6th STAMP Workshop 2018, Amsterdam

CAST Analysis of the 2016 Bromine Train Accident in Dimona, Israel Using Extended STAMP Model

Vitaly Shrager, **Daniel Hartmann** & Roni Shneck

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

Bromine as hazardous material

Bromine

Dark, red-brown liquid with an irritating odor. Corrosive! Causes severe irritation or burns to eyes/skin/ respiratory tract. Toxic! Also causes: dizziness, headache, coughing, and pulmonary edema. Strong oxidizer capable of igniting combustibles.

CAS No. 7726-95-6

- Bromine is a chemical element with symbol Br and atomic number 35.
- It is the third-lightest halogen, and is a fuming red-brown liquid at room temperature that evaporates readily to form a similarly colored gas.

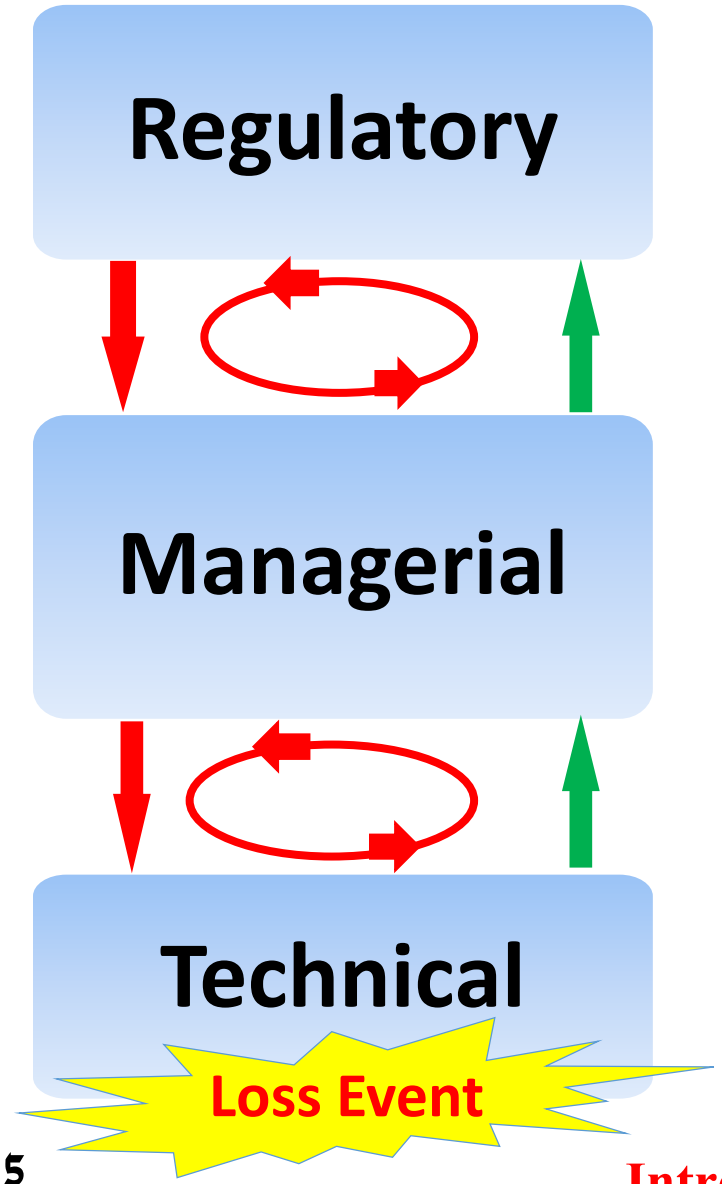
Bromine as hazardous material

- Bromine is both **corrosive** and **poisonous**.
- Bromine is shipped from the Dead Sea to the ports of Haifa and Ashdod on **nighttime trains** that run through population centers like **Dimona**, Beer-Sheva, Hadera and Haifa.
- The Israeli Environmental Protection Ministry has estimated that a container ruptured during transport would cause the deaths of anywhere from 6,500 to 350,000 people, and would go straight into the ground and damage infrastructure as well.

Bromine as hazardous material

- In the Middle East, the Dead Sea is estimated to contain 1 billion tons of Bromine.
- Israel is the one of the biggest producer of Bromine.
- Bromine is mined out of the Dead Sea, and produced by Dead Sea Bromine Company Ltd which is Israel Chemicals Limited (**ICL**) company.
- Israel uses a small amount domestically and exports ca. 150,000 metric tons a year.
- Israel Chemicals Limited (**ICL**) produces and transports worldwide approximately a third of the world's Bromine.
- Bromine is used in a variety of industries, including food processing, flame retardants, beauty products and water treatment.
- "Global Bromine Business 2018: Leading Players are Albemarle, Israel Chemicals Ltd, Jordan Bromine, …"

Model and Methods: STAMP, CAST (and STPA) for Hierarchical Sociotechnical Systems



STAMP: Accident Causation Model

Accidents arise From complex, Dynamic processes, Not Linear Chain of Events

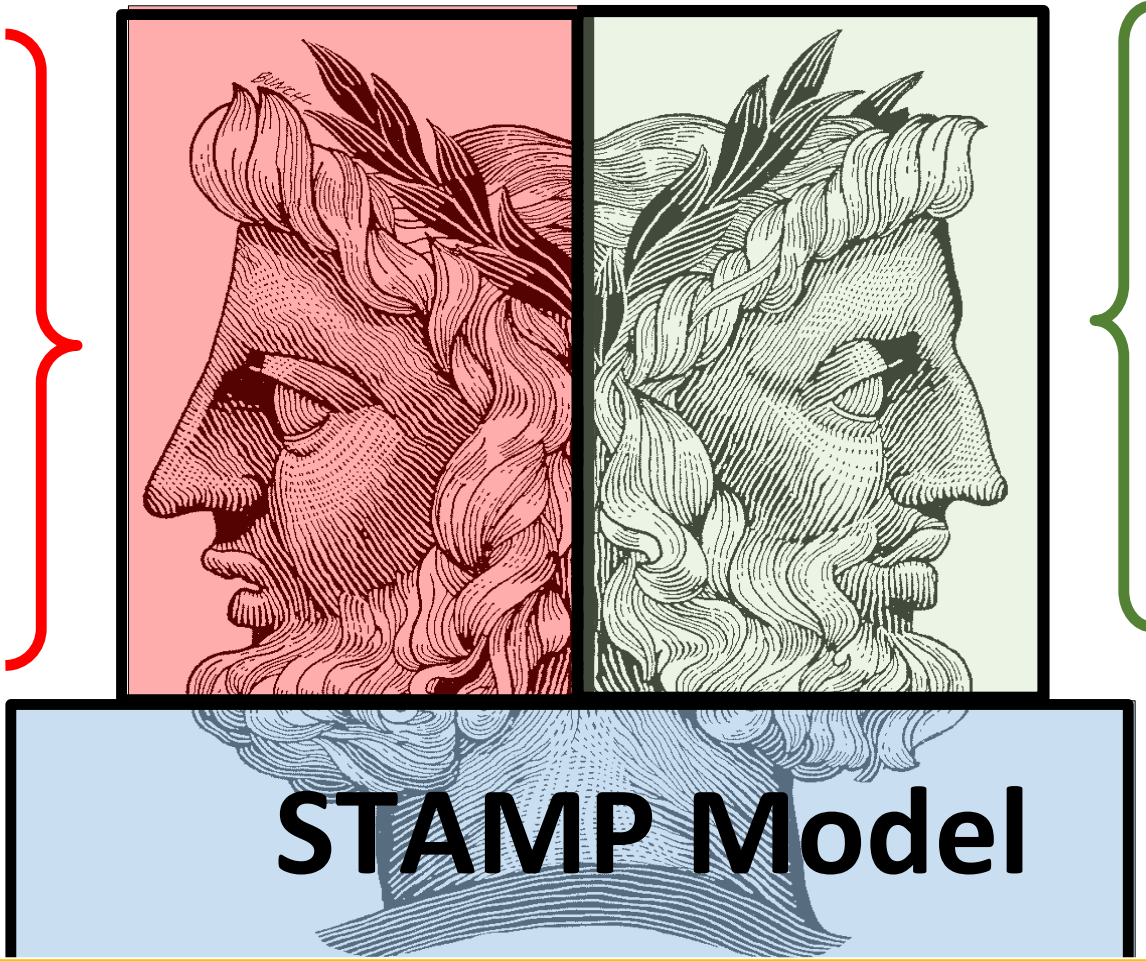
Accidents are a **Control Problem**, not a failure problem

Accidents Prevented by **Enforcing Constraints** on Systems Functions & Component Behavior and Interactions

CAST Accident Analysis ⟺ STPA Hazard Analysis

Reactive:

How do we find inadequate control **that caused** an accident?



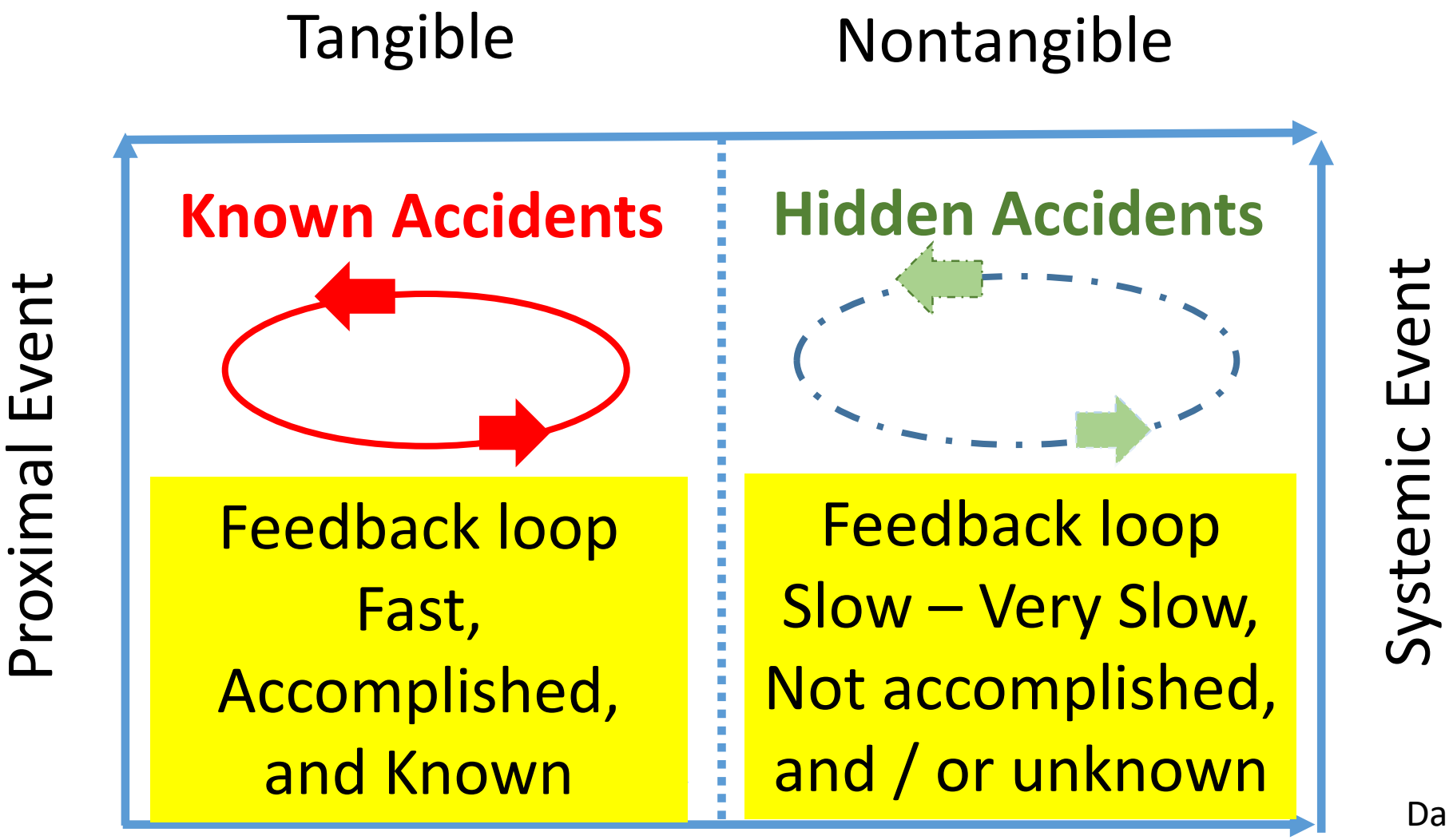
Proactive:

How do we find inadequate control **in a design** (Development, Operation, Response)?

Accidents are caused by inadequate control

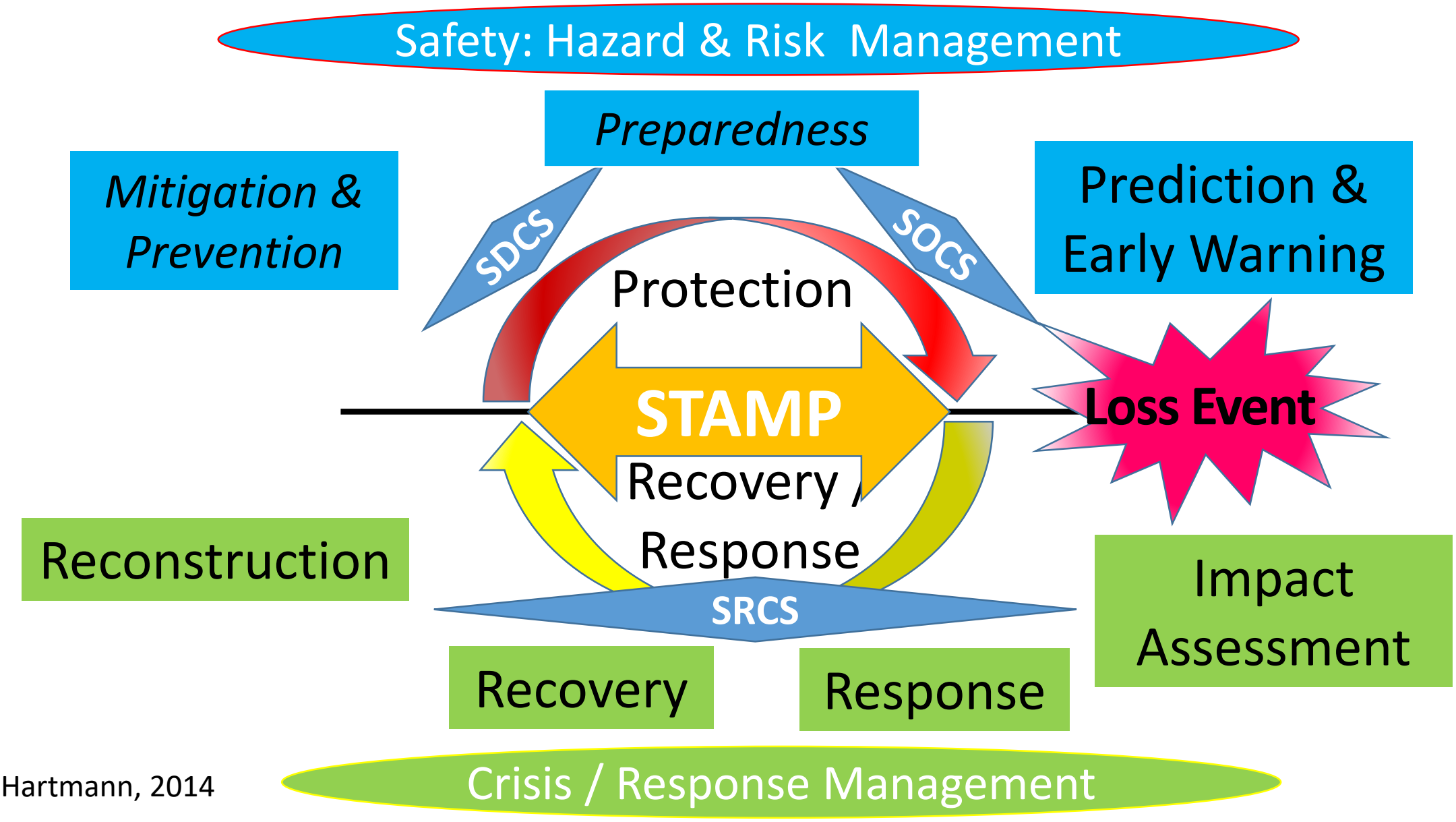
System Theory / Systems Engineering / Sociotechnical System / control theory / Emergent Property

New Loss-Events / Accidents Classification



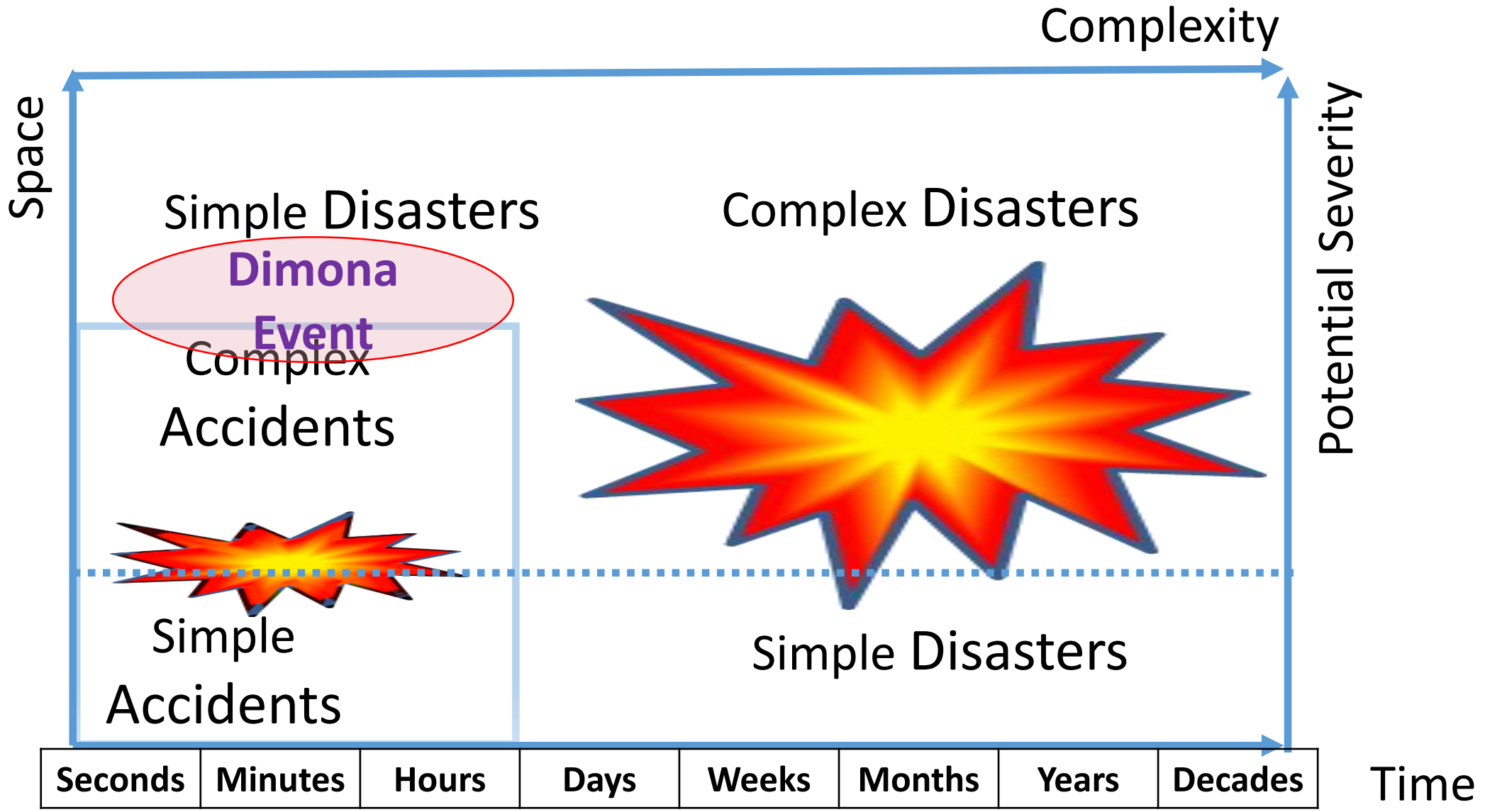
Daniel Hartmann, 2014

Disaster / Accident / Loss Event Lifecycle

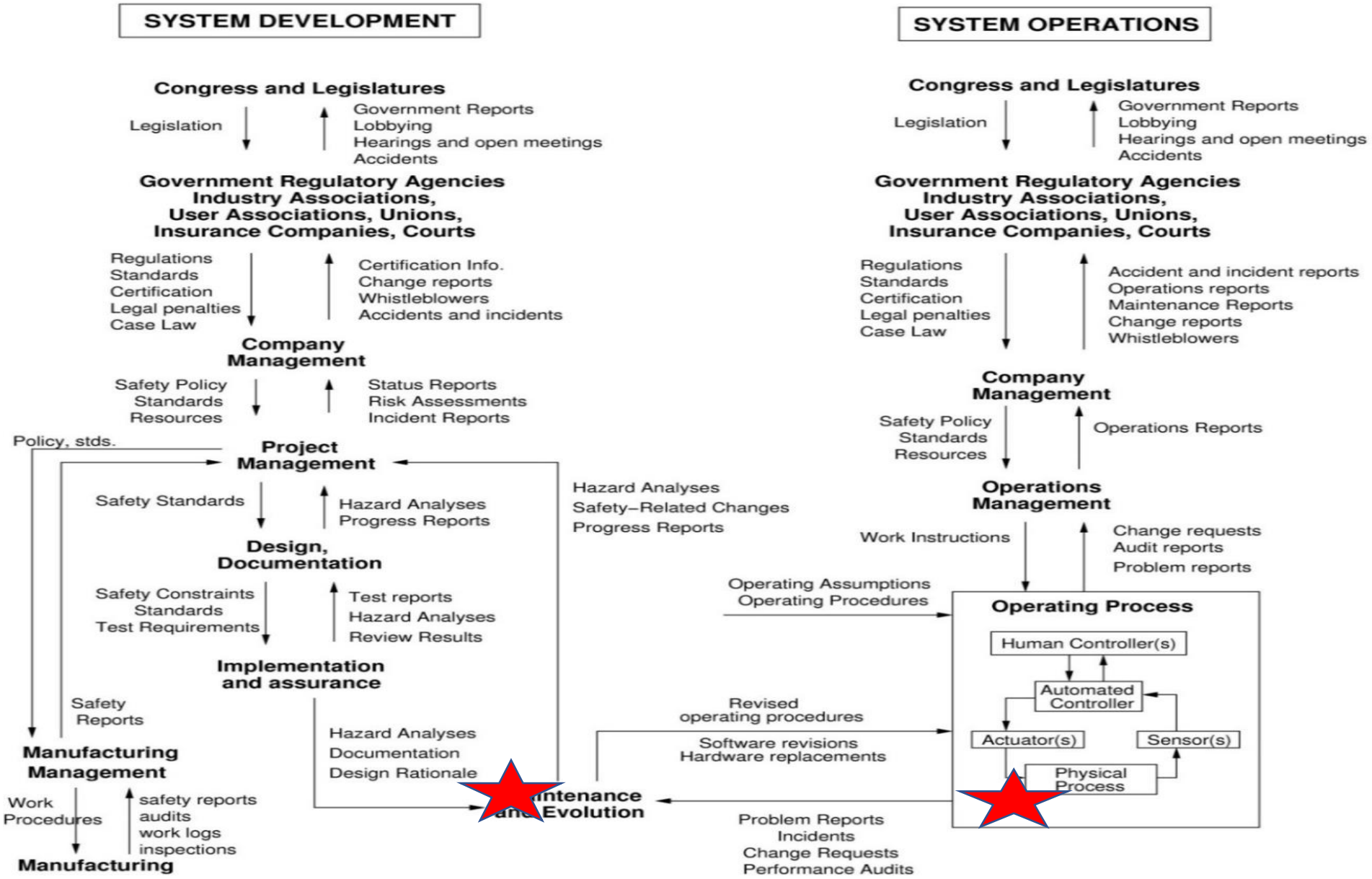


Daniel Hartmann, 2014

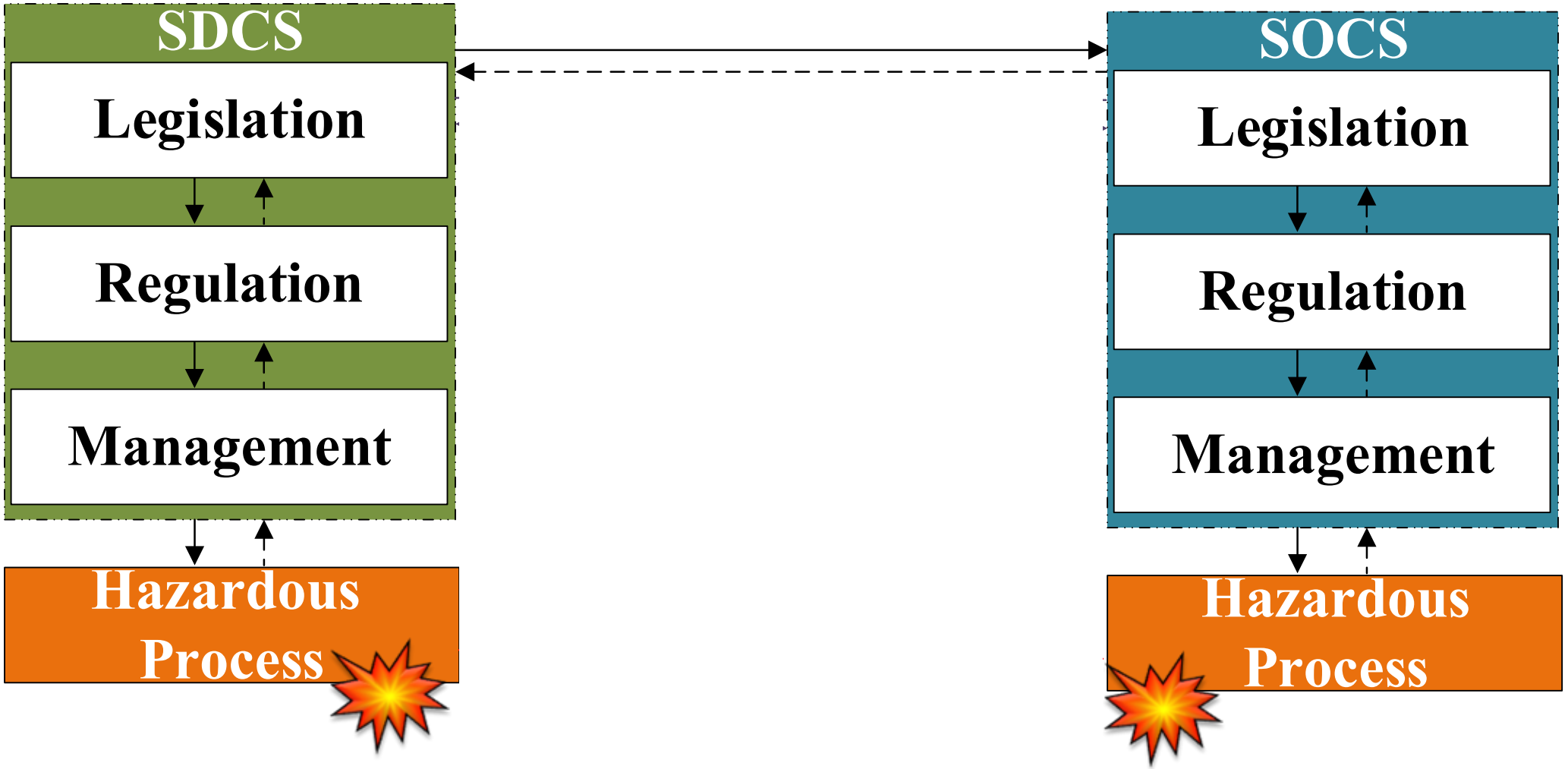
Accidents, Disasters and Loos Events



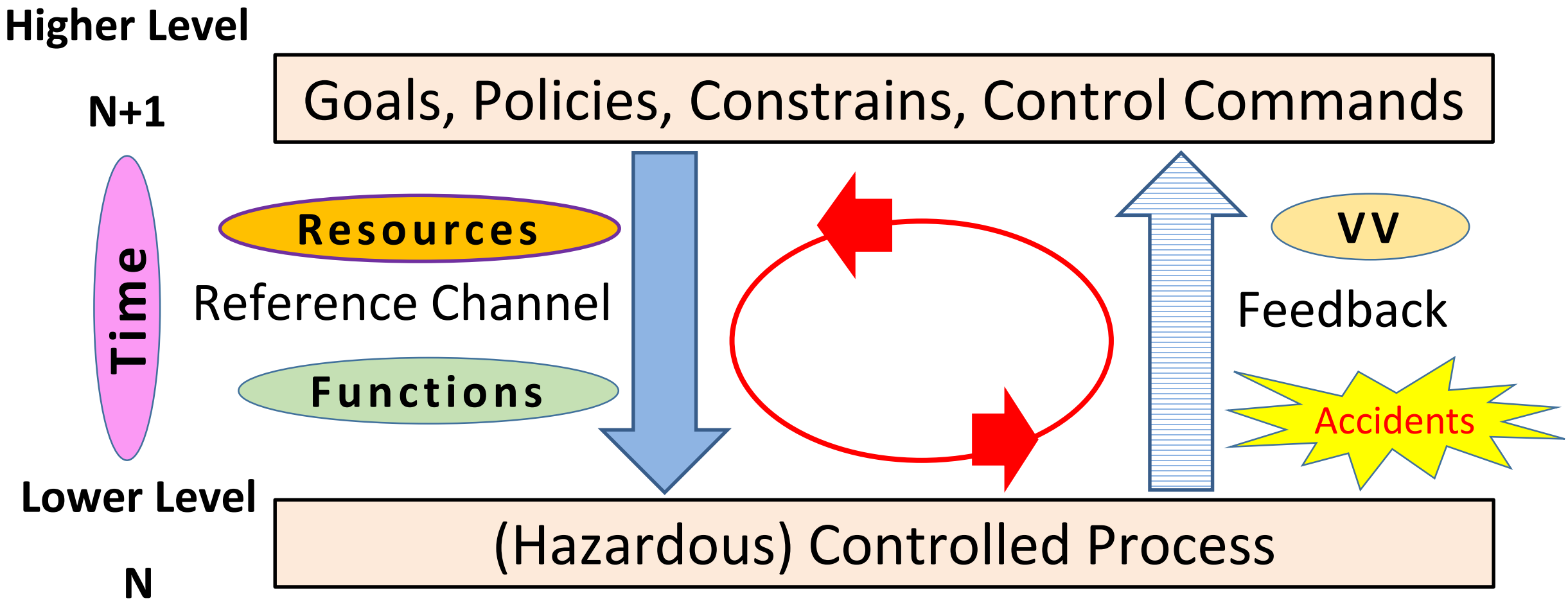
Hierarchical Functional Safety Control Structure (Leveson)



The Sociotechnical System as hierarchical control structures (Leveson)

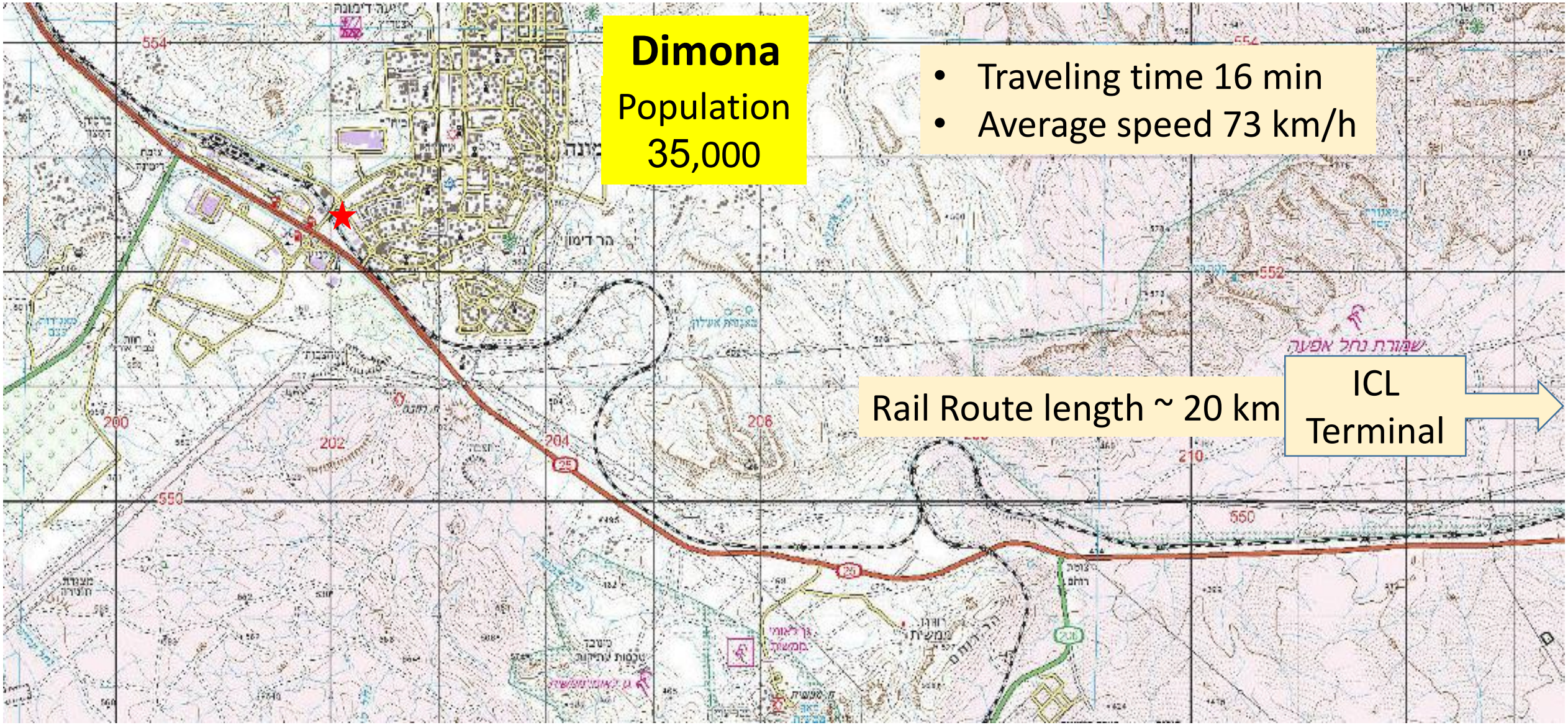


Simplified hierarchical functional Safety control loop



Simulation of the Events

Geographical Setup of the Area of Event - NE Negev, Israel



Identification of accidents and hazards involved in the events

Accident		STSs
Uncontrolled separation of freight cars (train A)	A1	SDCS & SOCS
Collision of Train B in freight cars of Train A	A2	SDCS & SOCS
Damage to the integrity of Bromine ISO tank and Bromine leakage	A3	SDCS & SOCS
Harm to population due to exposure to hazardous material	A4	SDCS & **SRCS**

Hazards		STSs
A train car may break up uncontrolled from a train	H1	SDCS & SOCS
keeping a minimum distance from another party on the way	H2	SDCS & SOCS
Uncontrolled release of energy	H3	SDCS & SOCS
Uncontrolled damage to structural integrity	H4	SDCS & SOCS
Uncontrolled release of hazardous materials into the environment	H5	SDCS & SOCS
Uncontrolled exposure of the population to hazardous materials	H6	SDCS & **SRCS**

Course of Phases and Events in Time

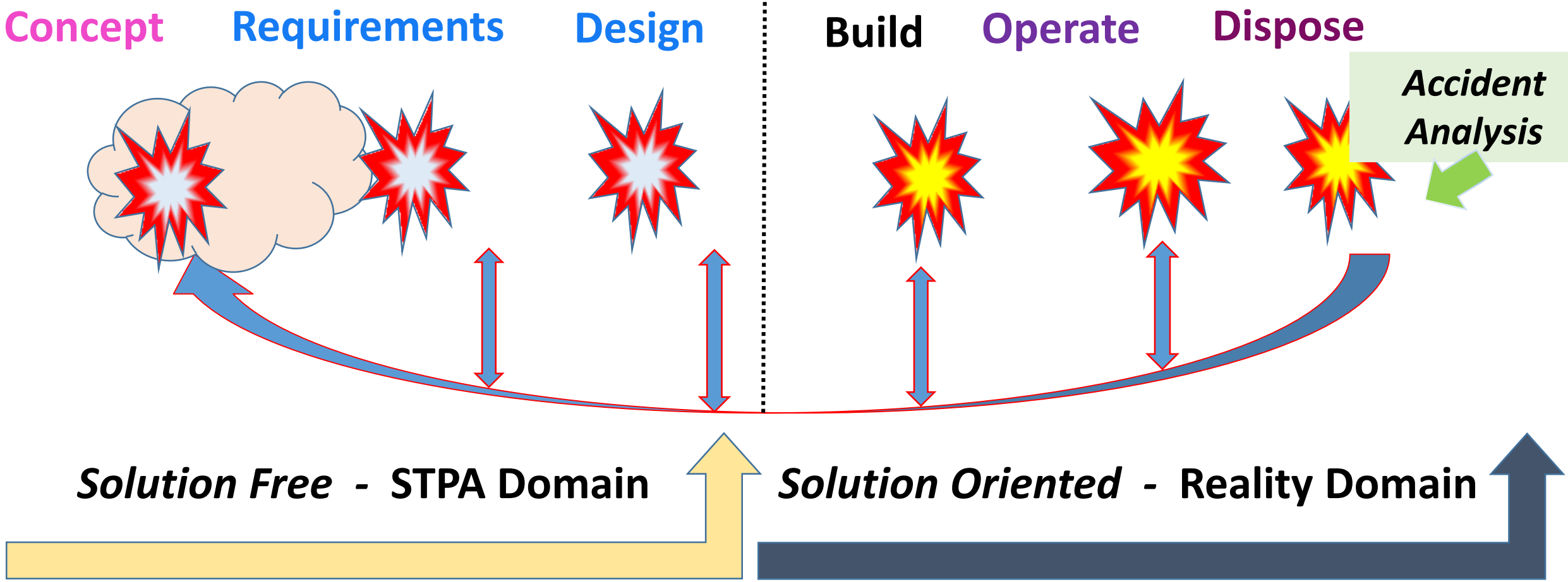
- Events were divided into six Phases of "time series“.
- Critical events **<u>preceding</u>** the **proximal events** and spread out over a period of a century.
- Critical events **<u>Leading to</u>** the **proximal events** and spread out over a period of many minutes.
- Proximal Events took few seconds.

✓ critical events (in **Respond Safety Control System**) that could contribute to the potential severity of the accident, spread out over a period of few hours after the immediate accidents.

History and "time series" related to the Bromine Event

Phases	Time Span	Duration	Activities – Hazardous Processes
The sequence of events **preceding** the accidents	ca. 1920 – 14 March 2016	ca. 100 Years	"Normal" Business Activities of rail transportation (SD, SO & SR)
Hidden Loss Events	14 March 2016 21:11 – 21:30	29 minutes	Uncontrolled separation of freight cars (train A) – Accident A1 (SO)
Sequence of loss events **leading** to disaster	14 March 2016 21:28 – 21:46	18 minutes	Unsafe Release & Travel of Train B (SO)
Proximal loss events	14 March 2016 21:46	Few seconds	Accidents A2, A3 & A4 (SO)
The sequence of events **following** the collision	14 March 2016 21:51	ca. 5 minutes	Begin of Response activities A4 (SR)
End of Respnse Events	15 March 2016 06:51	ca. 9 hours	End of event and back to Normality (SR & SO)

Value Chain, System's Lifecycle & Evidence Based Safety



Errors / "accidents" at various stages of system's lifecycle

Concept:

- Relationship of responsibilities between Ministry of Transport and Rail Company
- Transport of hazardous materials through population centers

Requirements:

- Signaling the integrity of train and its wagons
- Stability to real impact of carrying wagons
- Stability to real impact of ISO tanks

Design:

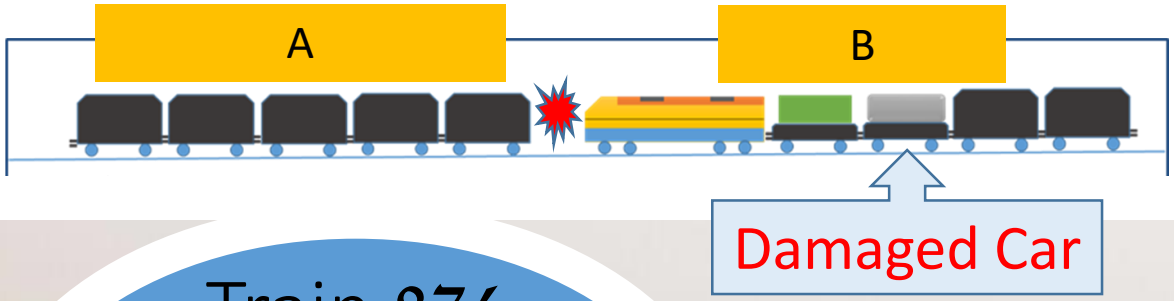
- The curvature of a railroad track
- Communication between active rail personnel

Build

- Stability to real impact of carrying wagons
- Stability to real impact of ISO tanks

Non-Realistic Crash Test – SDCS & SOCS

Second Accident - Collision



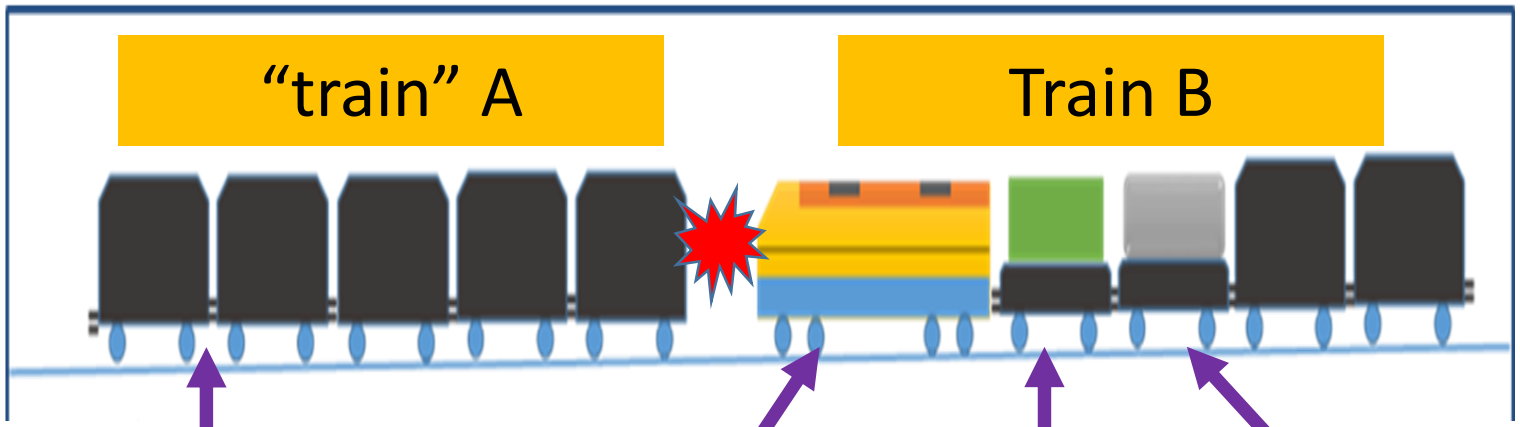
Train 876
(Train A)
"Phosphate Train"

Train 342
(Train B)
"Bromine Train"

Freight car – Train A

Locomotive - Train B

Schematic setup of elements involved in the proximal event



15 Freight cars – Train A

Locomotive - Train B

Emergency Container

Most damaged Freight car – Train B

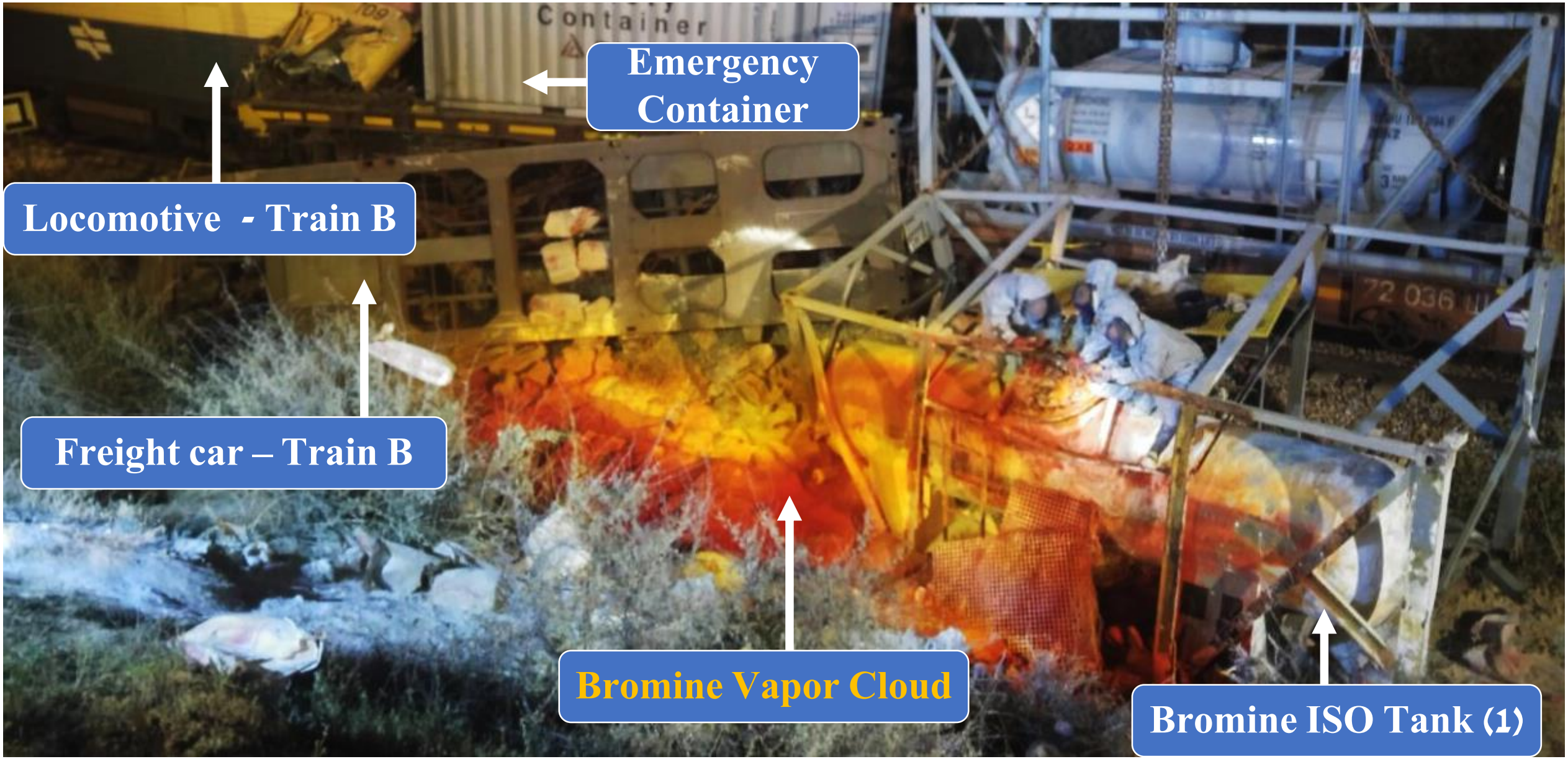
2 Bromine ISO Tanks

Third Accident – Impact to Bromine ISO Tank

The fate of the first Bromine ISO tanks carrying freight car

– Train B

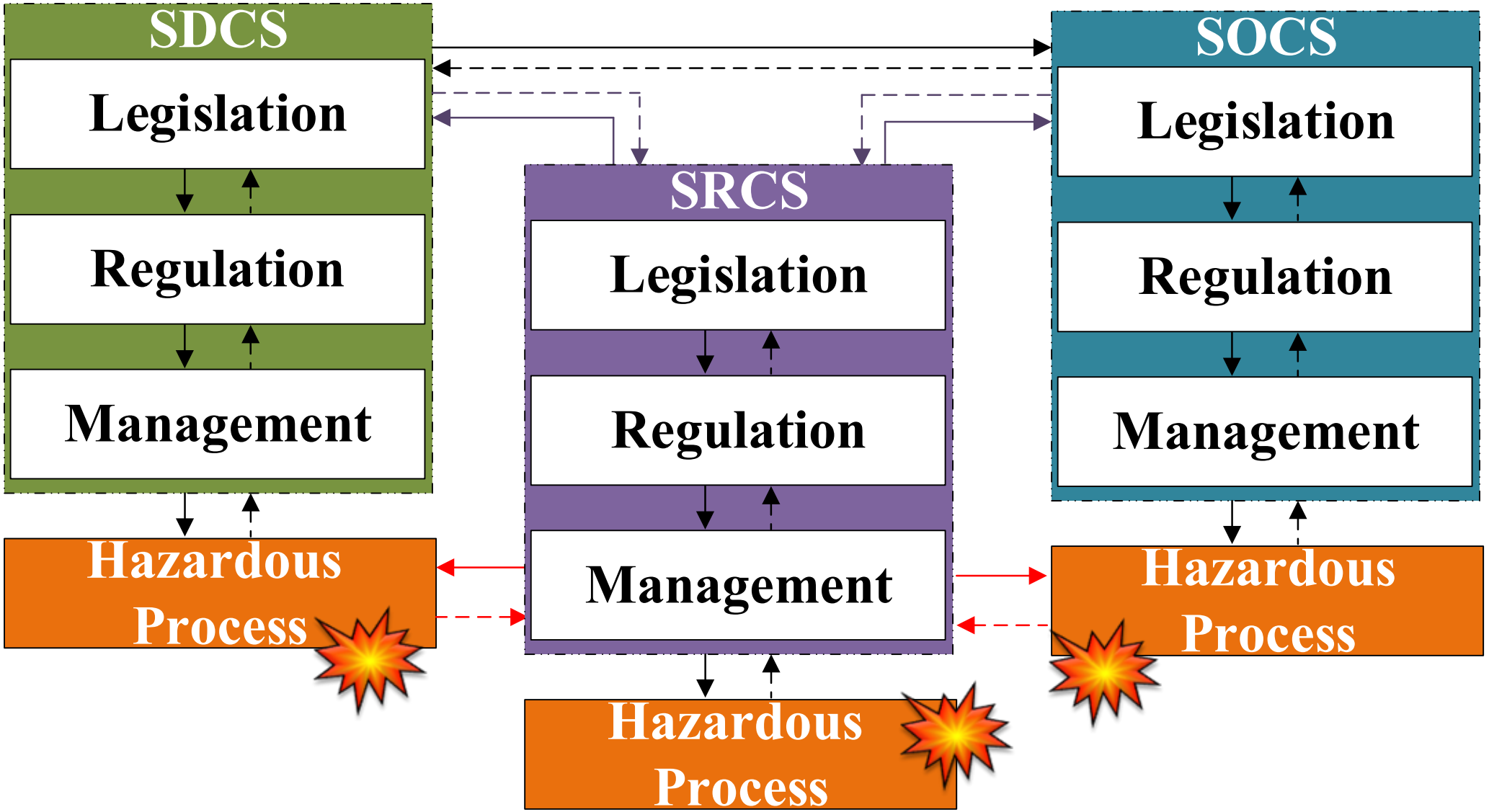
Fourth Accident: uncontrolled Bromine release demands - Emergency Response

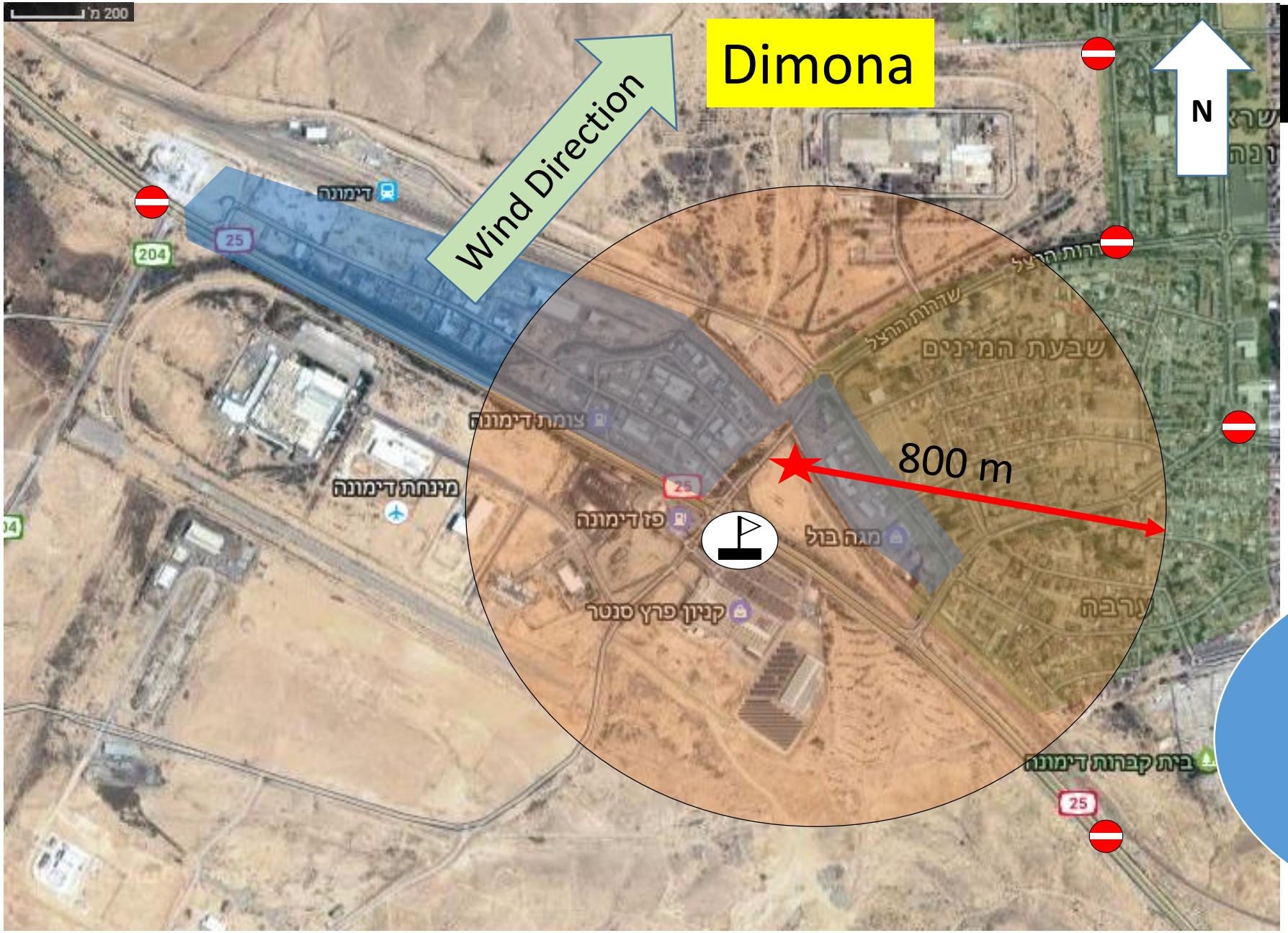


Relationship between Accidents and Disasters

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**

The Complete Sociotechnical System as hierarchical control structures





Theoretical area of Impact

Legend:	
INCIDENT	★
Shelter in-place	
Residential area	
Industrial Zone	
Command post	
Road blockage	

800 m

Radius of Shelter in-place

Emergency Response phase to the trains crash

Identification of accidents and hazards involved in the events

Accident		STSs
Uncontrolled separation of freight cars (train A)	A1	SDCS & SOCS
Collision of Train B in freight cars of Train A	A2	SDCS & SOCS
Damage to the integrity of bromine ISO tank and bromine leakage	A3	SDCS & SOCS
Harm to population due to exposure to hazardous material	A4	SDCS & **SRCS**

Hazards		STSs
A train car may break up uncontrolled from a train	H1	SDCS & SOCS
keeping a minimum distance from another party on the way	H2	SDCS & SOCS
Uncontrolled release of energy	H3	SDCS & SOCS
Uncontrolled damage to structural integrity	H4	SDCS & SOCS
Uncontrolled release of hazardous materials into the environment	H5	SDCS & SOCS
Uncontrolled exposure of the population to hazardous materials	H6	SDCS & **SRCS**

Relationship between System Safety Constraints, Hazards & Accidents

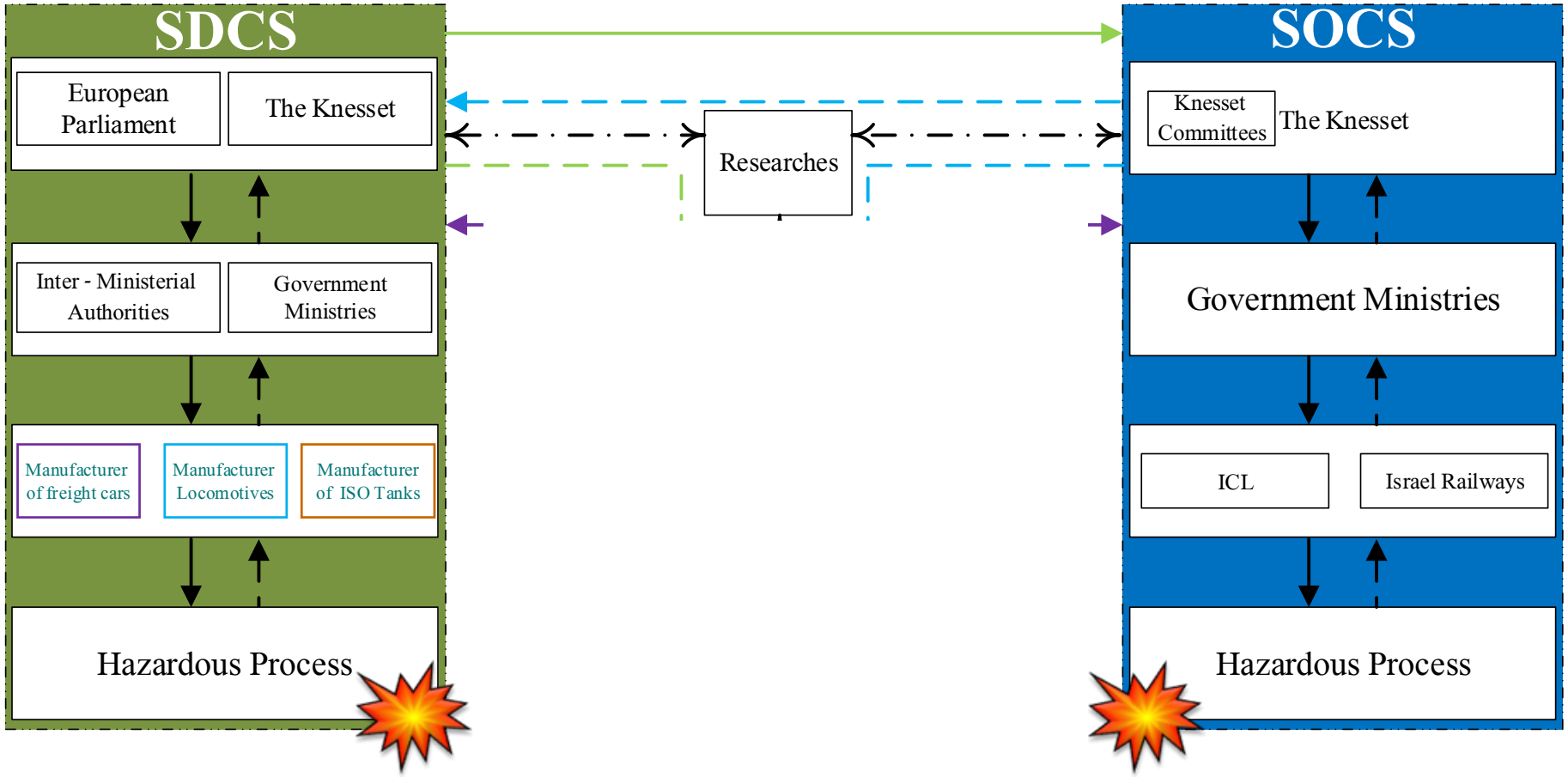
	SSC		Hazards		Accidents	
1	SSC1 **D**	Design of rail transport process must contain controls	H1	A train car may break up uncontrolled from a train	A1	Uncontrolled separation of freight cars (train A)
2	SSC1 **O**	Rail transport must be kept in control all the time				

	SSC		Hazards		Accidents	
1	SSC1 **D**	Design of rail transport process must contain controls	H2	keeping a minimum distance from another party on the way	A2	Collision of Train B in freight cars of Train A
2	SSC1 **O**	Rail transport must be kept in control all the time				
3	SSC2 **D**	Keeping a minimum distance between trains in motion and any other factor on the way must be assimilated in the design of rail operation				
4	SSC2 **O**	Keeping a minimum distance between trains in motion from any other factor on the way must be assimilated in the rail operation				
5	SSC3 **D**	If minimum distance is not maintained, the design of rail operation must take measures				
6	SSC3 **O**	If the minimum distance is not maintained, measures in operation must be taken				
7	SSC4 **D**	Design must control uncontrolled release of energy	H3	Uncontrolled release of energy		
8	SSC4 **O**	Uncontrolled release of energy must be prevented				
9	SSC5 **D**	Uncontrolled exposure to energy must be prevented by design				
10	SSC5 **O**	Uncontrolled exposure to energy must be prevented				
11	SSC6 **D**	If uncontrolled energy is released, measures by design must be taken				
12	SSC6 **O**	If uncontrolled energy is released, measures in operation must be taken				

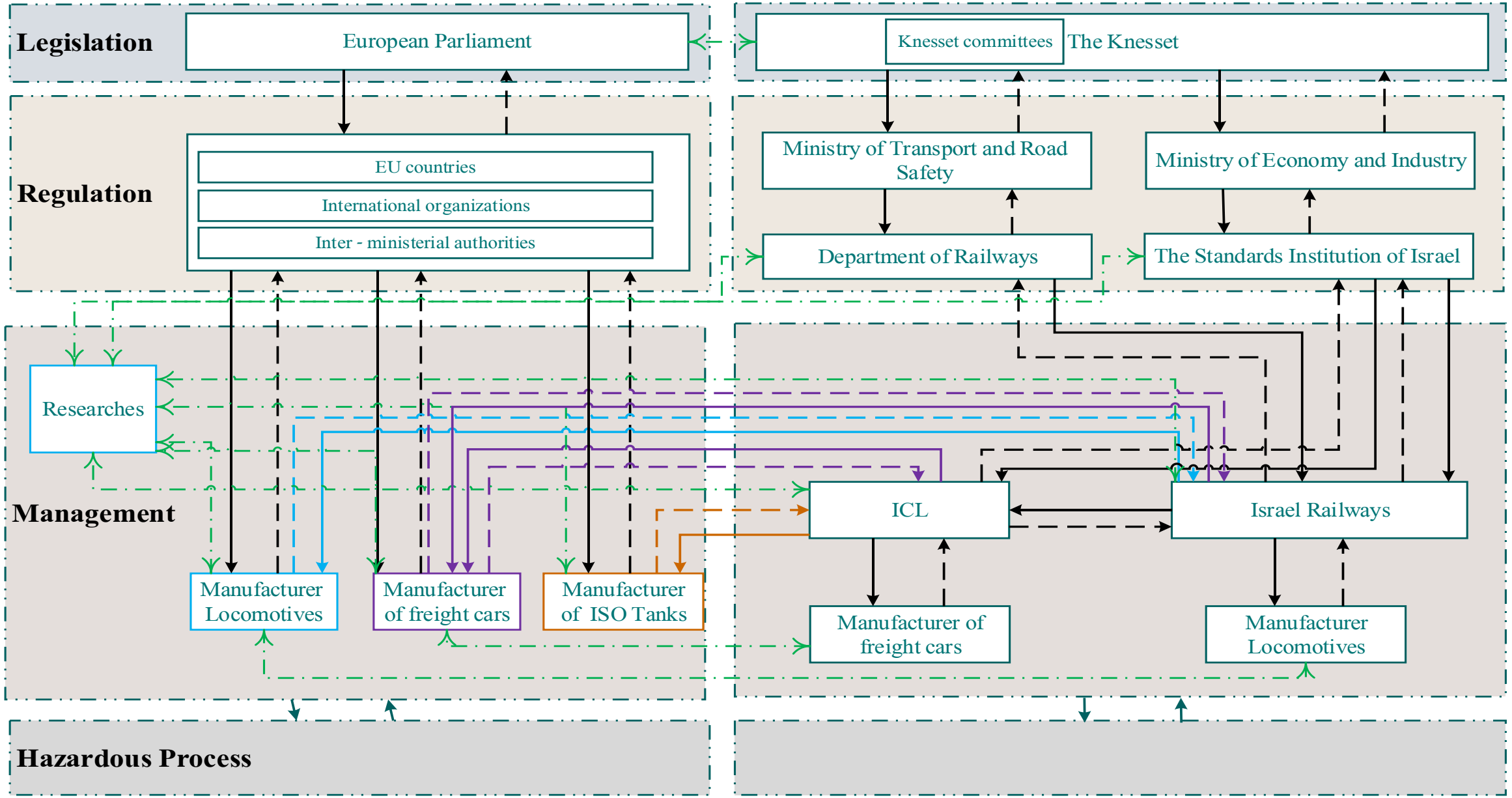
	SSC		Hazards		Accidents	
7	SSC4 **D**	Design must control uncontrolled release of energy	H3	Uncontrolled release of energy	A3	Damage to the integrity of Bromine ISO tank and Bromine leakage
8	SSC4 **O**	Uncontrolled release of energy must be prevented				
9	SSC5 **D**	Uncontrolled exposure to energy must be prevented by design				
10	SSC5 **O**	Uncontrolled exposure to energy must be prevented				
11	SSC6 **D**	If uncontrolled energy is released, measures by design must be taken				
12	SSC6 **O**	If uncontrolled energy is released, measures in operation must be taken				
13	SSC7 **D**	Design must prevent uncontrolled damage to the structural integrity of the carrier of hazardous materials	H4	Uncontrolled damage to structural integrity		
14	SSC7 **O**	Operation must prevent uncontrolled damage to the structural integrity of the carrier of hazardous materials				
15	SSC8 **D**	Uncontrolled release of hazardous materials into the environment must be implemented by design	H5	Uncontrolled release of hazardous materials into the environment		
16	SSC8 **O**	Uncontrolled release of hazardous materials into the environment must be prohibited				
17	SSC8 **R**	If uncontrolled released of hazardous materials occurs, measures must be taken				
18	SSC9 **D**	Epicenter of an uncontrolled hazardous materials release must be contained by design				
19	SSC9 **R**	Epicenter of an uncontrolled hazardous materials release must be contained by design				

	SSC		Hazards		Accidents	
15	SSC8 **D**	Uncontrolled release of hazardous materials into the environment must be implemented by design	H 5	Uncontrolled release of hazardous materials into the environment	A 4	Harm to population due to exposure to hazardous material
16	SSC8 O	Uncontrolled release of hazardous materials into the environment must be prohibited				
17	SSC8 **R**	If uncontrolled released of hazardous materials occurs, measures must be taken				
18	SSC9 **D**	Epicenter of an uncontrolled hazardous materials release must be contained by design				
19	SSC9 **R**	Epicenter of an uncontrolled hazardous materials release must be contained				
20	SSC10 **D**	Uncontrolled exposure of the population to hazardous materials must be prohibited by design	H 6	Uncontrolled exposure of the population to hazardous materials		
21	SSC10 **R**	Uncontrolled exposure of the population to hazardous materials must be prohibited				
22	SSC11 **D**	Measures by design must be taken if the population is exposed to hazardous materials				
23	SSC11 **R**	Measures must be taken if the population is exposed to hazardous materials				

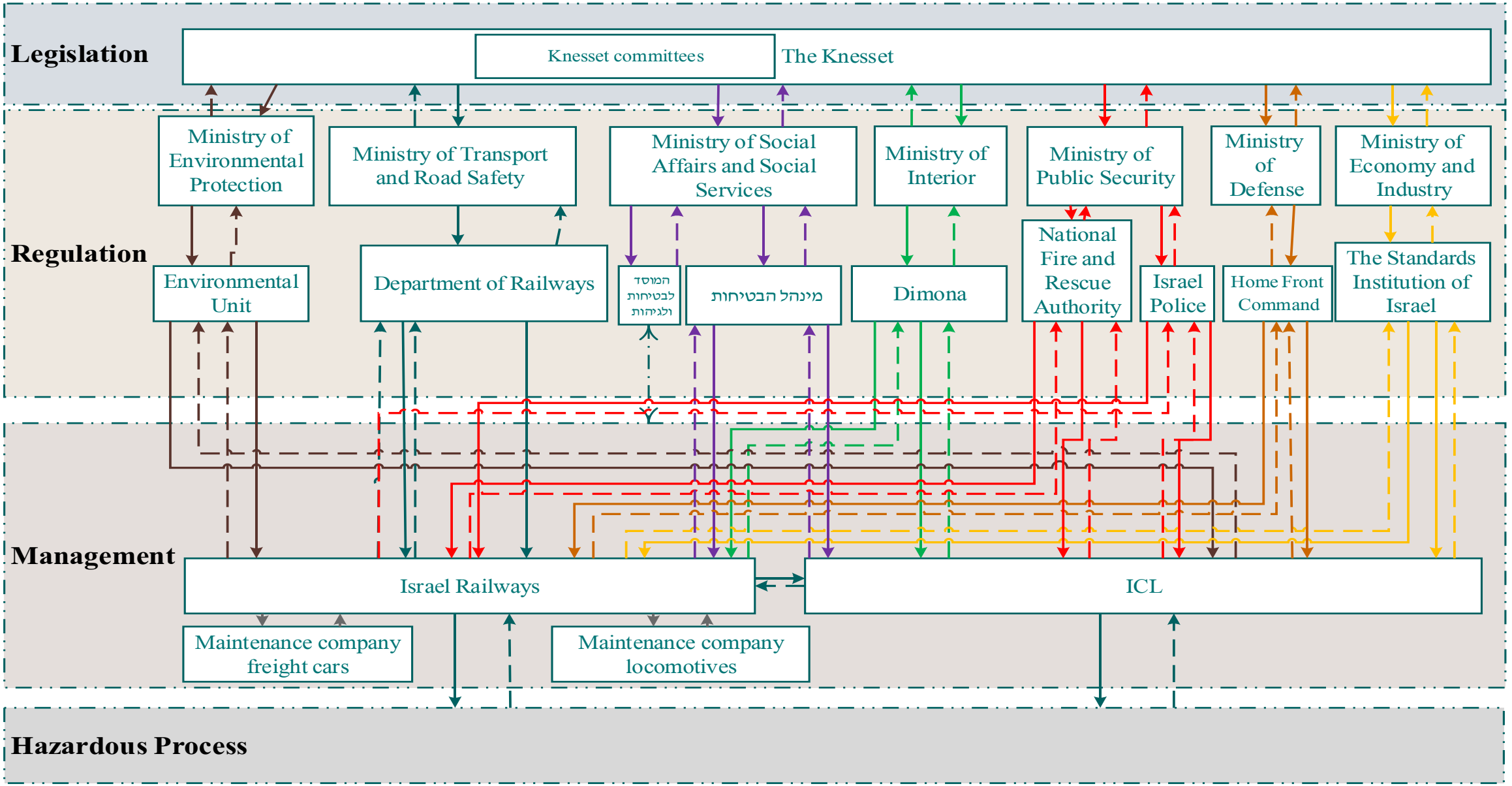
The Sociotechnical System as hierarchical control structures (Leveson)



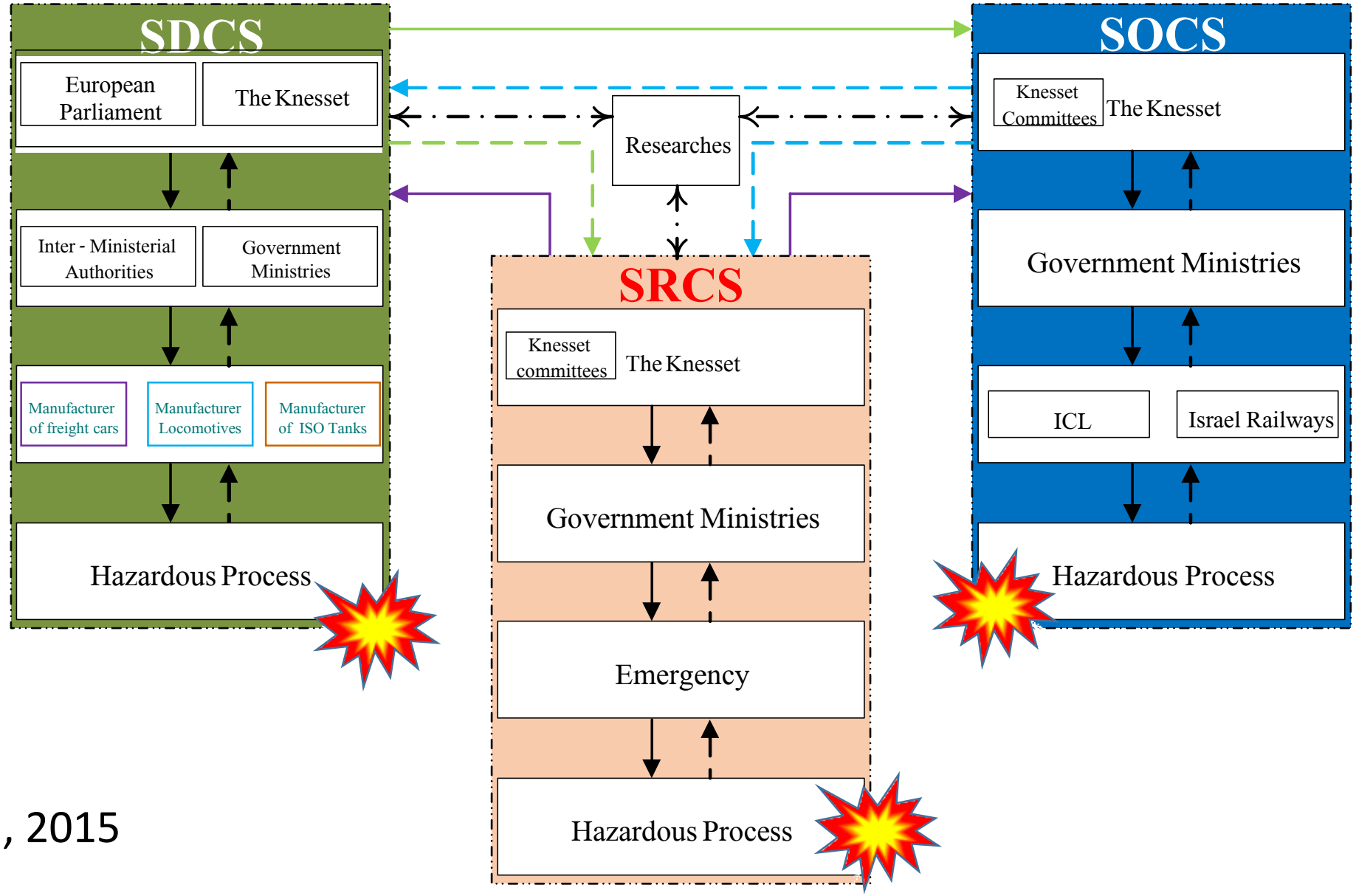
The Hierarchical Functional Safety Development Control Structure



The Hierarchical Functional Safety Operation Control Structure

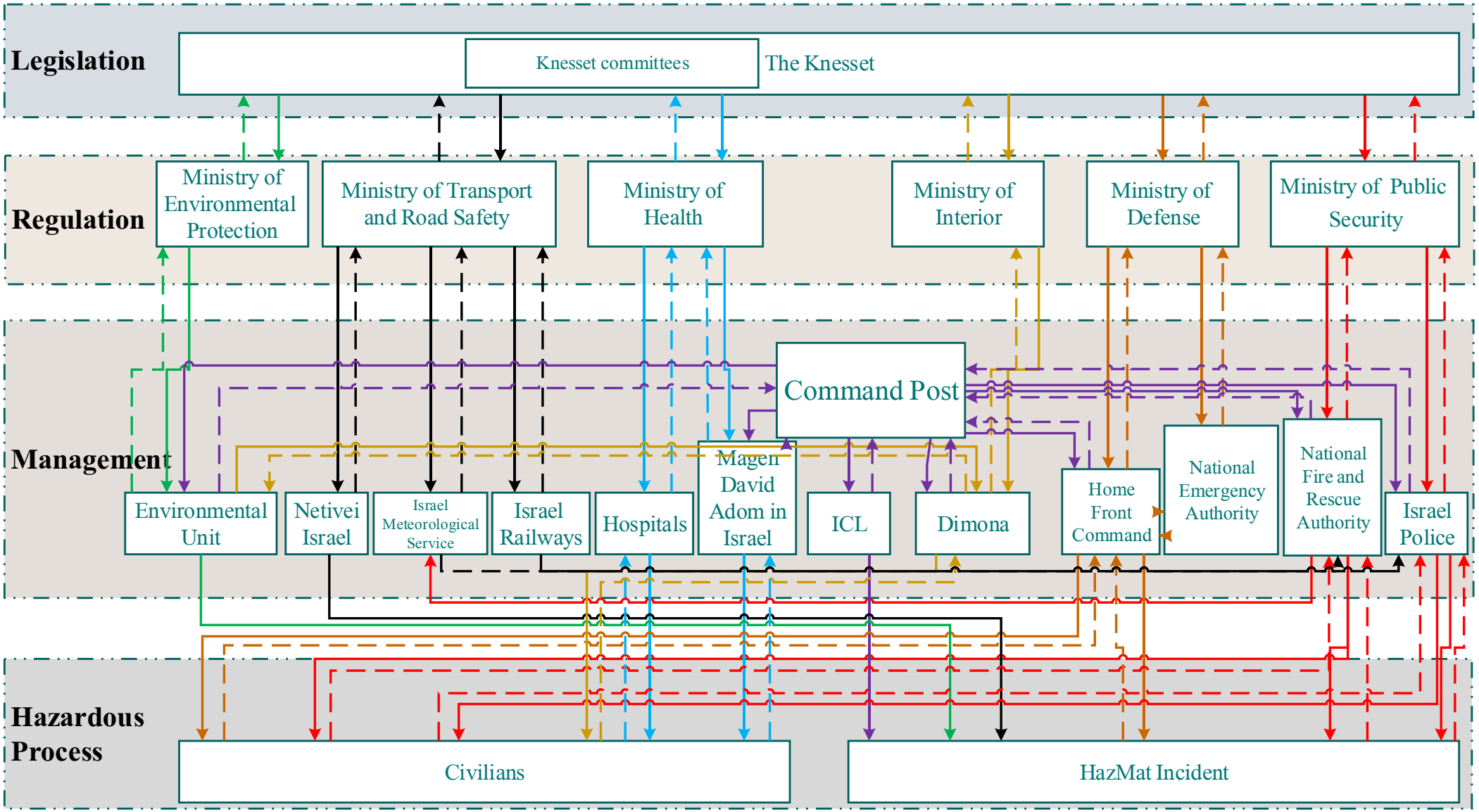


The Complete Sociotechnical System as hierarchical control structures

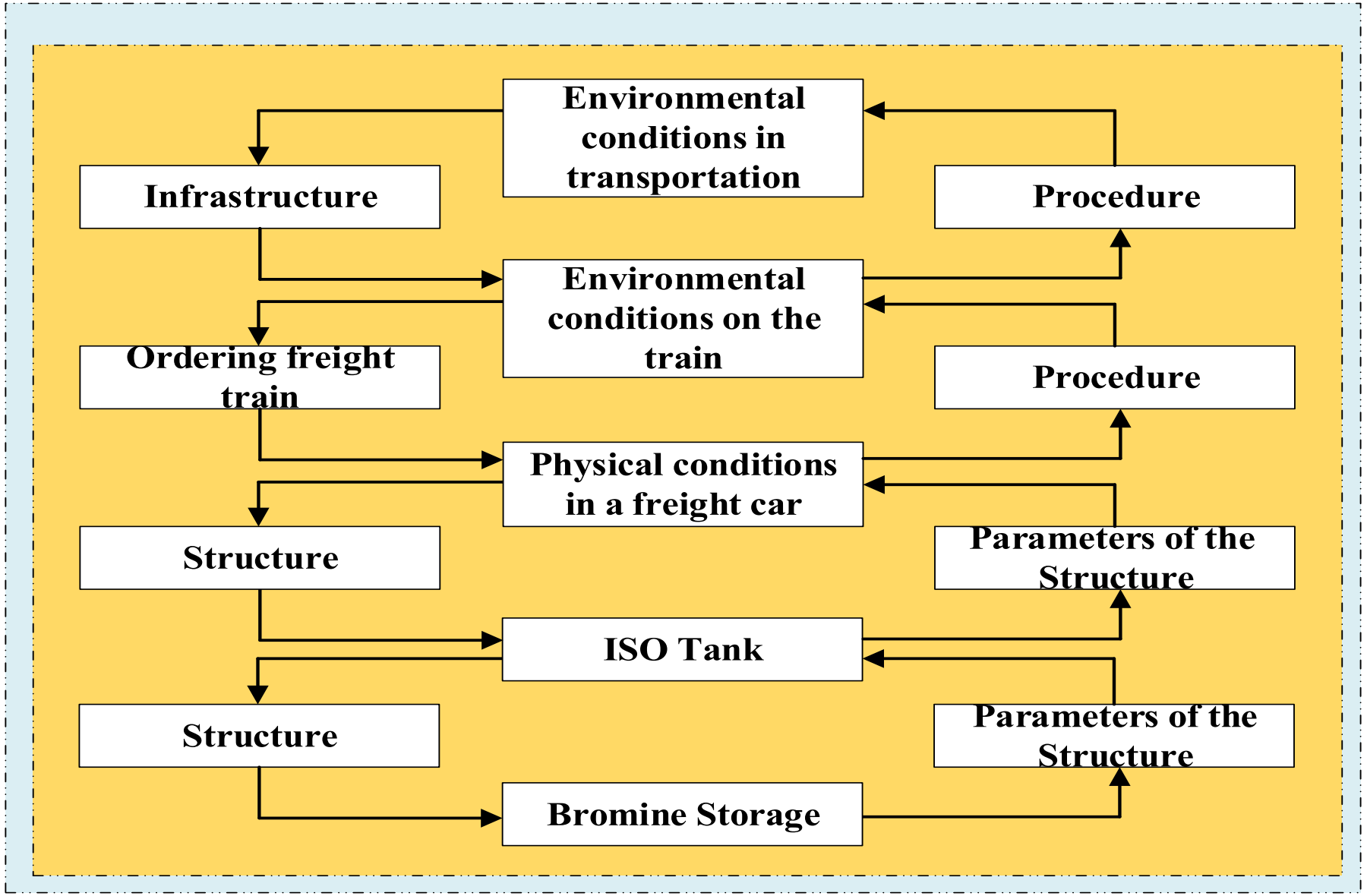


Hartmann, 2015

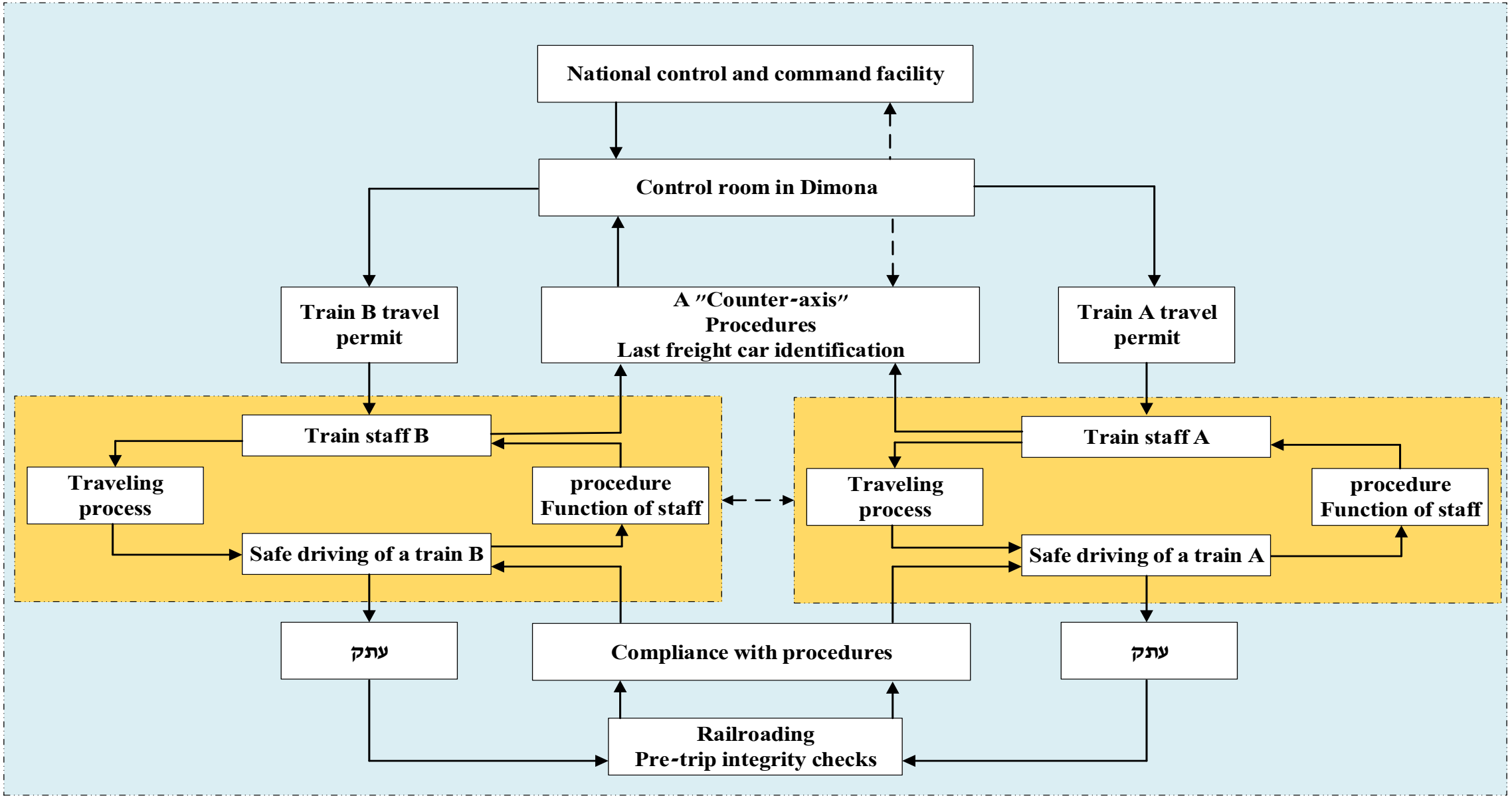
The Hierarchical Functional Safety Respond Control Structure



Physical Level of the System Development Control Structure



Physical Level of the System Operation Control Structure



Comparison: Official & CAST Investigations Results

Level in STS	Official Investigation	CAST Analysis
Legislation	0	6
Regulation	0	9
Management	4	10
Physical	6	24
Interactions	0	8
Total Results	10	57

General Conclusions as to SDCS Physical Level

- Very complex and worldwide dispersed Sociotechnical control structures.
- The organizations involved do not understand the full range of hazards and their potential consequences.
- No clearly defined Accountability and Responsibility in the SDCS.
- Structural weakness causing inconsistency in collecting and processing critical data, long-term and in real time.
- Synchronization and Coordination problems due to structural problems.

General Conclusions as to **SDCS** Upper Levels

- In Israel: Inefficient, bureaucratic Sociotechnical system.
- Regulations are outdated, inefficient and not involved in real life.
- A chronic shortage of resources to carry out policy.
- No ability nor effective inspection and enforcement.
- No change and / or drift management, and no understanding of their meaning regarding safety impact on the systems.

General Conclusions from **SOCS** Physical Level

- The organizations and persons involved do not understand the full range of hazards and their potential consequences.
- Israel Rail & ICL: No clearly defined Accountability and Responsibility in the SOCS.
- Structural weakness causing inconsistency in collecting and processing data in long-term and real time.
- Synchronization and Coordination problems due to structural problems.

General Conclusions from **SOCS** Upper Levels

- In Israel: Inefficient, bureaucratic Sociotechnical system.
- Regulations are outdated, inefficient and not involved in in real life.
- A chronic shortage of resources to carry out policy.
- No effective inspection and enforcement.
- No change and / or drift management, and no understanding of their meaning regarding safety impact on the systems.

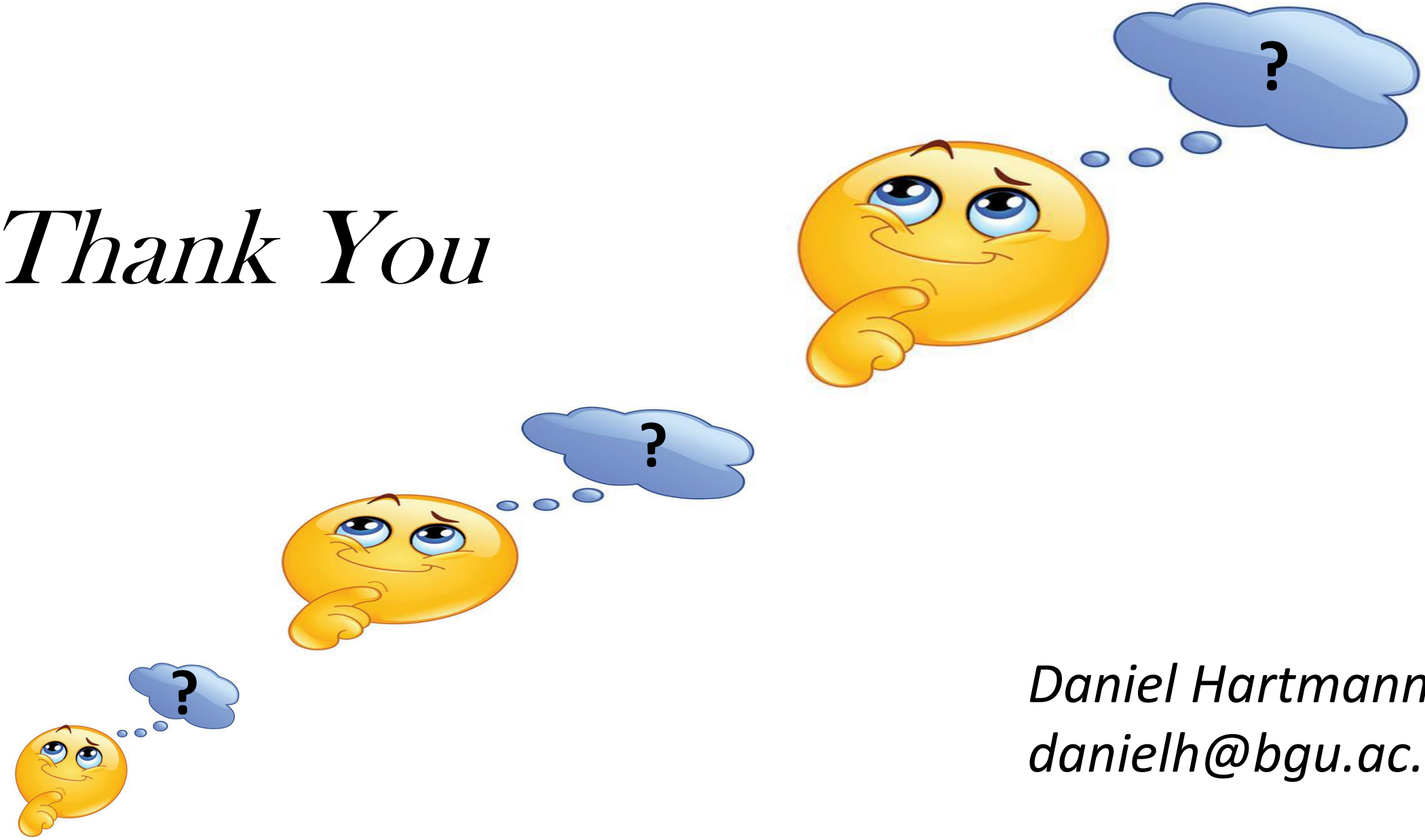
Lessons Learned

- The need for **Evidence Based Safety**:

➢ To achieve a “safer world”, input from analysis of accidents and any other “loss-events” is crucial for any system hazard analysis.

- The entire Sociotechnical System comprising of **SDCS**, **SOCS** and **SRCS** and all their interactions should be considered and analyzed.
- Apart of the Physical level, most upper levels in the Socio-Technical System can contribute **generic** Hazards, Safety Constrains and problems that can be defined and contribute to any Hazard analysis of similar systems and domains of operation.
- The importance of Hazard analysis for any crucial **change** in systems.

Thank You



Daniel Hartmann
danielh@bgu.ac.il