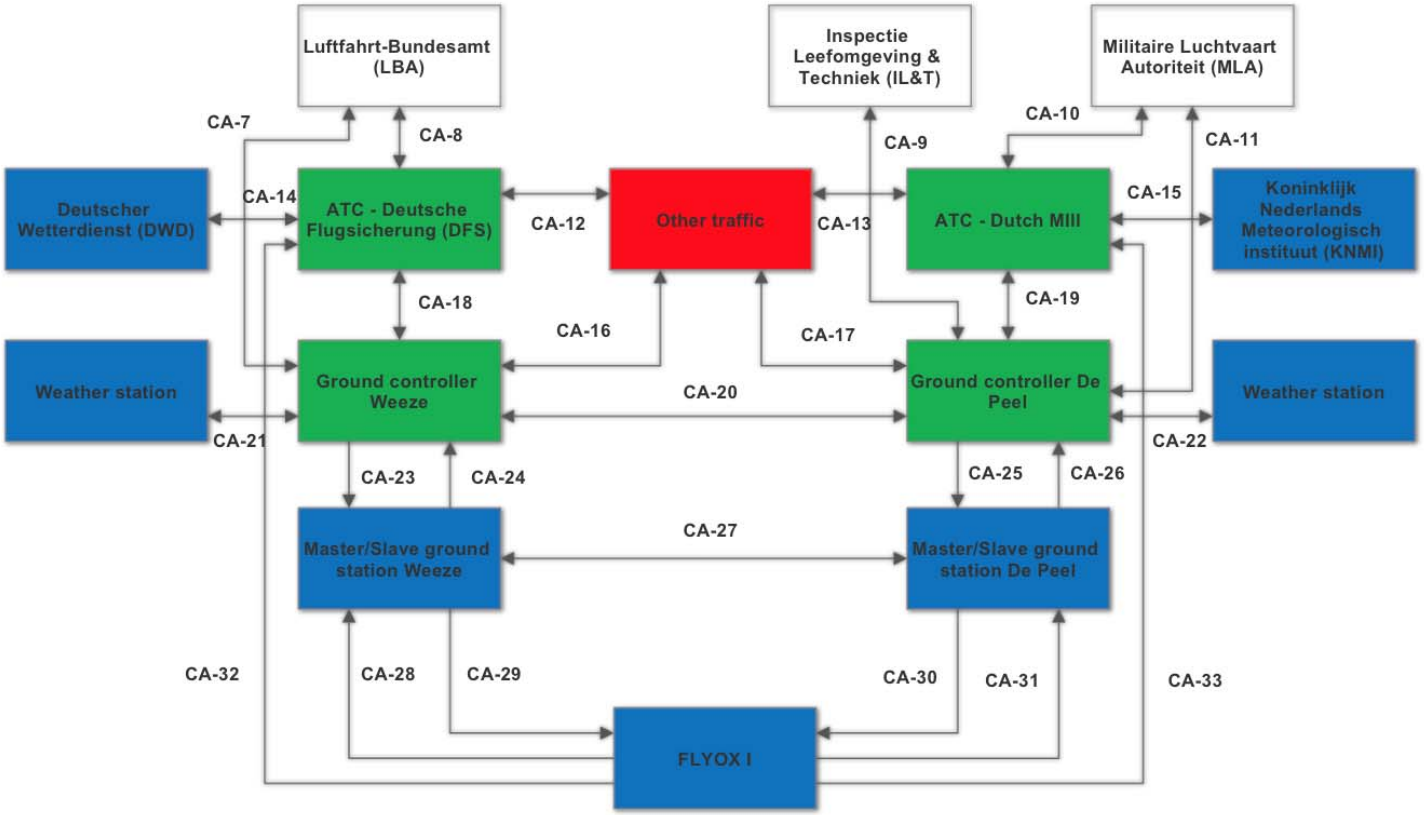
- Accidents might occur when, for example:
  - The control algorithm is outdated, inappropriate etc.
  - The process model is incorrect.
  - Control actions and feedback are (not) provided as designed.
  - The uncontrolled hazards are not monitored.
  - The assumptions made during design and operation become invalid.
  - The reliability of simple sub-systems and components is not achieved.

POSSIBLE FLAWS IN THE CONTROL LOOP



Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

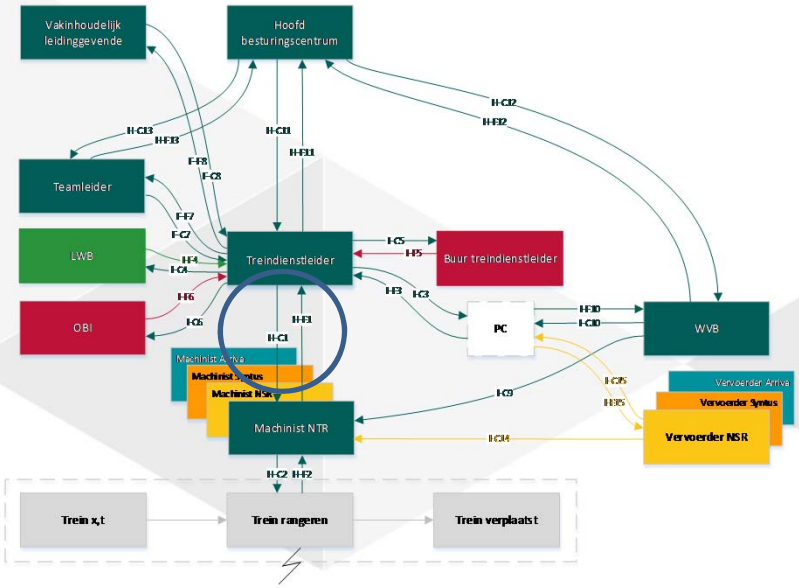
THE STAMP METHODOLOGY IS USED TO MAP ALL INTERACTIONS AND IDENTIFY FLAWS



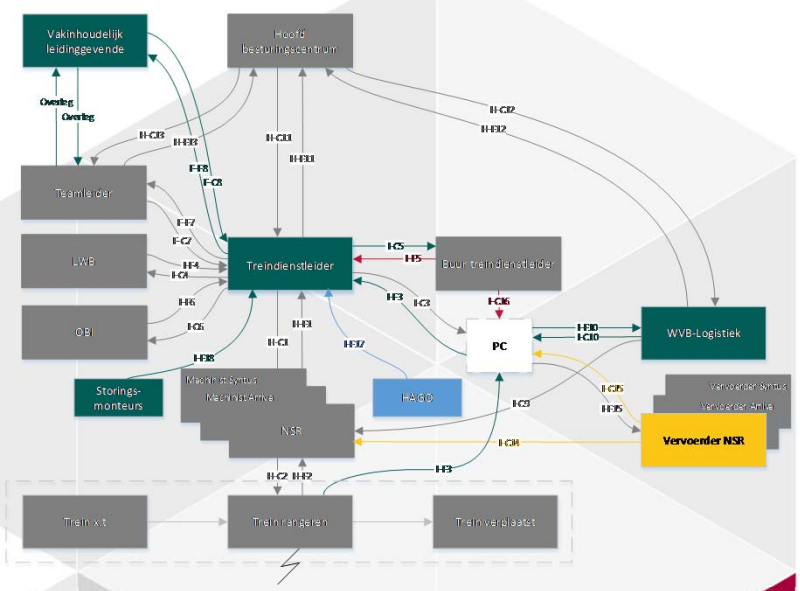
Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

WORK-AS-DONE VERSUS WORK-AS-IMAGINED

Work-as-imagined

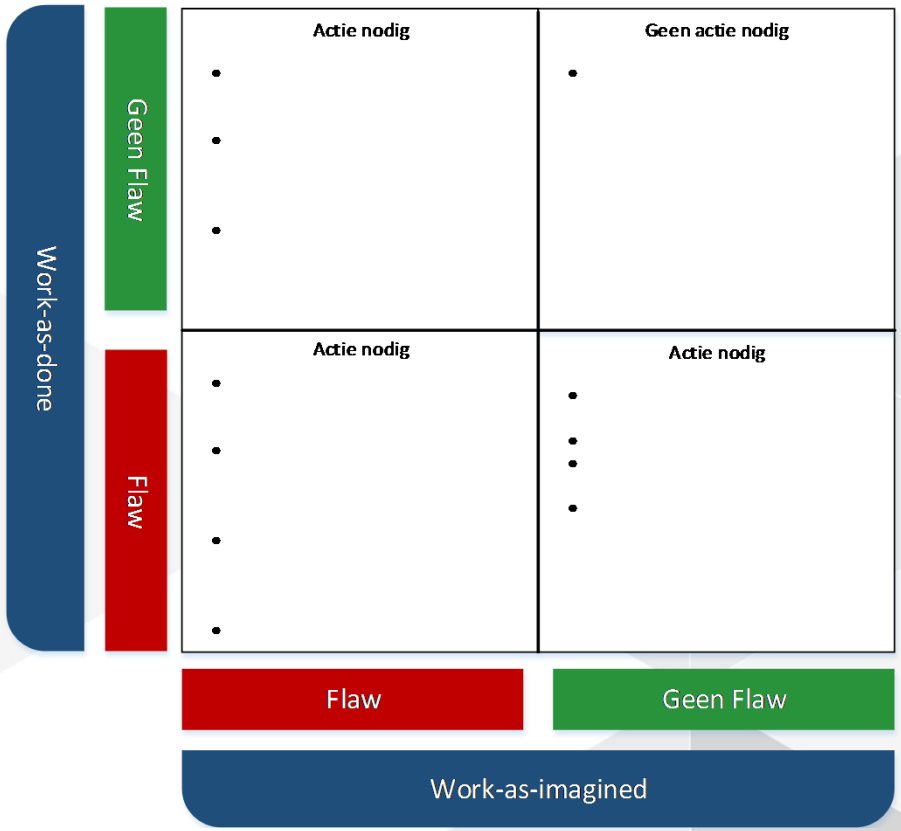


Work-as-done location Zwolle



Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

FLAWS BOTH IN WAD AND WAI



Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

CONDUCTING A STAMP ANALYSIS

www.international.hva.nl

www.griffith.edu.au/griffith-enterprise

THE SIX STEPS OF A STAMP ANALYSIS

1. Establish the system engineering foundation for the analysis and for the system development.
2. Create the hierarchical control structure (HCS).
3. Define control actions.
4. Identify potentially unsafe control actions.
5. Use the identified unsafe control actions to create safety requirements and constraints.
6. Determine how each potentially hazardous control action could occur to enable mitigation actions.

(Leveson, An STPA Primer, 2013)

1. ESTABLISH THE SYSTEM ENGINEERING FOUNDATION

- Identify the system objective. In the objective(s) of the system is defined how the system is expected to behave. This will include the safety objectives and criteria along with high-level requirements and safety design constraints. When a system is under design, the design criteria can also be stated in the system objectives.
- Identify the system accidents. An accident is defined as “an undesired and unplanned event that result in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc.” (Leveson et al., 2013).
- Identify the system hazards. A hazard is defined as “a system state or set of conditions that together with a worst-case set of environmental conditions, will lead to an accident (loss).” (Leveson et al., 2013).
- Identify the system safety constrains/requirements The safety constrains/requirements are a set of rules that under no circumstances can be broken or violated. They guard the safety of the system and ensure that the defined objectives are met

(Leveson, An STPA Primer, 2013)

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

IMAGINE AN UNMANNED CARGO AIRCRAFT

CONCEPT OF OPERATIONS: UNMANNED CARGO AIRCRAFT

- Without any people on board ➔ no pressurization
- Maximum payload will be 10,000 kg
- Range at least 3,000 km, possibly 6,000 km
- Propulsion:
  - conventional concepts such as a turbo-prop engine or a turbojet engine.
  - Distributed propulsion: many small, electric-driven propellers on the leading edge of the wing.
- Flies a pre-programmed route autonomously
- People monitoring the flights
  - 1 UCA per remote pilot during take-off and landing
  - about 10 UCA per remote pilot during cruise

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

3000 KM RANGE FROM AMSTERDAM

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

6000 KM RANGE FROM AMSTERDAM

WHAT ARE FOR AN UNMANNED CARGO AIRCRAFT FLIGHT…

- … the system objectives?
- … the system accidents (ways the objectives are not met)?
- … the system hazards (worst cases possibly leading to an accident)?
- … the system safety constrains/requirements (avoiding hazards)?

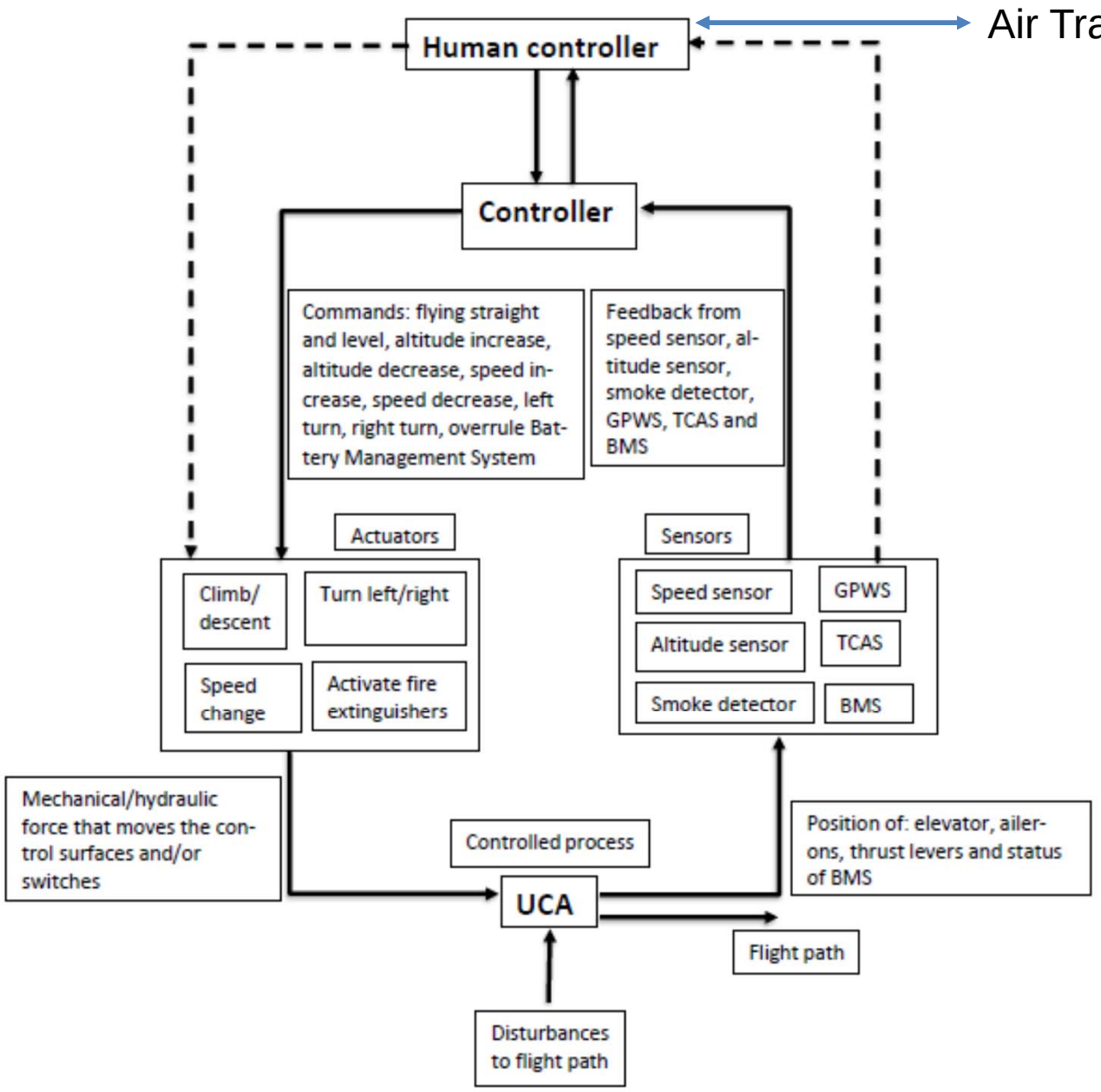
Accidents	Description	Related ICAO occurrence categories
UCA collides with other aircraft	The UCA gets so close to another aircraft, manned or unmanned, that a collision cannot be avoided anymore.	MAC, FUEL, ATM, LOC-I, MED, NAV, SFC-NP, SFC-PP
UCA collides with ground/objects on the ground during flight	A collision with the ground cannot be avoided anymore.	CFIT, FUEL, ATM, LOC-I, MED, NAV, SFC-NP, SFC-PP
UCA crashes during take-off or landing	During the take-off or landing, control over the aircraft is lost or the UCA approaches stall speed, causing the UCA to crash during take-off or landing.	ARC, CTOL, RE, RI, USOS, FUEL, LOC-I, LOC-G, MED, SFC-NP, SFC-PP
Disintegration/major damage of UCA during mission	The UCA is damaged so that the mission cannot be continued or control is lost during the mission.	BIRD, EXTL, F-NI, ICE, TURB, WSTRW, GCOL, RAMP,
Mission (delivering cargo) fails while structural integrity of UCA is maintained	The mission fails if the cargo is not delivered correctly at the required destination and at the required time, even though the structural integrity of the UCA is being maintained.	AMAN, TURB, WSTRW, ATM, NAV

Table 5.1 Accidents

Hazards	Description	Related accidents
UCA violates separation minima in relation to other aircraft in controlled flight	If UCA violates separation minima in relation to other aircraft, this could relate into colliding with that aircraft, manned or unmanned.	1, 5
UCA violates separation minima in relation to the ground	If the UCA fly too close to the ground, this could result in colliding with the ground, even though control is not lost (CFIT).	2, 5
UCA control is lost	If UCA control is lost, neither the automated controller nor the human controller can do anything about it.	1, 2, 3
UCA approaches stall speed	If the UCA approaches the stall speed, this often means that some of the altitude will be lost as well.	2, 3
Short circuit within electrical circuit	Short circuit in electrical circuit causes heat in the batteries, which on its turn could cause the batteries to catch fire.	4, 5
Overcharging of Li-ion batteries	Overcharging of batteries causes heat and the heat could cause fire.	4, 5
Take-off or land without permission	The UCA needs permission in order to take-off or land.	2, 3
Cargo is damaged	Cargo can be damaged in different ways. One can think of water damage from the fire extinguishers, fire, or from the self-destruct function. The damaged cargo could also have consequences for the rest of the UCA, when for example dangerous goods are being transported.	4, 5

2. CREATE THE HIERARCHICAL CONTROL STRUCTURE (HCS) & 3. CONTROL ACTIONS

- Go on, do it…


Air Traffic Control
Human controller
Controller
Commands: flying straight and level, altitude increase, altitude decrease, speed increase, speed decrease, left turn, right turn, overrule Battery Management System
Feedback from speed sensor, altitude sensor, smoke detector, GPWS, TCAS and BMS
Actuators
Climb/ descent
Turn left/right
Speed change
Activate fire extinguishers
Sensors
Speed sensor
GPWS
Altitude sensor
TCAS
Smoke detector
BMS
Mechanical/hydraulic force that moves the control surfaces and/or switches
Controlled process
UCA
Position of: elevator, ailerons, thrust levers and status of BMS
Flight path
Disturbances to flight path

Control actions	Description
1. Control autopilot and FMS	The human controller can set up the autopilot and FMS for take-off and landing before the flight by entering the departure runway, SID, route waypoints, altitudes, speeds, STAR, arrival runway, and parking position.
1. Flight path control	The automated controller and human controller control the flight path of the UCA. The human controller monitors the variables during the flight that he/she has put in before take-off. The automated controller makes sure that the entered variables, the process model, is met during the flight. The automated controller can also make corrections in order to keep the UCA within the tunnel in the sky.
1. Activate fire extinguishers	The automated controller and the human controller have the ability to activate the fire extinguisher when there is a fire.
1. ATC control	The human controller is responsible for keeping contact with ATC. He/she is responsible for responding to ATC, complying with ATC instructions and for requesting possible diversions, for example for weather.

4. IDENTIFY POTENTIALLY UNSAFE CONTROL ACTIONS

- Four scenarios:
  - When a control action is not provided it causes a hazard
  - When a control action is provided it causes a hazard
  - When a control action is provided at the wrong time or order it causes a hazard
  - When a control action is stopped too soon or applied too long it causes a hazard

(Leveson, An STPA Primer, 2013)

Control action	Not provided (*)	Provided incorrectly (*)	Too early, too late or wrong order (*)	Stopping too soon/applying too long (*)
1. Control autopilot and FMS	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3) T/O or land without permission (7)	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3) T/O or land without permission (7)	Not hazardous	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3) T/O or land without permission (7) Not hazardous
2. Flight path control	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3)	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3)	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3)	Violate separation minima (1, 2) Approach stall speed (4) Control loss (3)
3. Activate fire extinguishers	Cargo damage (8) Control loss (3)	Cargo damage (8)	Cargo damage (8) Cargo damage (8) Control loss (3) Not hazardous	Cargo damage (8)
4. ATC control	Violate separation minima (1, 2) T/O or land without permission (7)	Violate separation minima (1, 2) T/O or land without permission (7)	Not hazardous Violate separation minima (1, 2) Not hazardous	Violate separation minima (1, 2)

5. USE UCA TO CREATE SAFETY REQUIREMENTS & 6. TO ENABLE MITIGATION

Scenario	Associated Causal Factors (*)	Rationale/Notes
Activate fire extinguishers – Too early, too late or wrong order	Output of controlled process contributes to system hazard (1)	The output of the controlled process contributes to the system hazard that cargo is damaged. This is acceptable.
	Sensor measurement delay (2)	The activation of the fire extinguishers could be started too late because of sensor measurement delay.
	Sensor to controller signal inadequate, missing, or delayed: Communication bus error (4)	The signal from the sensor to the automated controller could be delayed because of a communication bus error, causing the fire extinguishers to be activated too late.
	Controller to actuator signal ineffective, missing, or delayed: Communication bus error (6)	The signal between the automated controller and the fire extinguisher activation actuator could be delayed because of communication bus error.
	Actuation delivered incorrectly or inadequately: Actuation delayed (8)	The late actuation of the fire extinguishers could happen when the actuation of the fire extinguishers is performed incorrectly. This means that the actuation is delayed.

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

CONCLUSIONS

www.international.hva.nl

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

OUR CURRENT TOOLS ARE ALL 40-65 YEARS OLD BUT OUR TECHNOLOGY IS VERY DIFFERENT TODAY

1940 1950 1960 1970 1980 1990 2000 2010 2020

FMEA

FTA HAZOP

ETA

Bow Tie
(CCA) FTA
+ ETA

- Introduction of computer control
- Exponential increases in complexity
- Lots of new technology

STANDARD HAZARD ANALYSIS METHODS DO NOT HANDLE:

- Component interaction accidents
- Systemic factors (affecting all components and barriers)
- Software and software requirements errors
- Human behavior (in a non-superficial way)
- System design errors
- Indirect or non-linear interactions and complexity
- Migration of systems toward greater risk over time (e.g., in search for greater efficiency and productivity)

WHAT IS STAMP ABOUT?

- It addresses interconnections of system components (hardware, humans, software etc.).
- It provides structured guidance for hazard identification at the first stages of the design / analysis (STPA method).
- It combines and extends concepts and advantages of traditional hazard analysis methods.
- It still relies on reliability theory and human performance when reaching down to the component level.
- It leads to identification of more hazards than the current methods do.
- It depends on experience and expertise of the analyst.

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

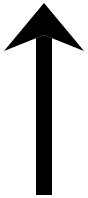
System Engineering (e.g., Specification, Safety-Guided Design, Design Principles)

Risk Management

Operations

Management Principles/ Organizational Design

Regulation



Tools

Accident/Event Analysis **CAST**

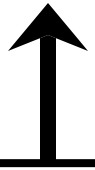
Hazard Analysis **STPA**

Early Concept Analysis **STECA**

Organizational/Cultural Risk Analysis

Identifying Leading Indicators

Security Analysis **STPA-Sec**

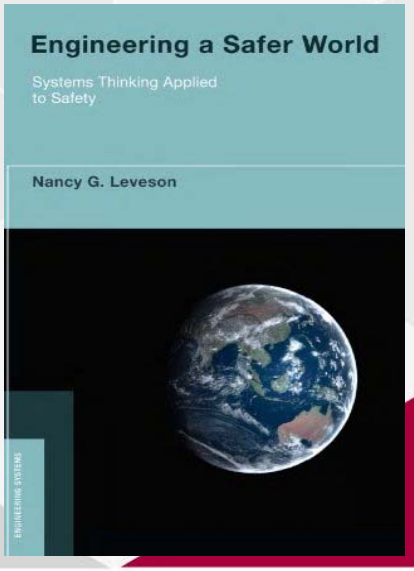


STAMP: Theoretical Causality Model

Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

FOR MORE INFORMATION

- STPA Primer: Written for industry to provide guidance in learning STPA
- Website: mit.edu/psas: Previous MIT STAMP workshop presentations
- Book: “Engineering a Safer World” by Nancy Leveson
- Sunnyday.mit.edu: Academic STAMP papers, examples



Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

THANK YOU FOR YOUR ATTENTION

Professor of Aviation Engineering: Robert J. de Boer,
rj.de.boer@hva.nl

Website: http://www.hva.nl/aviation

CREATING TOMORROW