A Different Look at the Entire Accident / Disaster Cycle affecting Safety of Complex Sociotechnical Systems by Using STAMP

Daniel Hartmann, PhD

Management & Safety Engineering Unit,

Ben-Gurion University, Israel

Outline

- Motivation
- Harmonizing...
- Accident / Disaster Cycle
- Some thoughts about Sociotechnical Systems,

  Accident / Disaster Cycle & STAMP

Radiation Accident in Israel: Official & CAST Investigations Results

S-T System Levels	Loop Number	Official Results	CAST Results
State – Regulation	1, 2, 3	0	3
State – Professional Regulation	4, 5, 6, 7, 8, 9	3	6
External Institutions	10, 11, 12	0	5
Management & Operation	13	2	3
Physical Level		2	4
Total Results		7	21
Total in %		100%	300%

Anacortes Accident: CSB & CAST Investigations Results

S-T System Levels	Loop Number	CSB Results	CAST Results
Federal – Regulation	1	6	8
State – Regulation	2, 3, 4, 5	5	8
External Institutions	6, 7	0	1
External Experts	8, 9	2	5
Management & Operation	10, 11	10	14
Physical Level		9	14
Total Results		32	50
Total in %		100%	156%

A very crude and bold Assumption

New Socio-technological Systems	Old, well established Socio-technological Systems
< 0.1 %	*>99.9%*
STPA needed, but…	STAMP not wanted as long as…

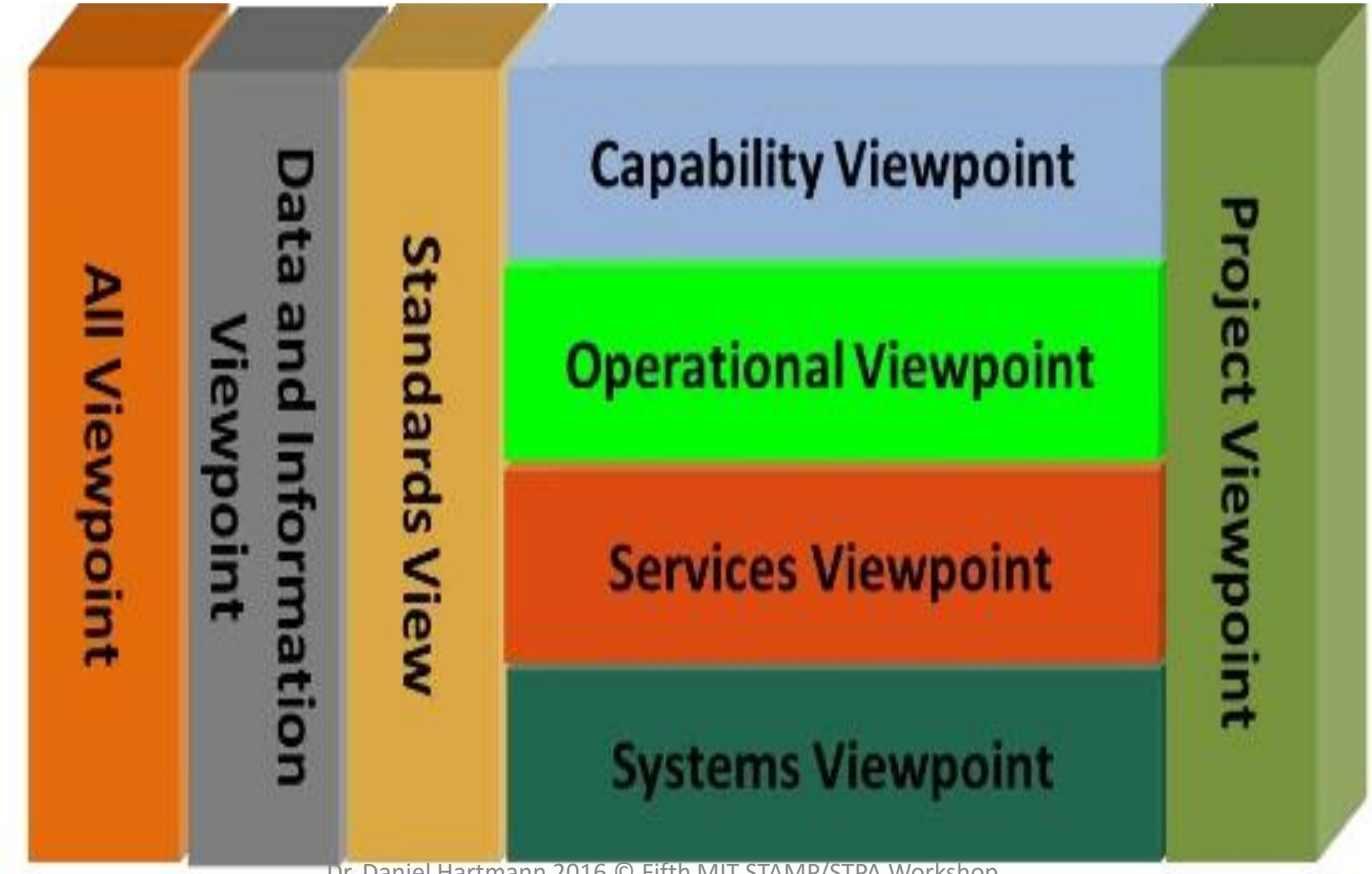
Outline

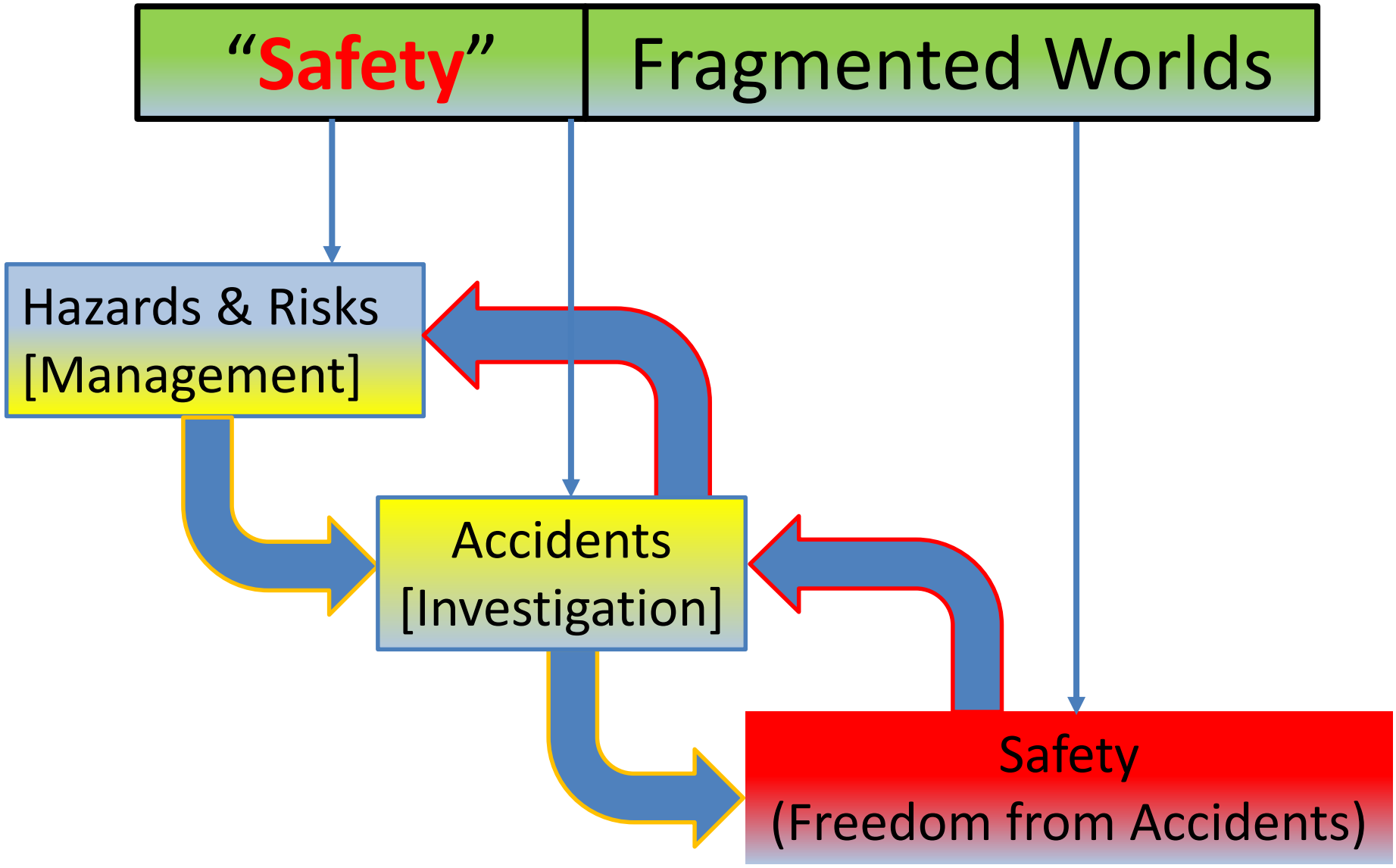
- Motivation
- Harmonizing...
- Accident / Disaster Cycle
- Some thoughts about Sociotechnical Systems,

  Accident / Disaster Cycle & STAMP

A Normal Variability of Viewpoints…

Systems Engineering & DoDAF Viewpoint Structure



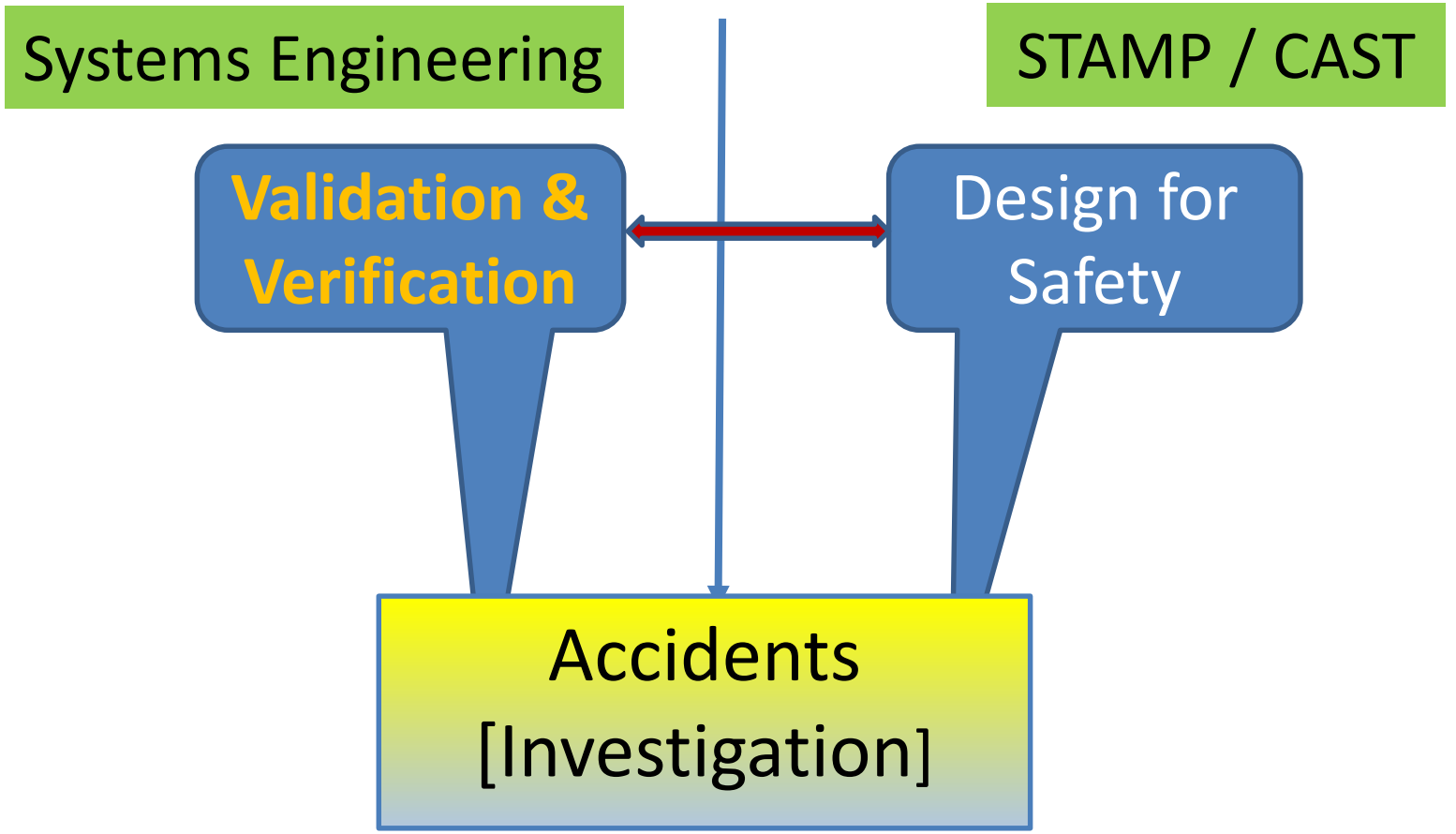


Definitions of Accident

- An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).
- **Loss [event] that is unacceptable to the stakeholders.**

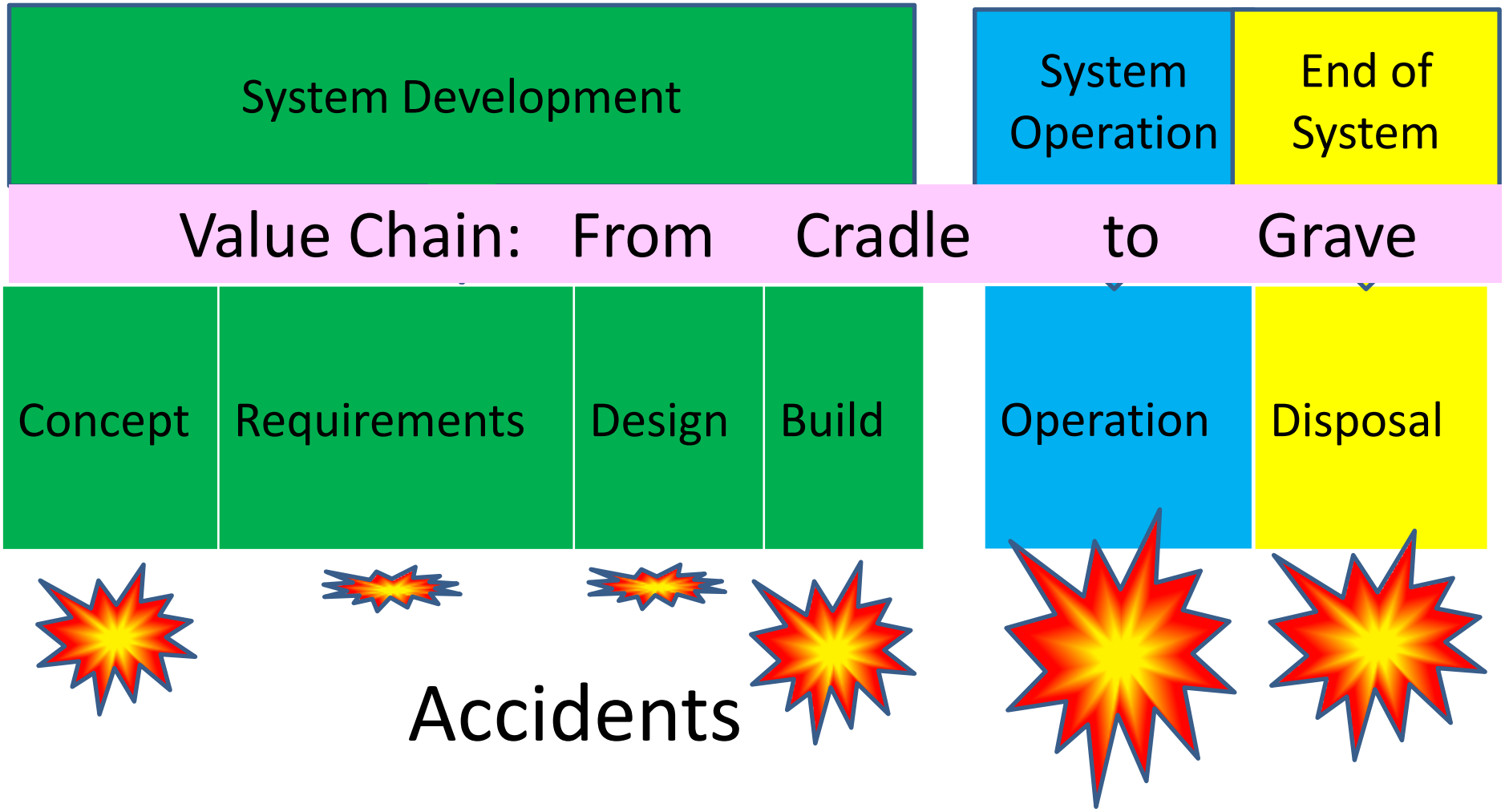
- An unexpected and undesirable event, especially one resulting in damage or harm.
- anything that occurs unintentionally or by chance
- a misfortune or mishap, esp. one causing injury or death.
- any event that happens unexpectedly, without a deliberate plan or cause

"Accidents" | Fragmented Worlds



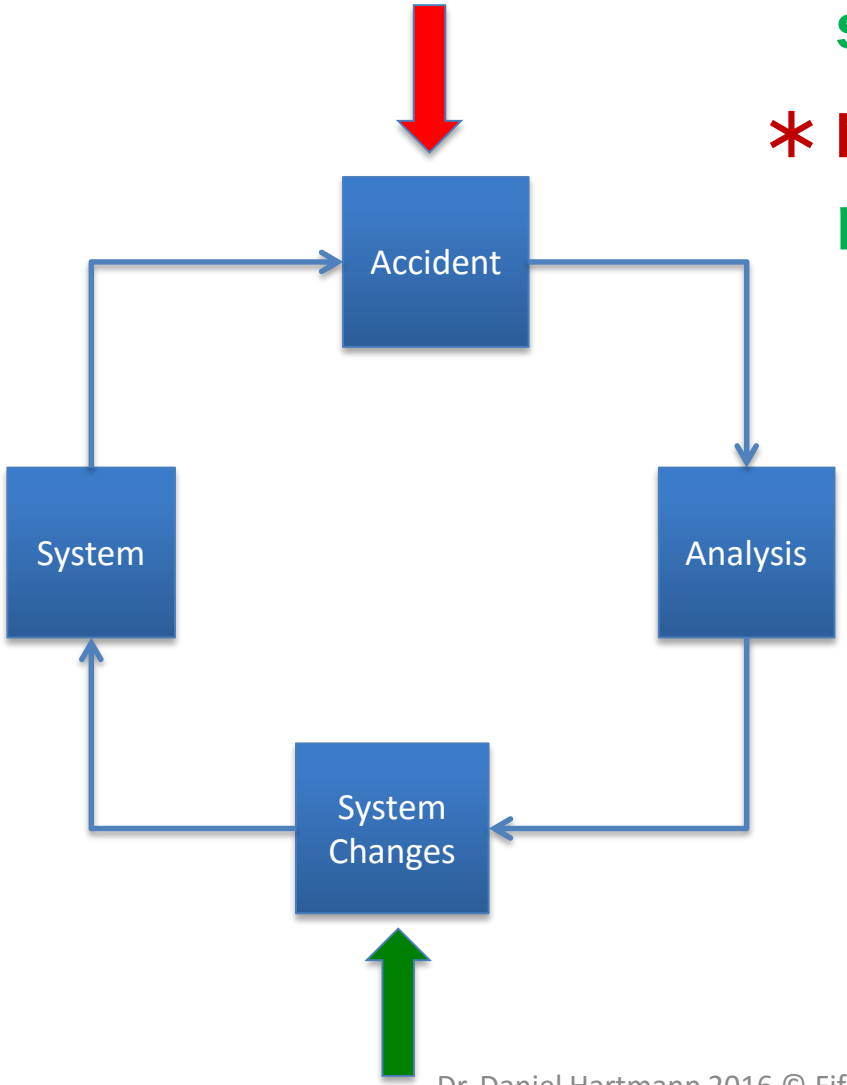
STAMP & Systems Lifecycle

Safety & Accidents

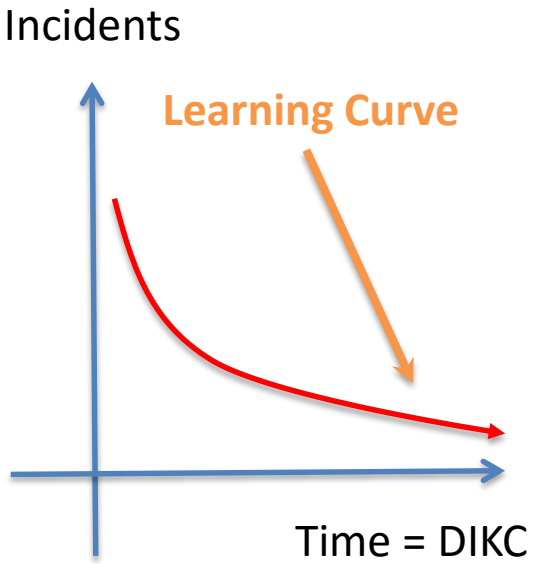


Why do Accident* Analysis along the entire Value Chain?

* loss that is unacceptable to the stakeholders
* Non accomplishment of the mission



Sociotechnical System as A Learning Organization



"Hidden" / Latent Accidents in Criminal Justice*

- The **Hidden Accidents principle** refers to reality in which accidents in **criminal law** — false convictions — tend to remain concealed. In contrast to aeronautics, for example, where an airplane crash is an open fact, no one — except the person accused, who is almost never believed — ever knows or can know that a defendant has been wrongly convicted. This enables legal decision-makers to optimistically assume the system is close to perfect, and makes it virtually impossible to prove otherwise.
- the Hidden Accidents Principle is what facilitates many optimists about the criminal justice system to compellingly claim that false convictions never occur, or else understate their frequency.
- Due to the Hidden Accidents Principle in criminal law, many people continue to have great faith in the system and are confident that the rate of false convictions is low. … this is hardly the case.

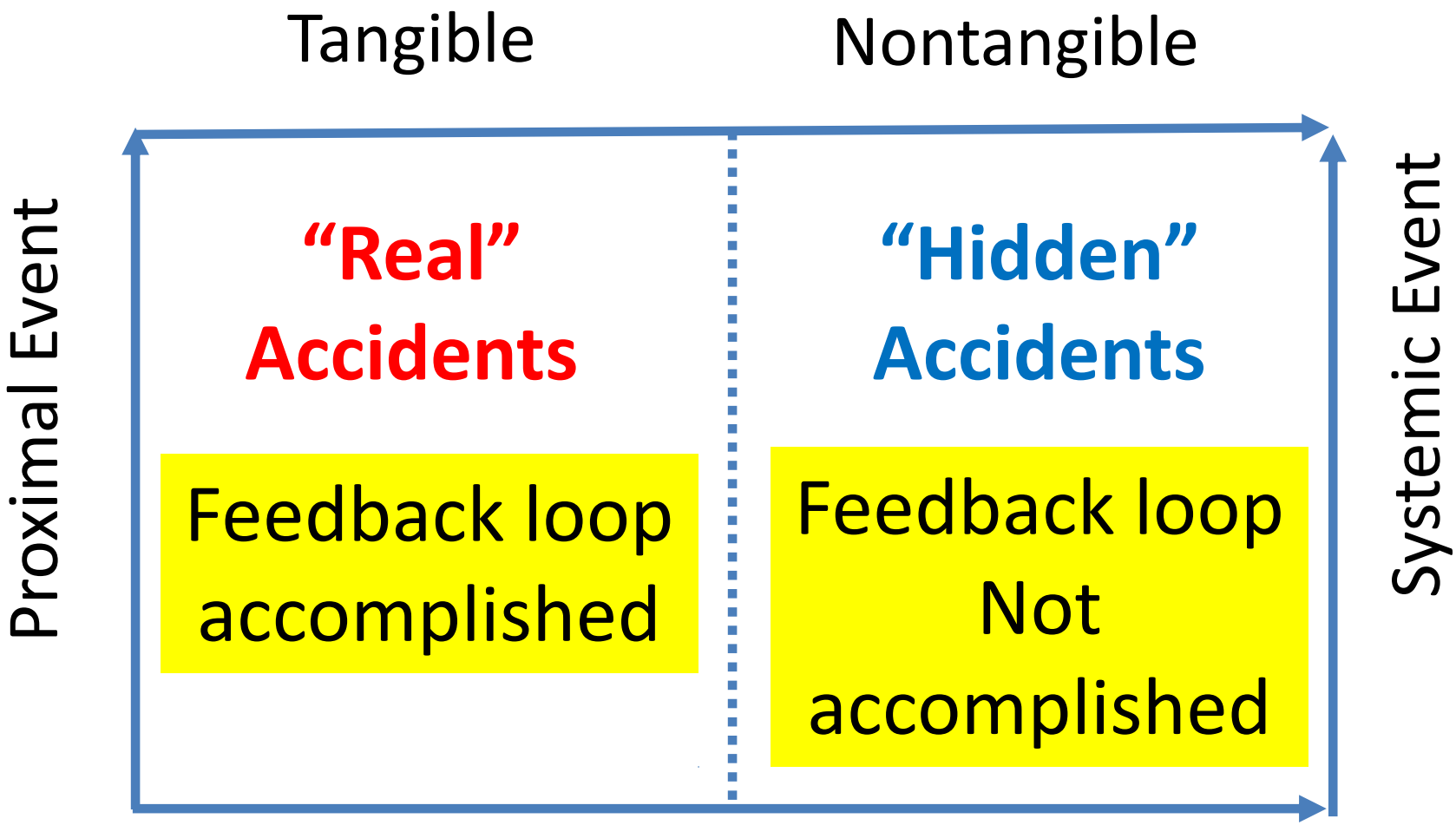
* Boaz Sangero, Safety from False Convictions

"Hidden" / Latent Accidents in Criminal Justice, Cont.

- This inability to detect **wrongful decision** is a highly significant feature of sociotechnical system, which we call the "Hidden Accident Principle." This principle can be formulated as follows:
- A sociotechnical system is characterized by accidents (wrongful decision) that typically remain undetected. The inability to detect these accidents translates into optimism on the part of policymakers that **false decision** only occur at a negligible rate.
- In a reality in which wrongful decision go undetected, the sociotechnical system in fact receives **no immediate feedback** or a delayed feedback once the wrongful decision materializes and the hidden accident become visible as a tangible accident

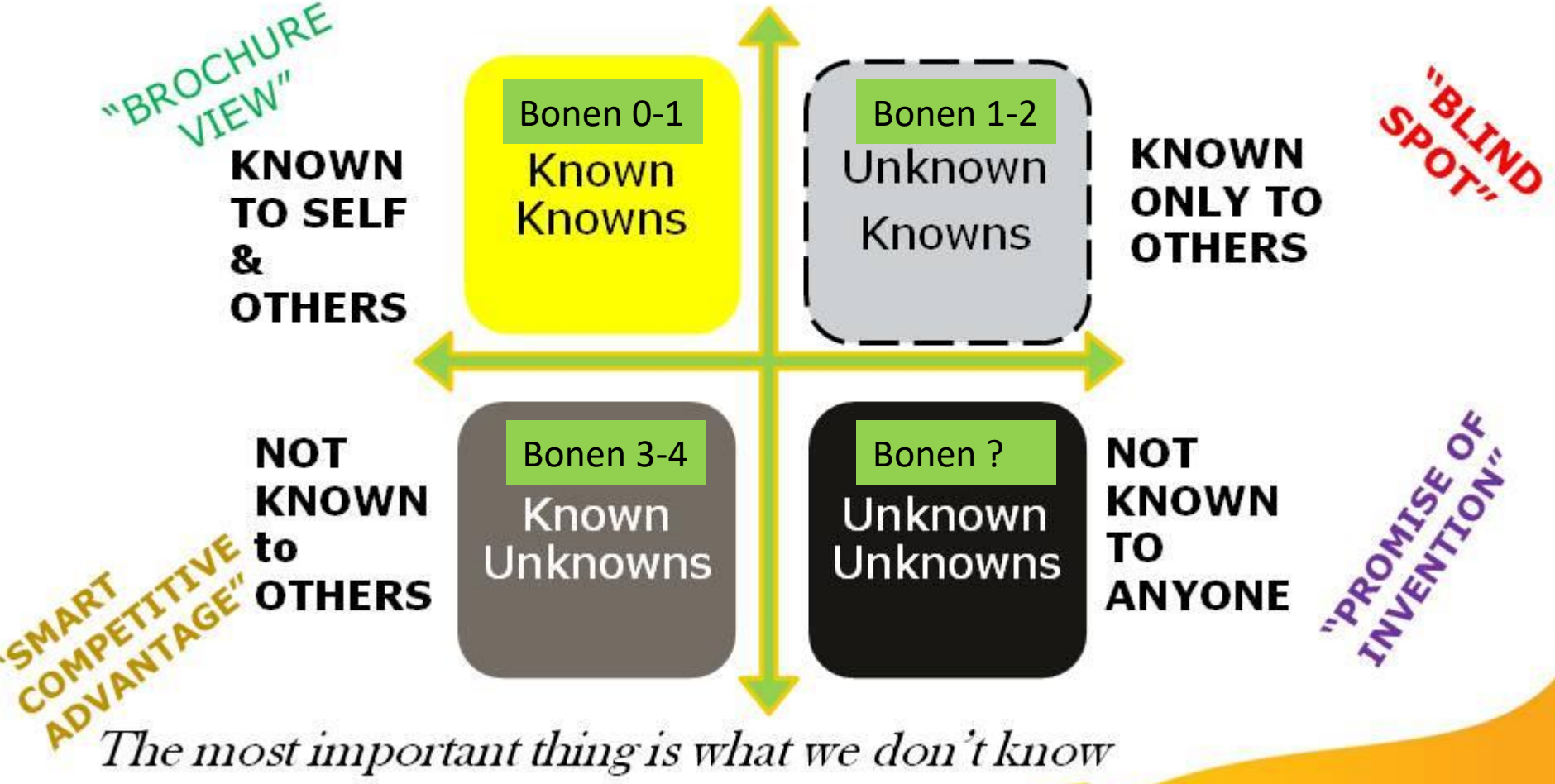
The higher we are in the Hierarchical Safety Control Structure, the more prominent the problem of wrongful decision is!

Another view of **Accidents Classification**



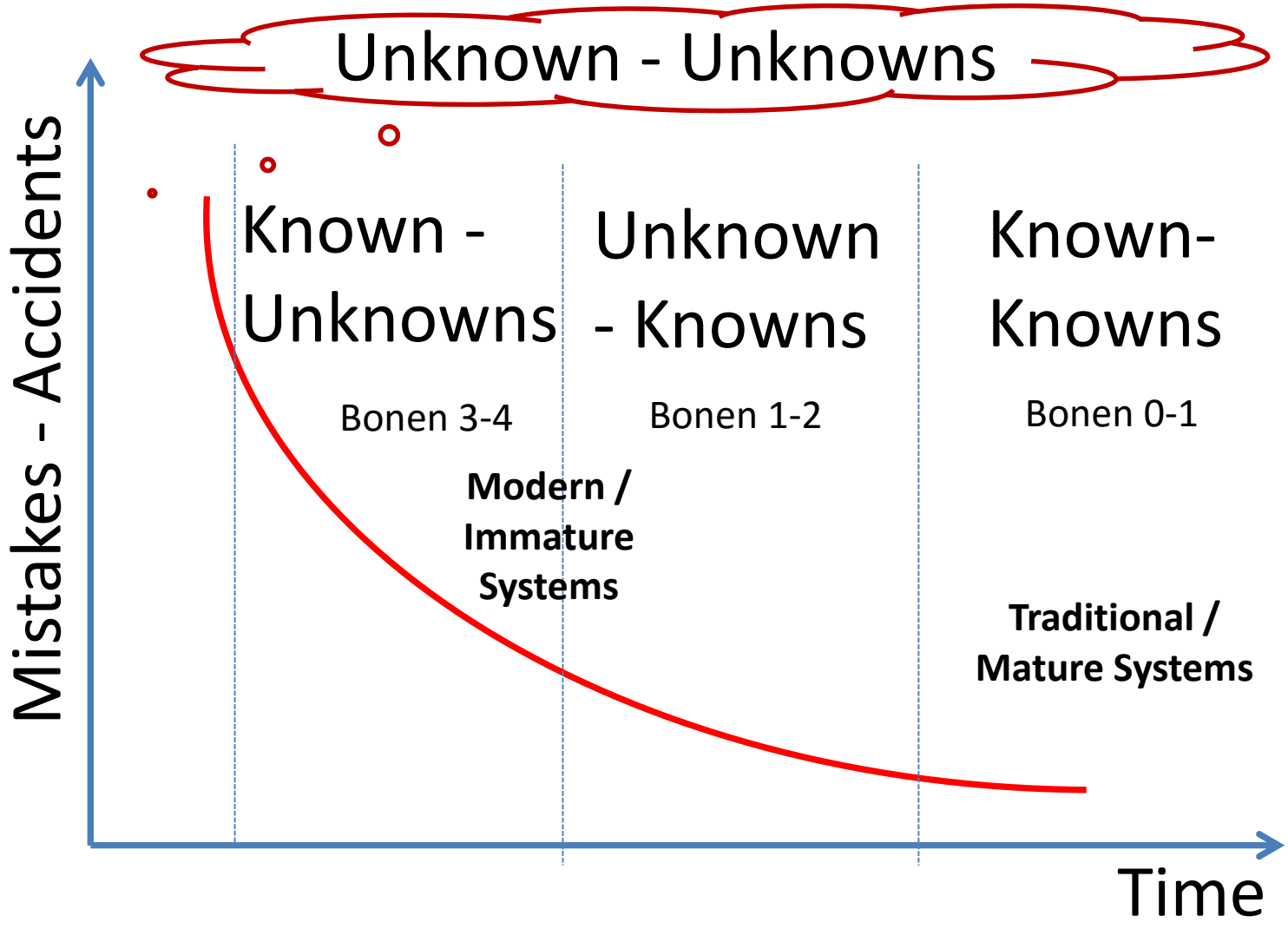
"Rumsfeld's Dilemma"

Information, knowledge is everything



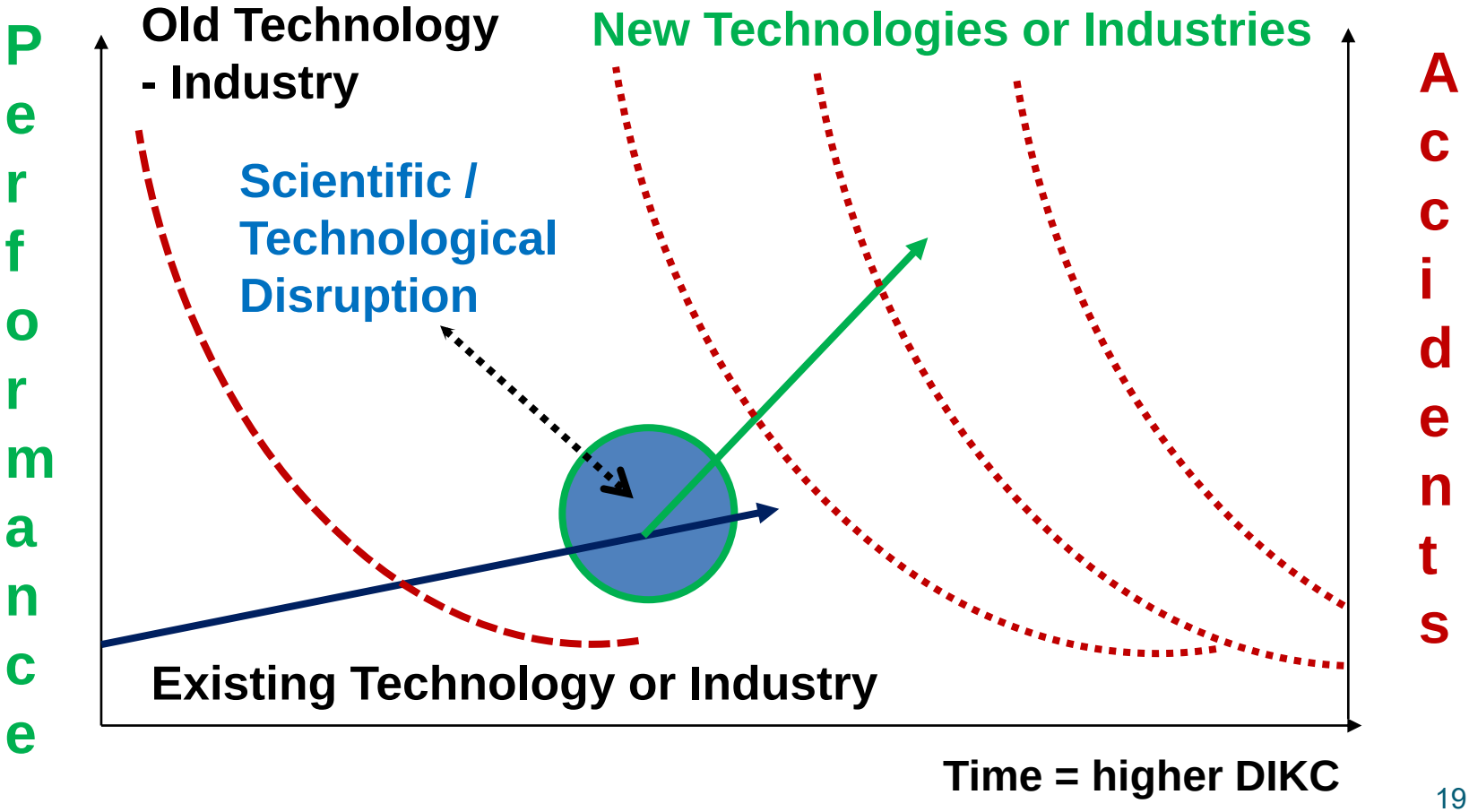
The most important thing is what we don't know

Learning Curve & "Knowledge"

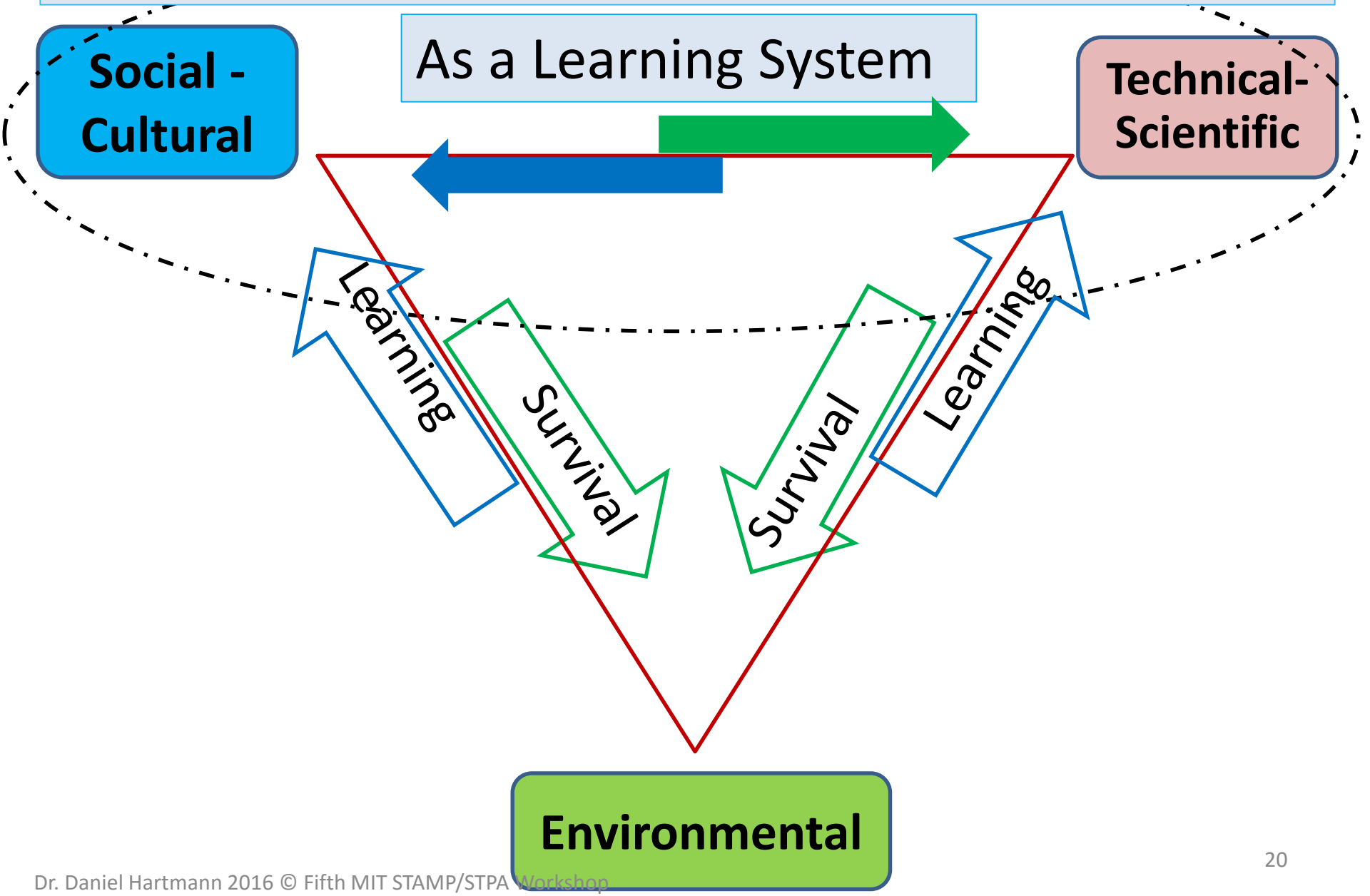


Dynamics, Change, Disruptive Technology, Accidents and DIKC

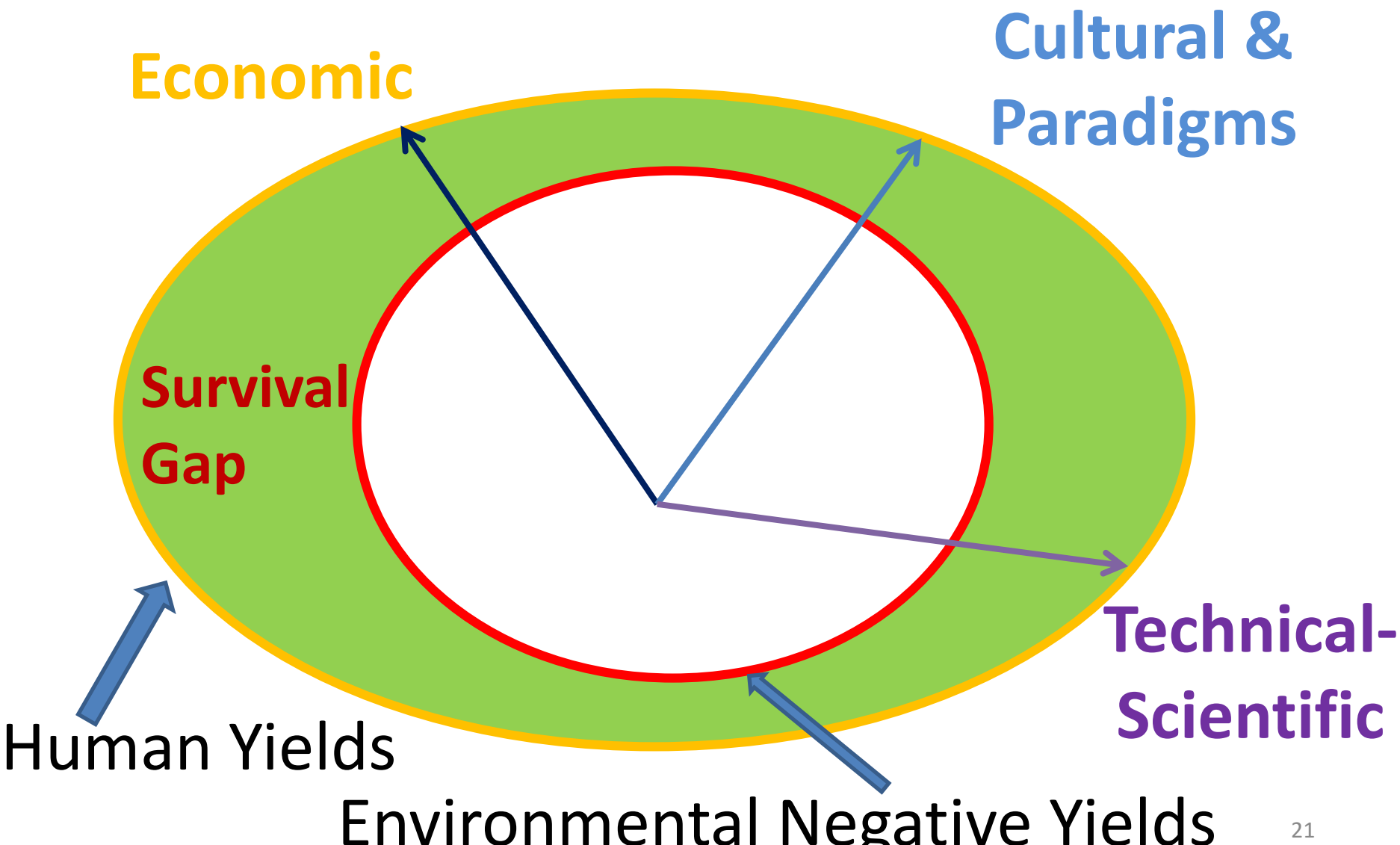
Performance = speed, availability, quality, productivity, profit, technology, reliability, **safety**, etc.



The “Real System” and a Socio-technical System

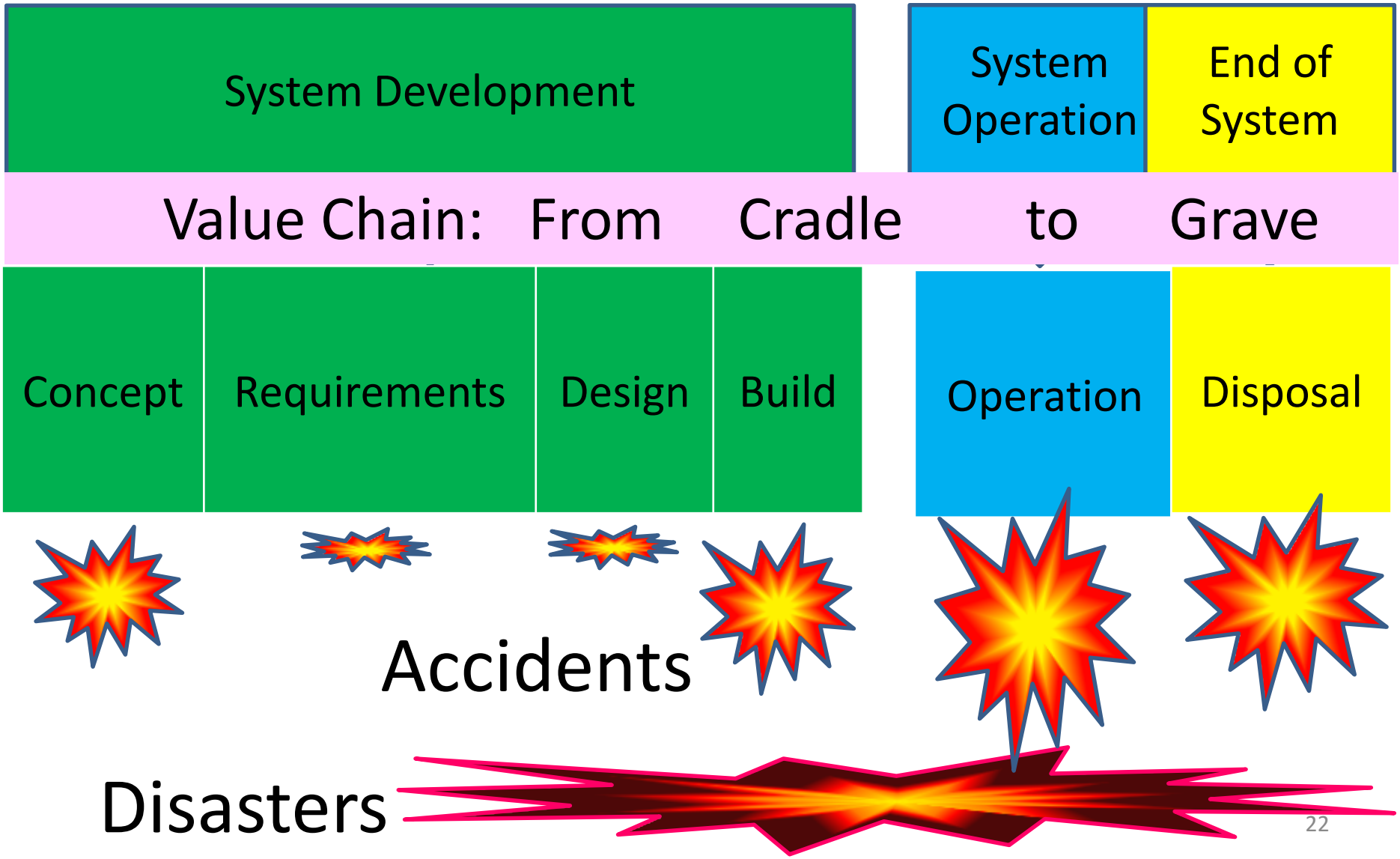


Learning Socio-technical Systems, Safety & Survival Gap



STAMP, Sociotechnical Systems Lifecycle

Safety, Accidents & Disasters



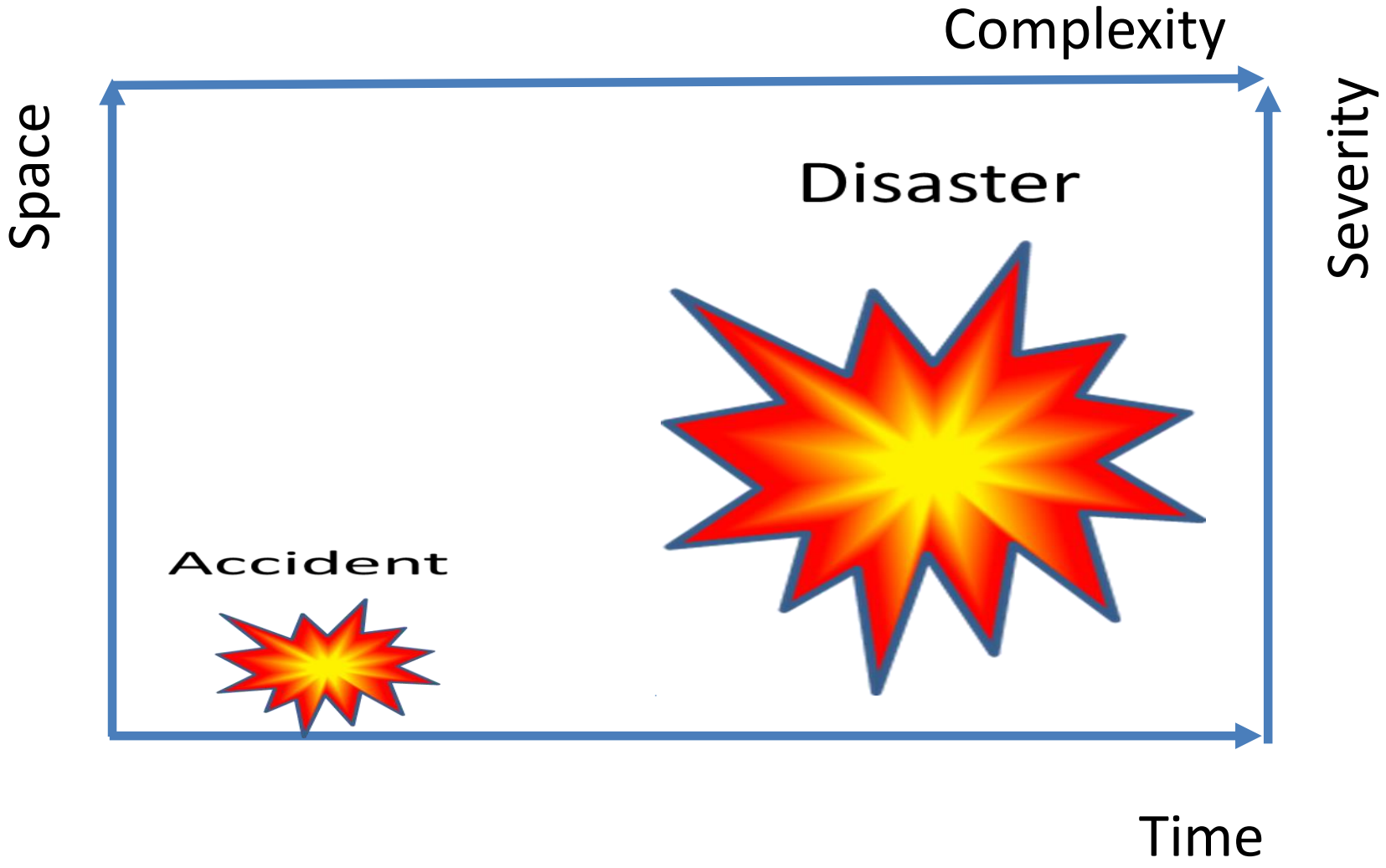
Definitions of Disaster

- a sudden event, such as an **accident** or a natural catastrophe, that causes great damage or loss of life.
- an event or fact that has unfortunate consequences.
- a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts…
- A disaster is a sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community's or society's ability to cope using its own resources.

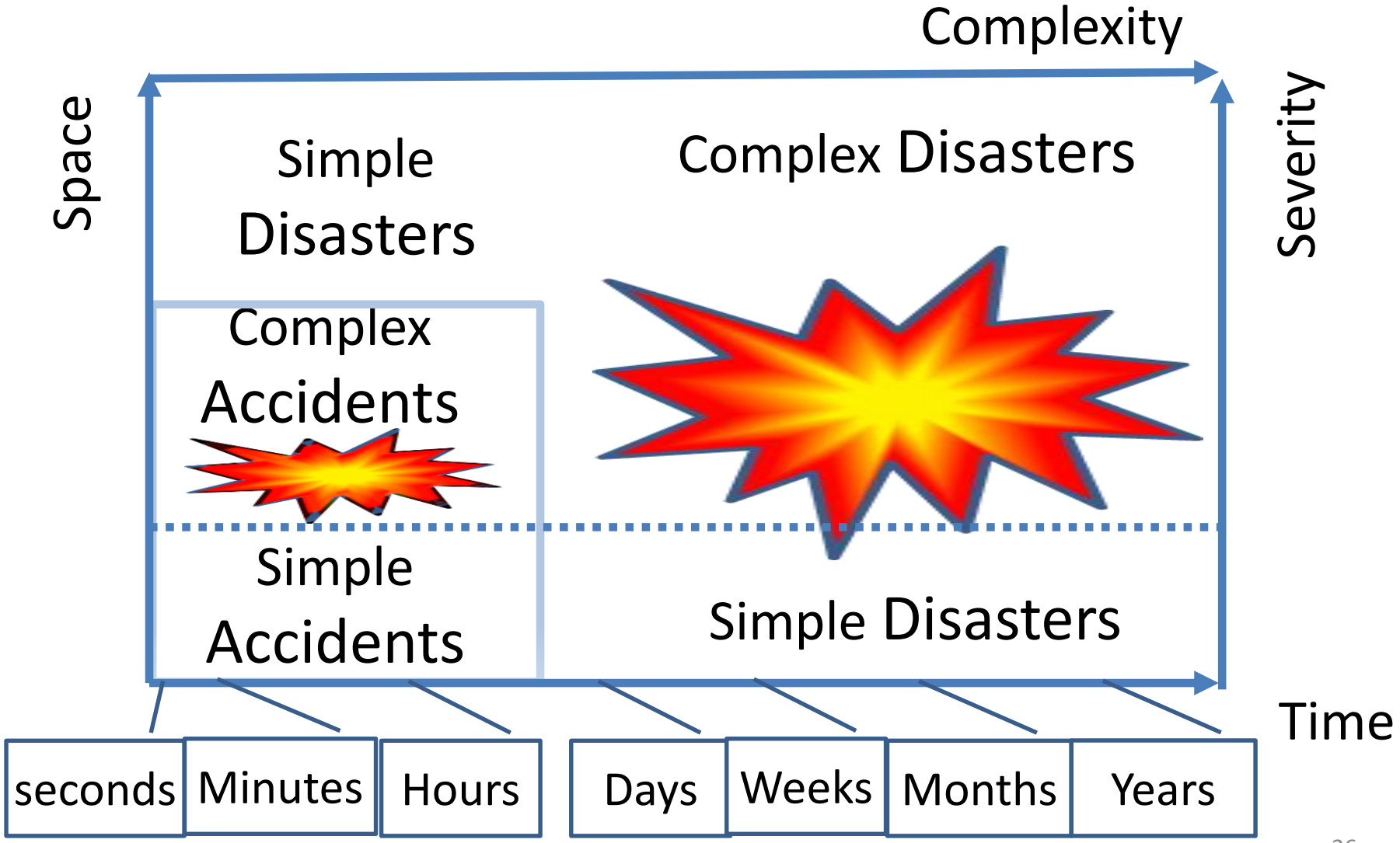
Harmonizing “Different” Worlds

Accident = Disaster

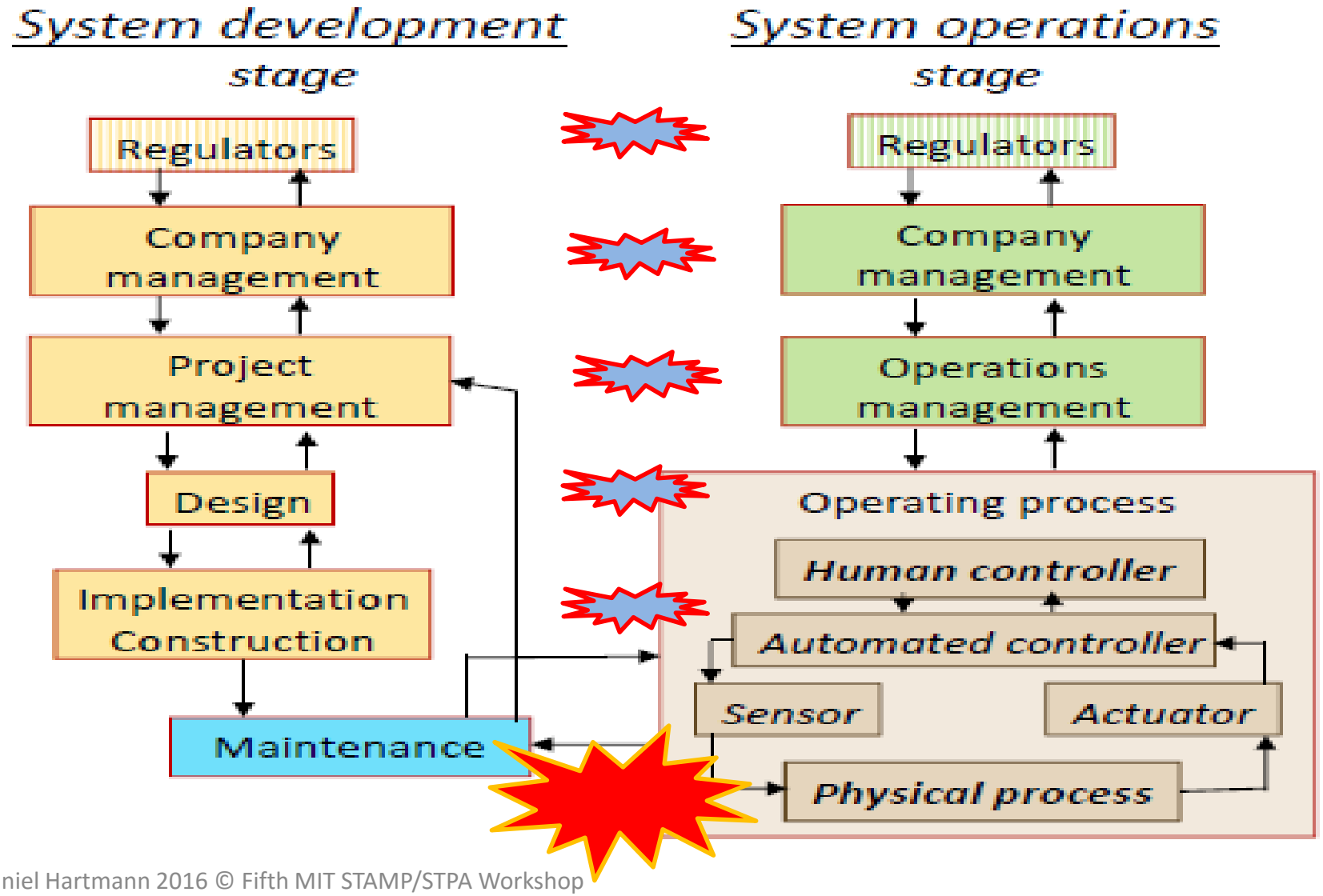
Relationship between
Accidents and Disasters



And another view of Classification of **Accidents and Disasters**



Hierarchical Sociotechnical Systems with Levels connected by Control Flows



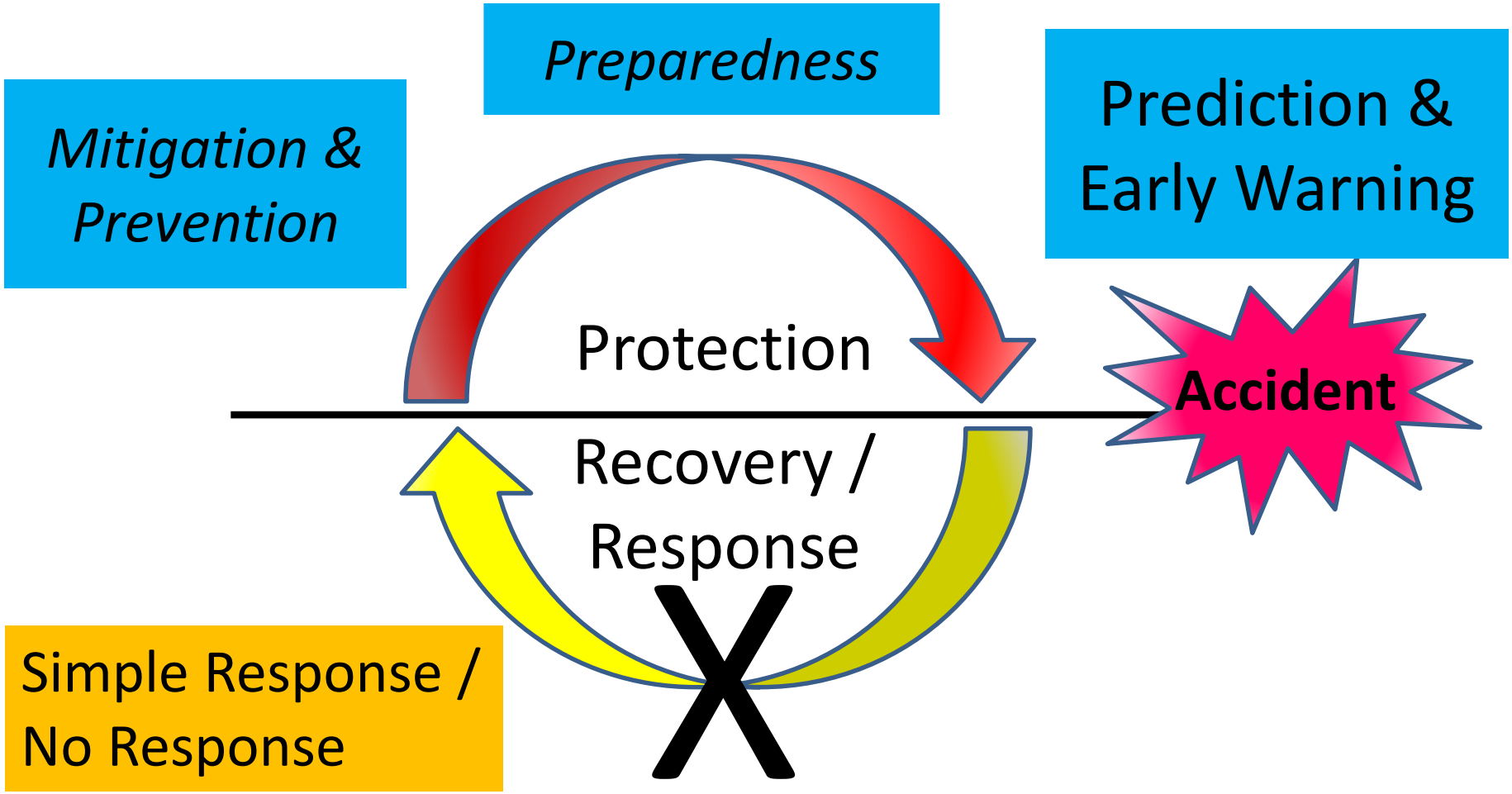
Outline

- Motivation
- Harmonizing...
- Accident / Disaster Cycle
- Some thoughts about Sociotechnical Systems,

  Accident / Disaster Cycle & STAMP

Accident Lifecycle

Safety: Hazard & Risk Management



Relationship between
Accidents and Disasters

Accidents	Disasters
Time Limited	Time Limited - Unlimited
Space Limited	Space Limited - Unlimited
Complexity Limited	Complexity Limited - Unlimited
Severity Limited	Severity Limited - Unlimited
Simple Response	**Complex Response**

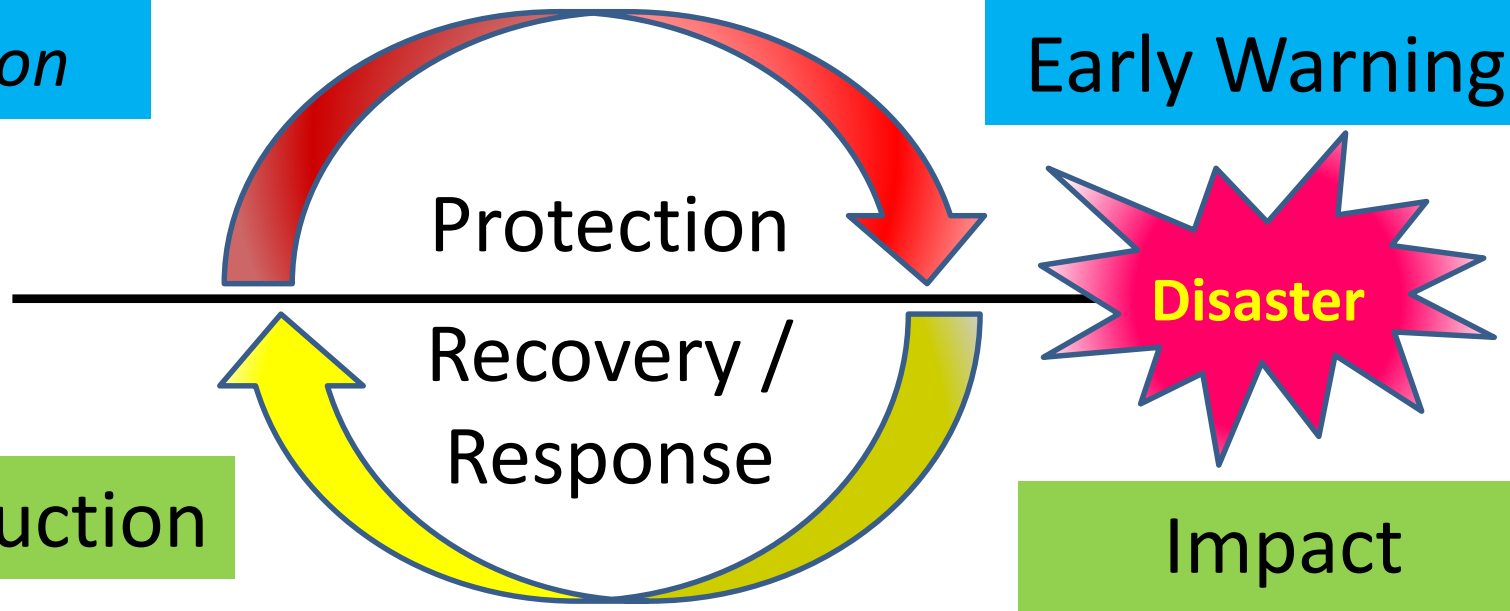
Disaster (Accident) Lifecycle

Safety: Hazard & Risk Management

Preparedness

Mitigation & Prevention

Prediction & Early Warning



Reconstruction

Impact Assessment

Recovery

Response

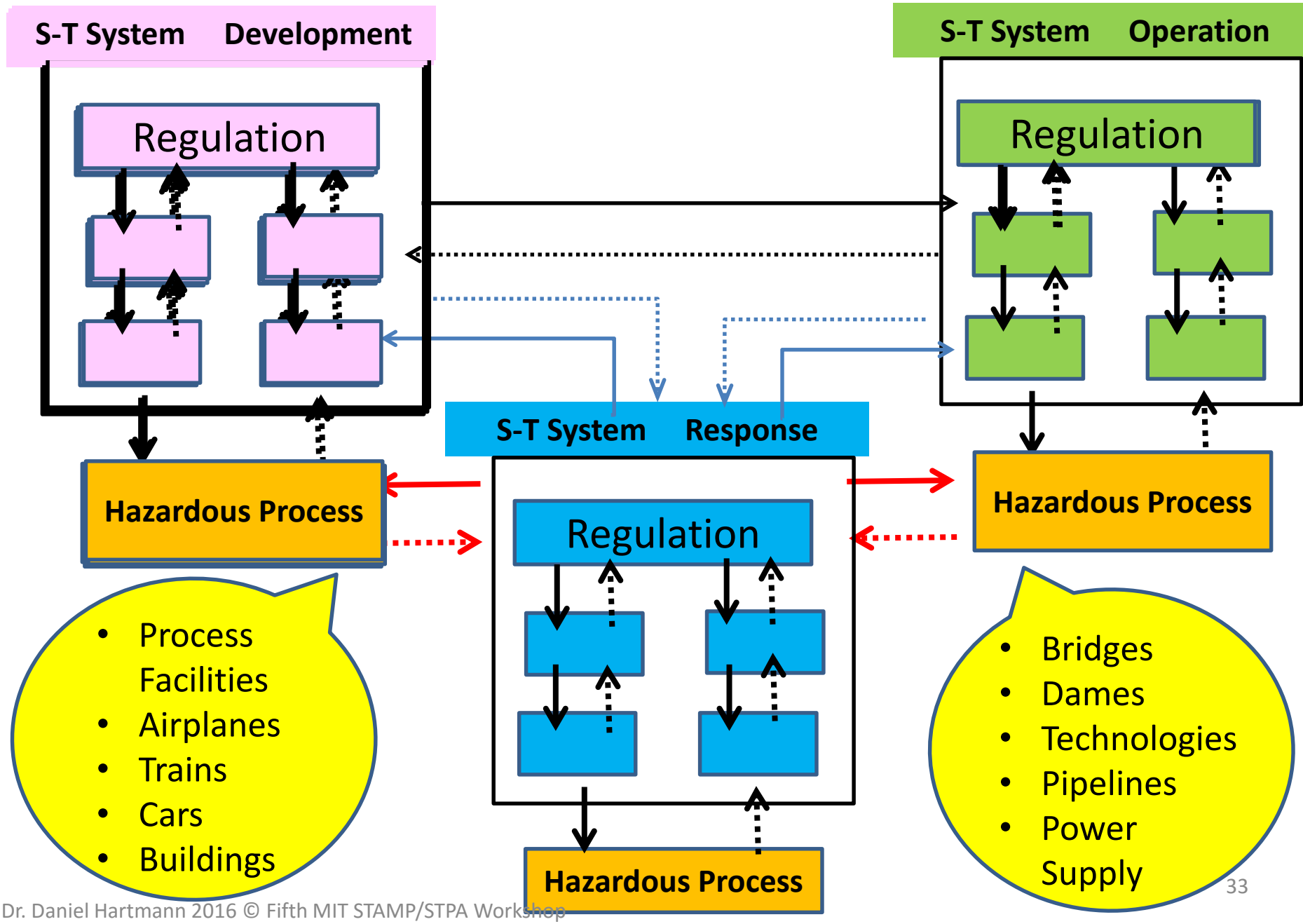
Crisis / Response Management

Outline

- Motivation
- Harmonizing...
- Accident / Disaster Cycle
- Some thoughts about Sociotechnical Systems,

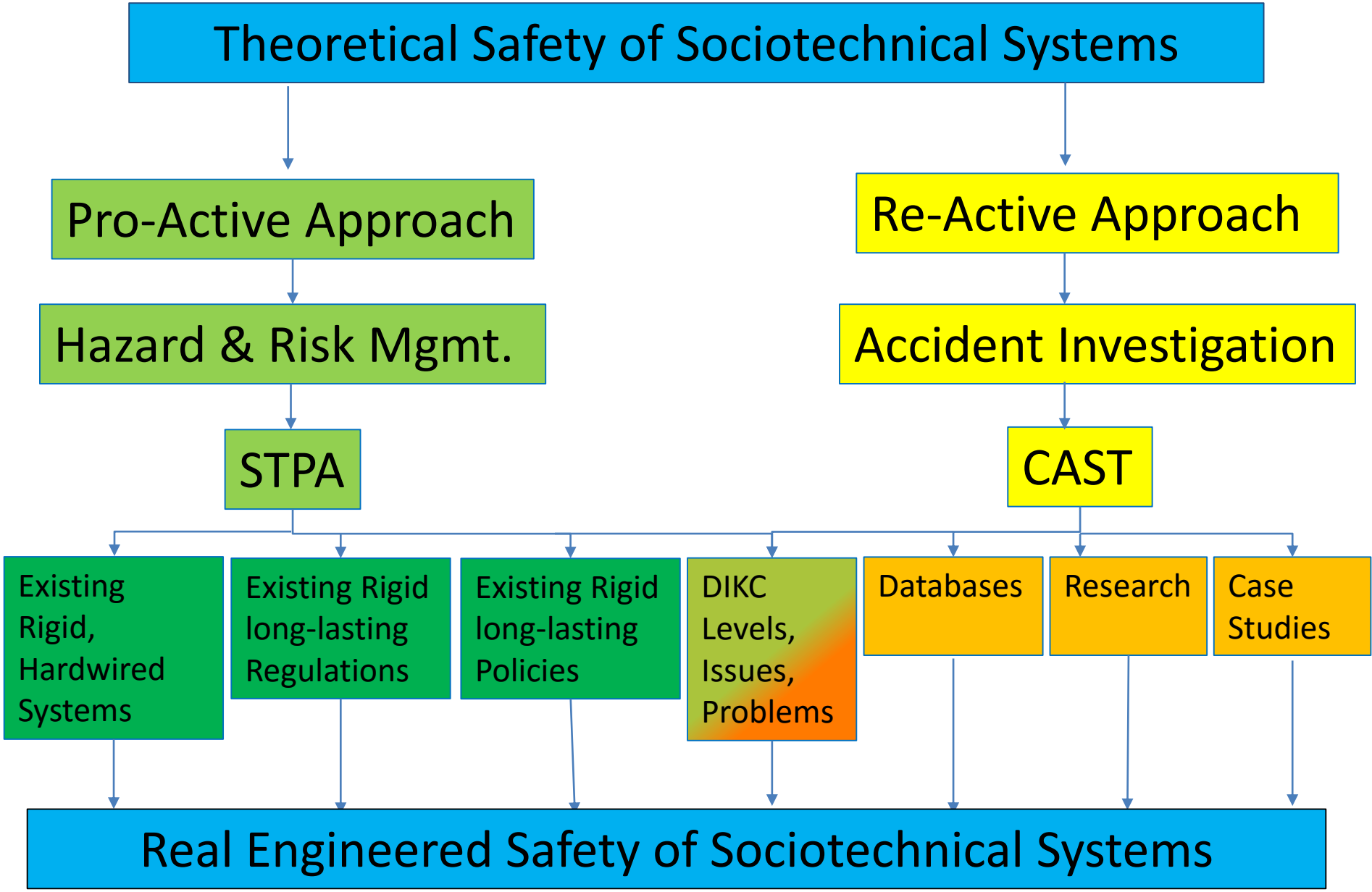
  Accident / Disaster Cycle & STAMP

Sociotechnical Systems and Full Lifecycle [Development, Operation & Response]



Safety Lifecycle of Sociotechnical Systems [Development, Operation & Response]

S-T System Development	S-T System Operation	S-T System Response
Legislation	Legislation	Legislation
Regulation	Regulation	Regulation
Corporate Management	Corporate Management	"Corporate" Management
Company Management	Company Management	"Company" Management
Project Management	Project Management	Project Management
Manufacturing Management	Operation Management	Operation Management
Manufacturing: Hazardous Processes	Operating Process: Hazardous Processes	Operating Process: Hazardous Processes



Daniel Hartmann
danielh@bgu.ac.il

Daniel Hartmann
danielh@bgu.ac.il