# A Meta-analysis of CAST Investigations of Accidents Related to Diverse Sociotechnical Systems (STSs)

**Daniel Hartmann, PhD**

Management & Safety Engineering Unit,

Ben-Gurion University, Israel

# Outline

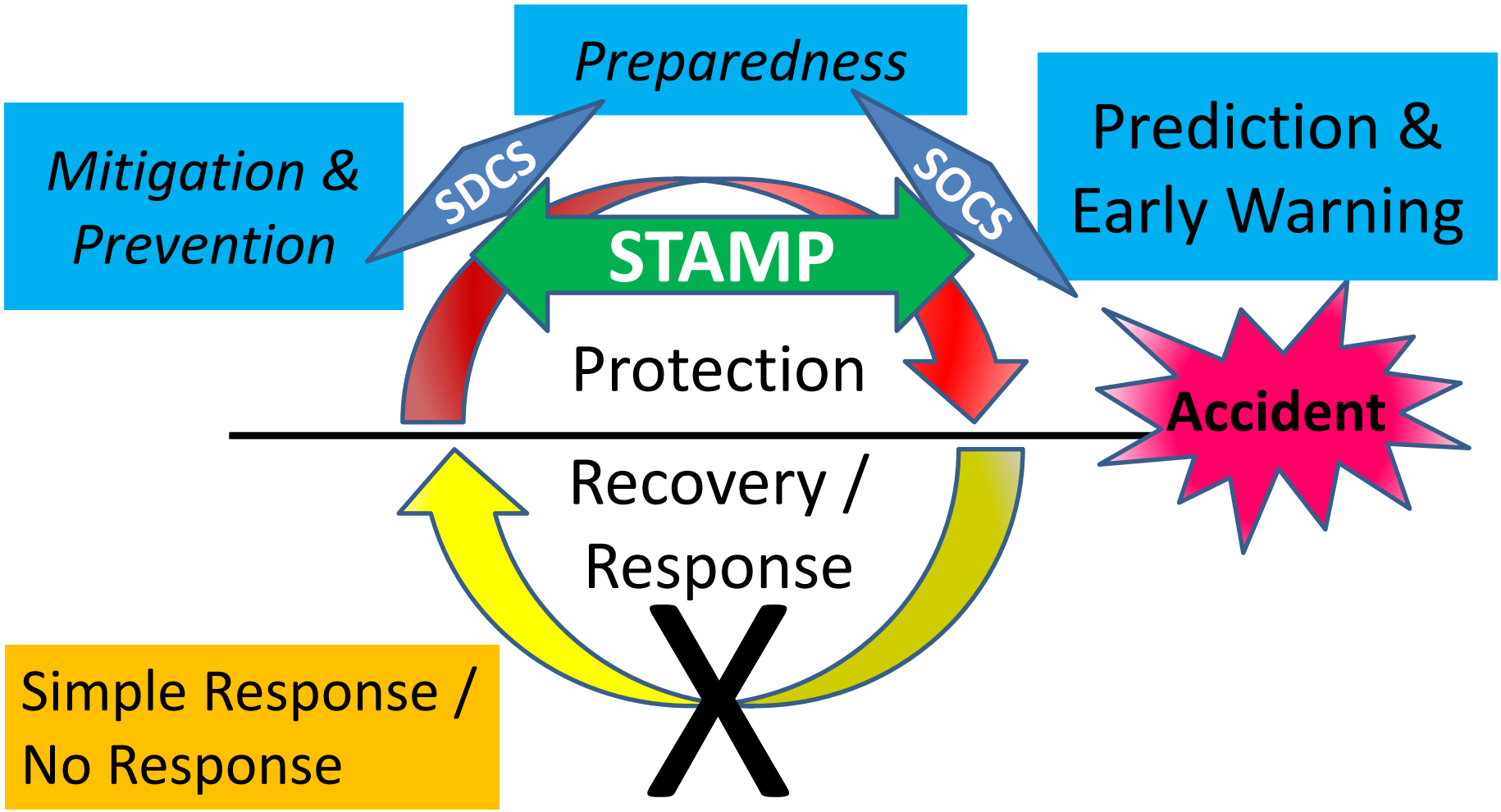
- ✓ Short Introduction to “my ideas”
- Short Description of Accidents
- Some Preliminary Thoughts and Ideas

# A very crude and bold Assumption

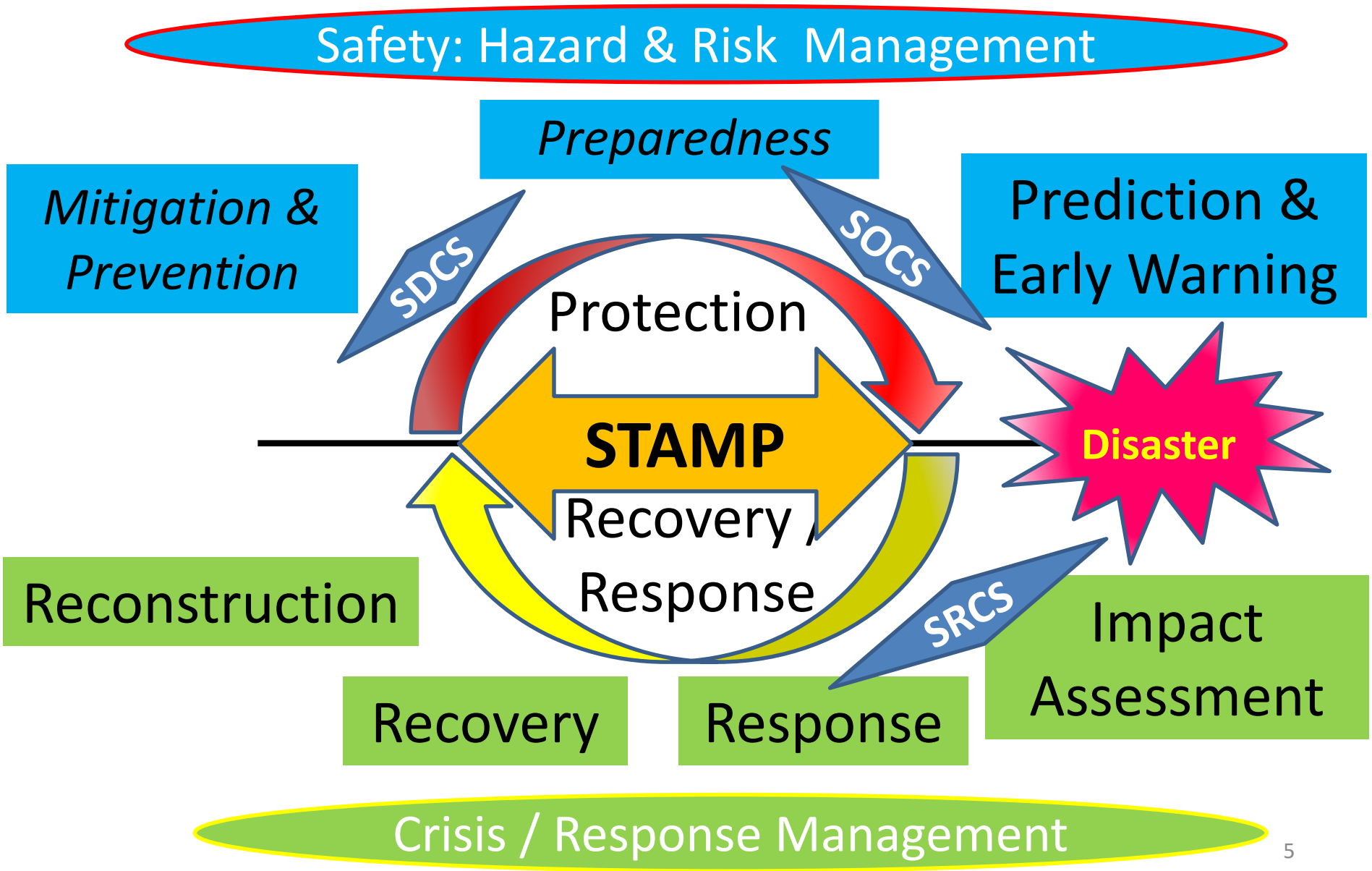
| New Socio-technical Systems | Old, well established Socio-technical Systems |
|---|---|
| *< 0.1 %* | *>99.9%* |
| STPA needed, but… | STAMP & STPA not wanted as long as… |

# Loss Event / Accident Lifecycle

Safety: Hazard & Risk Management

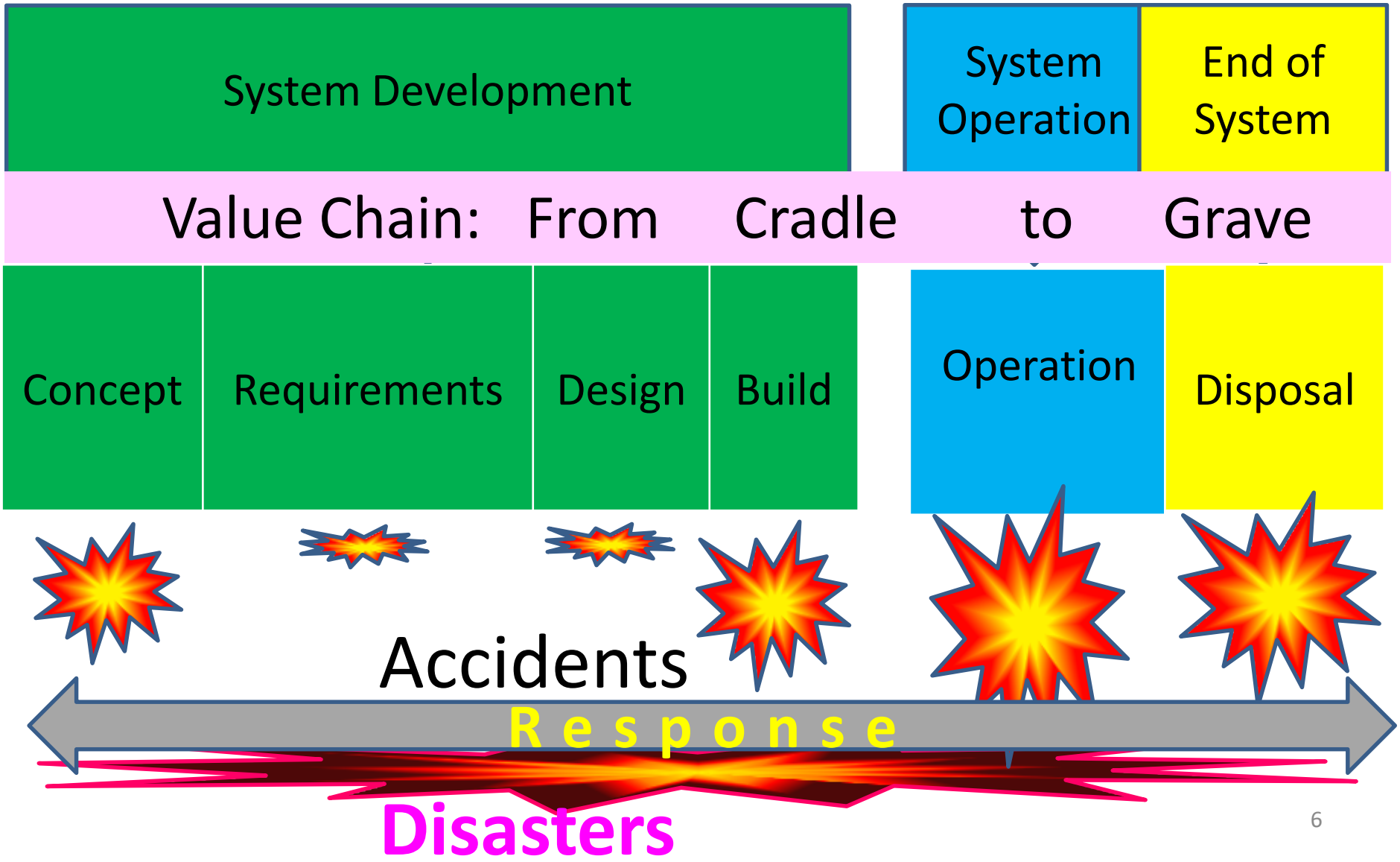


# Disaster / Accident / Loss Event Lifecycle



# STAMP, Sociotechnical Systems Lifecycle

## Safety, Accidents & Disasters

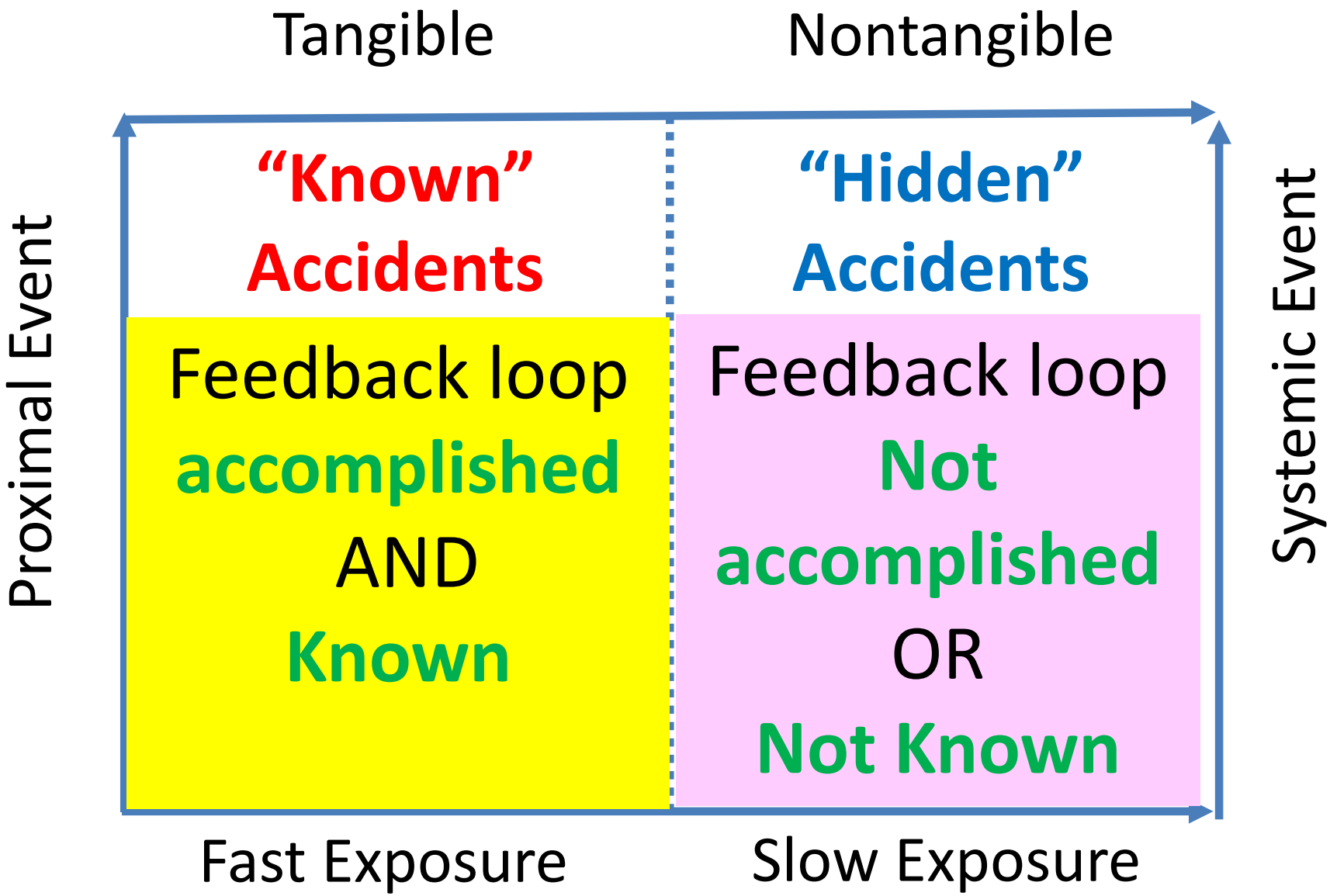


# A New view of **Loss Events** Classification

# 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** |

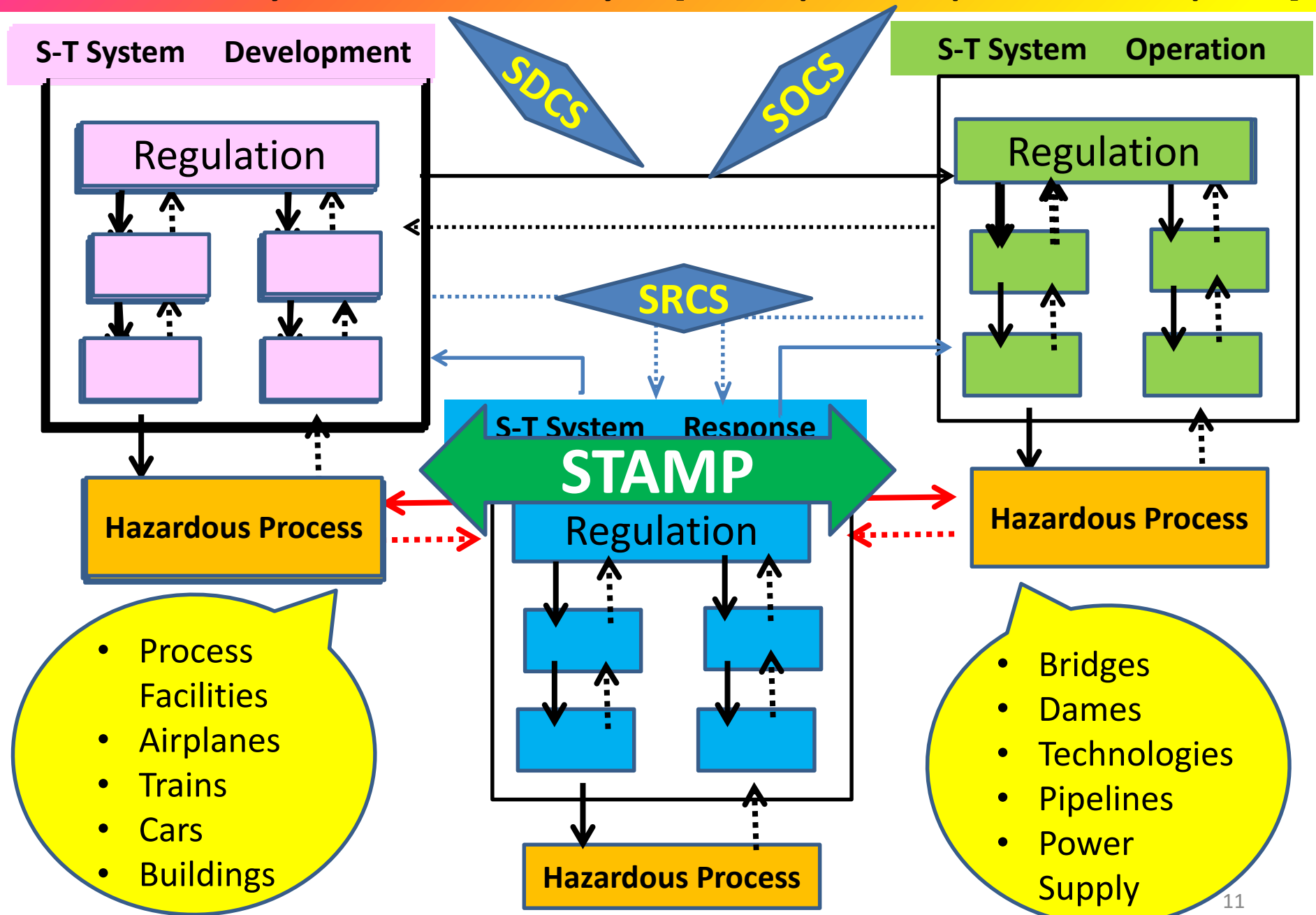
# Another view of **Accidents Classification**



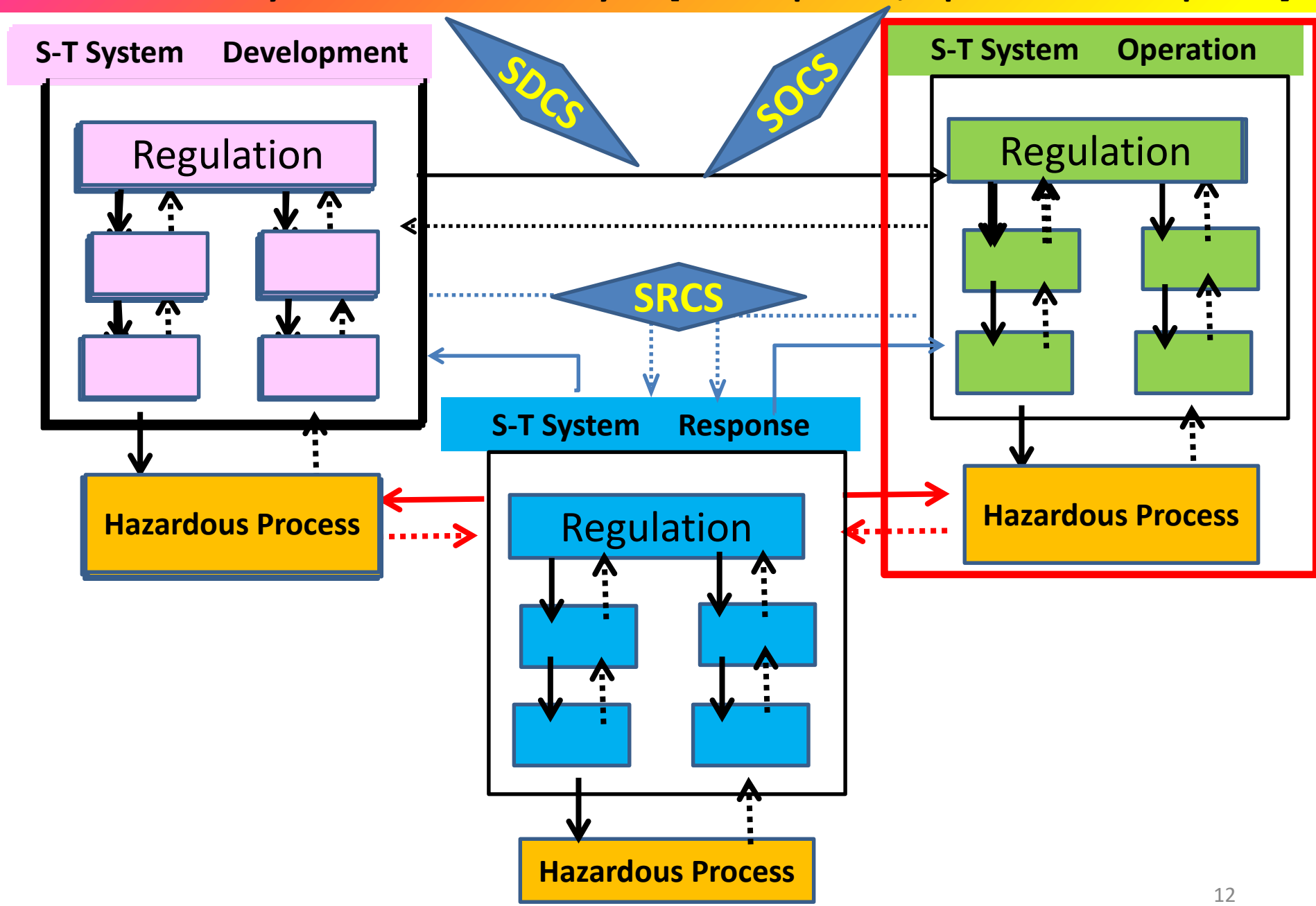
# Some Sociotechnical Domains with Hidden Accidents

- **Justice System**
  - **Criminal Justice**
- **Health Systems**
  - **Health treatment**
  - **Drug treatment**
- **Nourishment System**
  - **Critical Food**
  - **Food**
  - **Water / Beverage**
- **Environmental System**
- **[bad] Decisions Making**

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



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



# Stages in System Operation Control Structure (SOCS)

- **System (new) Initiation (Stephanie)**
- **System Routine Operation**
- **System Non-Routine Operation (Kanarit)**
- System Shutdown
- System Maintenance
- System Repairs
- **System Startup** (after Maintenance / Repairs)

# 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 | Complex "Corporate" Management |
| Company Management | Company Management | Complex "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 |

# Outline

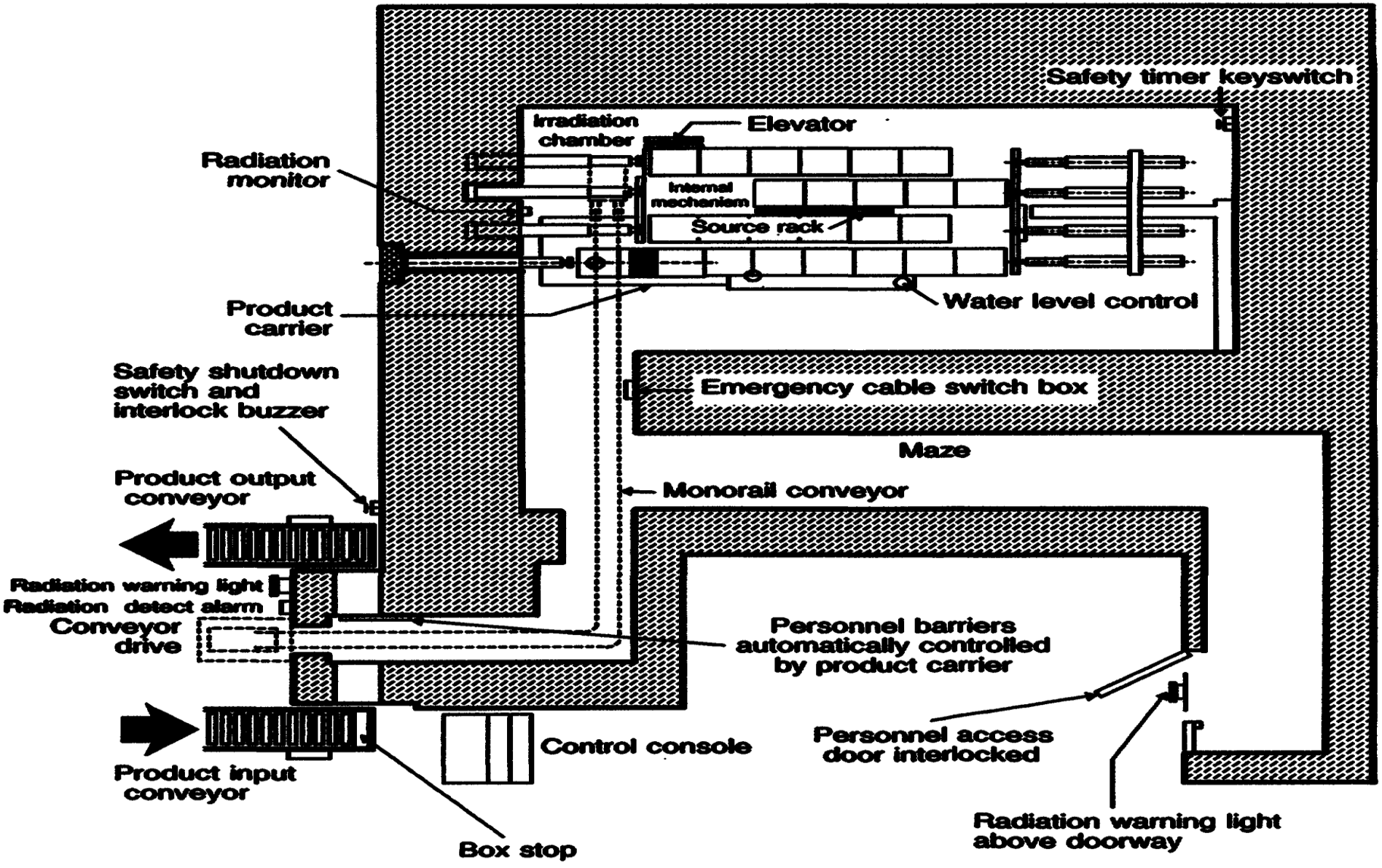
- ✓ Short Introduction to “my ideas”
- ✓ Short Description of Accidents
- Some Preliminary Thoughts and Ideas

# The Radiological Accident in Soreq

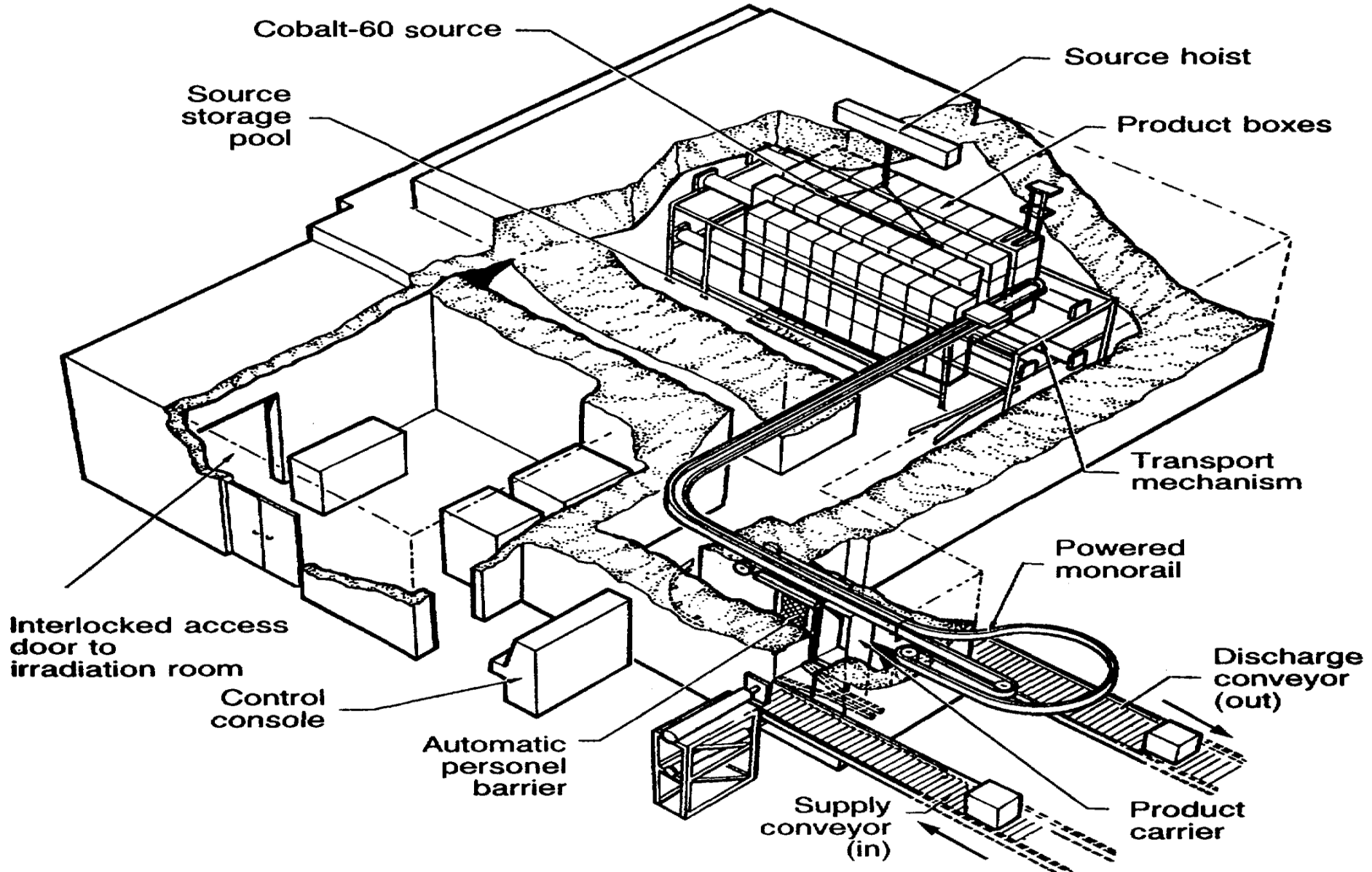
An Accident in a System Operation Control Structure (SOCS) - System Routine Operation

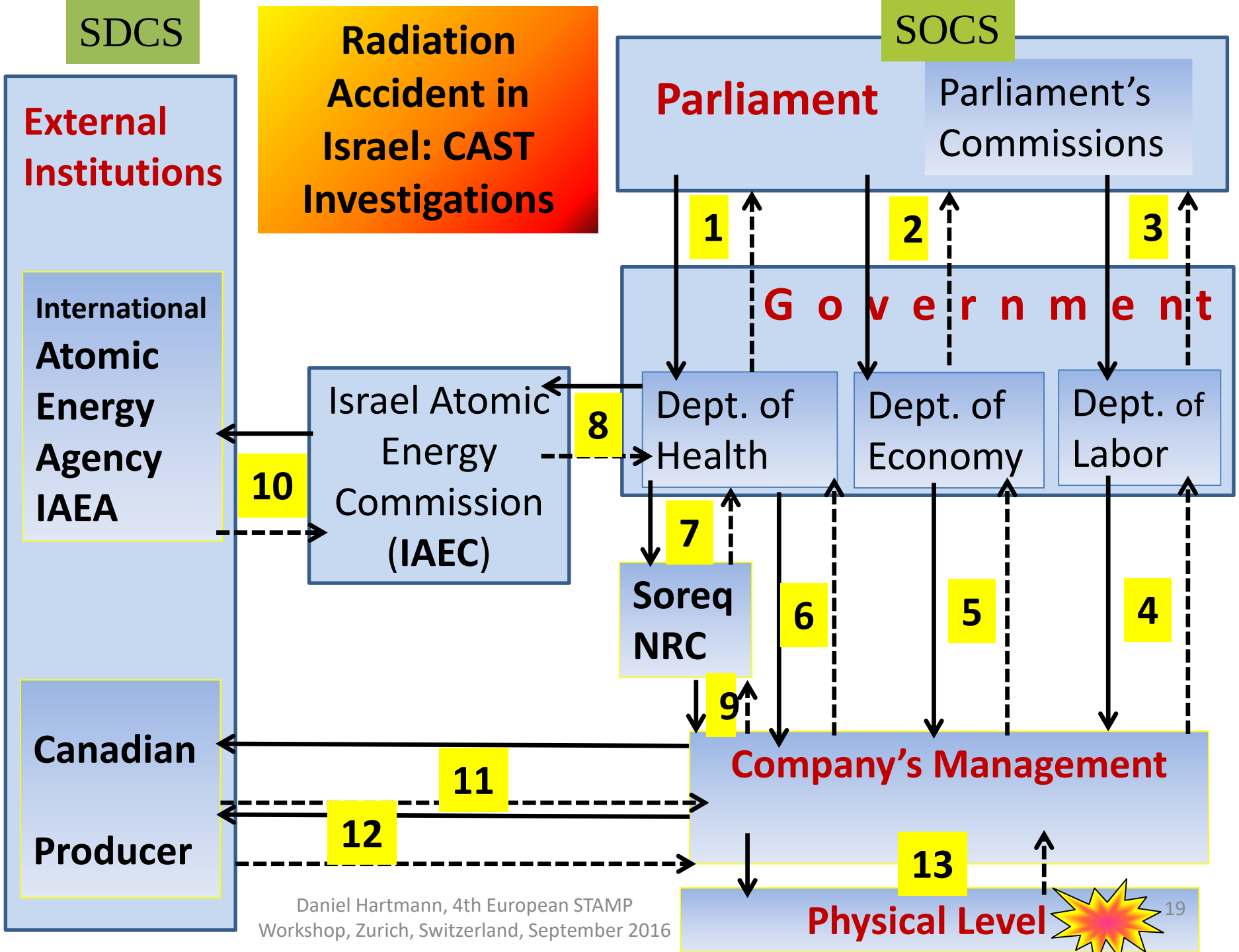
IAEA

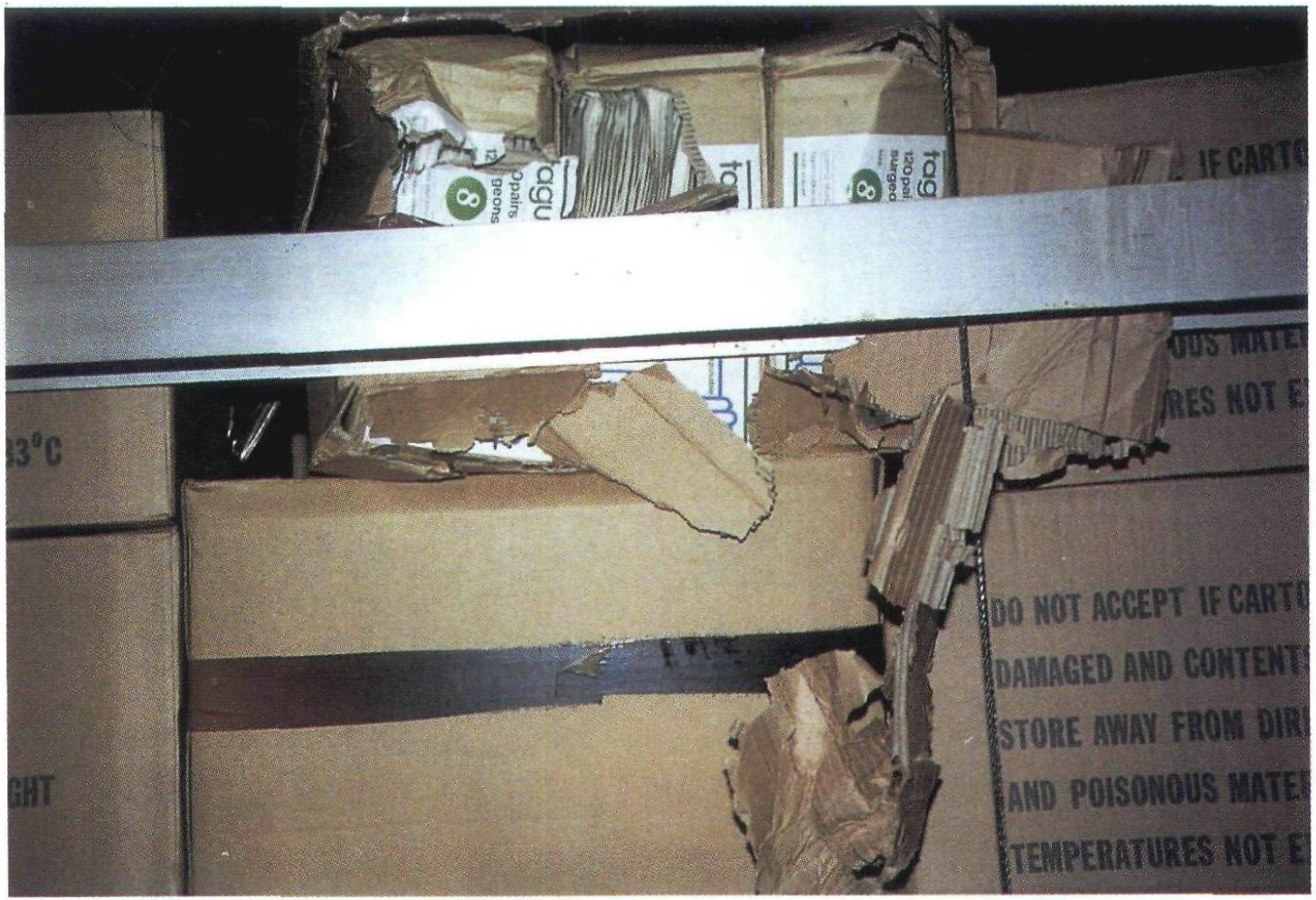
# A floor plan of the irradiation facility and JS6500 irradiator



# A cutaway three dimensional diagram of the JS6500 irradiator and the irradiation facility



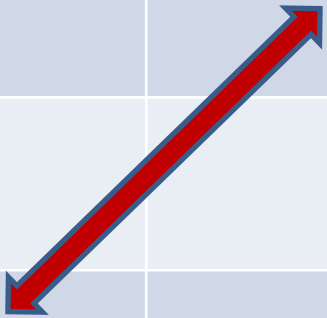

SDCS
Radiation Accident in Israel: CAST Investigations
SOCS
External Institutions
Parliament
Parliament's Commissions
1
2
3
G o v e r n m e n t
International Atomic Energy Agency IAEA
10
Israel Atomic Energy Commission (IAEC)
8
Dept. of Health
Dept. of Economy
Dept. of Labor
7
Soreq NRC
6
5
4
9
Canadian
Producer
11
12
Company's Management
13
Physical Level




3. The carton on the inner lower conveyor that obstructed the source rack. Also shown are the steel guide bar and the source hoist cable.

# 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% |



# Accident's Dimensions

- **Time**:
  - Proximal Event: Seconds – Minutes
  - t Δ between Design and Accident: > 20 years
- **Space**: few square meters
- **Severity**
  - Tangible & Direct: **One** fatality
  - Intangible & Indirect: N/A
- **Complexity**
  - Internal (PE): very Simple
  - External (SOCS): very Simple
- **Response:** very Simple

# An Accident in a System Operation Control Structure Within the SOCS stage: System Startup (after Maintenance / Repairs)

# View of D/E/F NHT Heat Exchanger Bank Before Accident (CSB Animation)

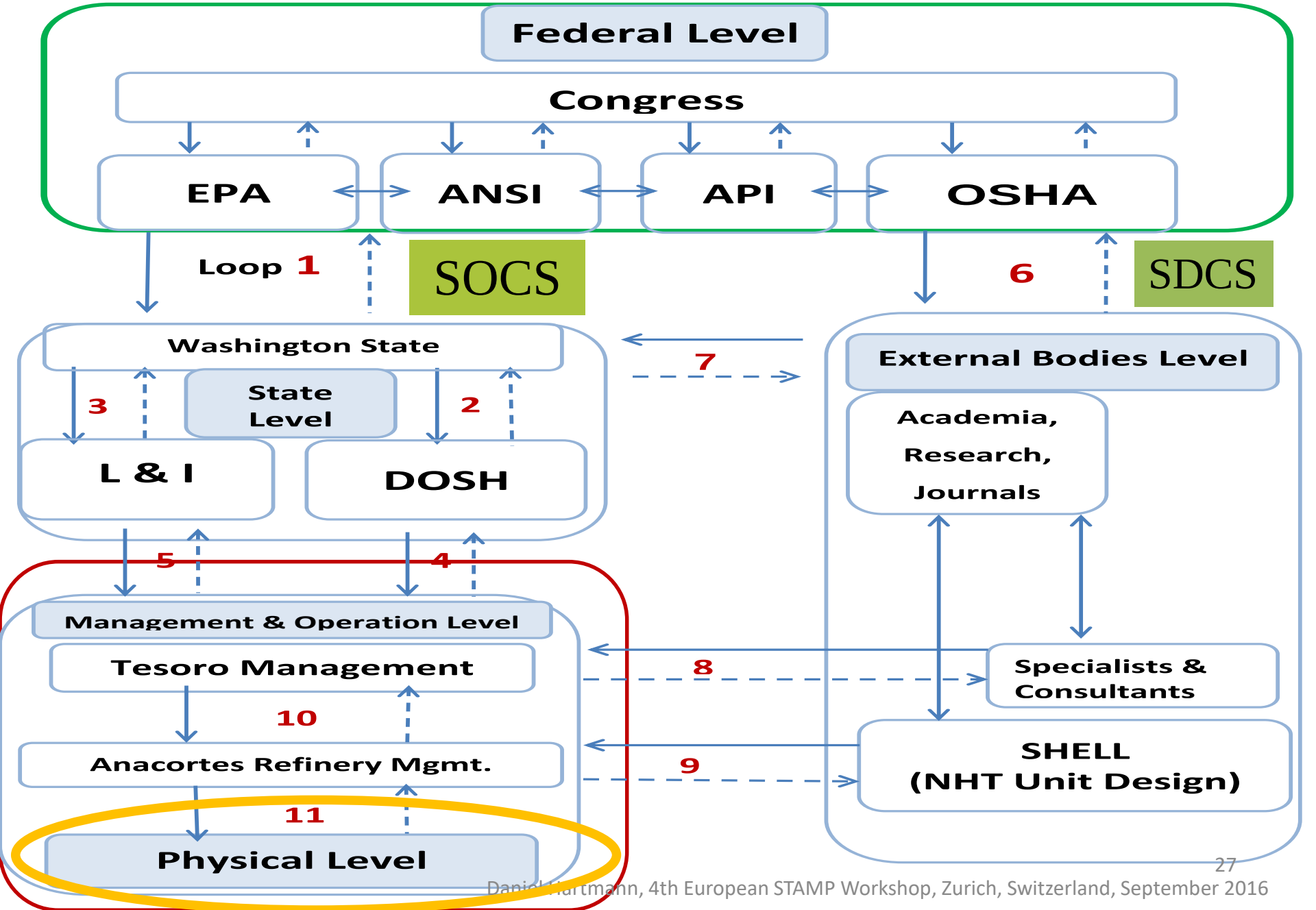
# Catastrophic Rupture of Heat Exchanger (Seven Fatalities)

## Tesoro Anacortes Refinery

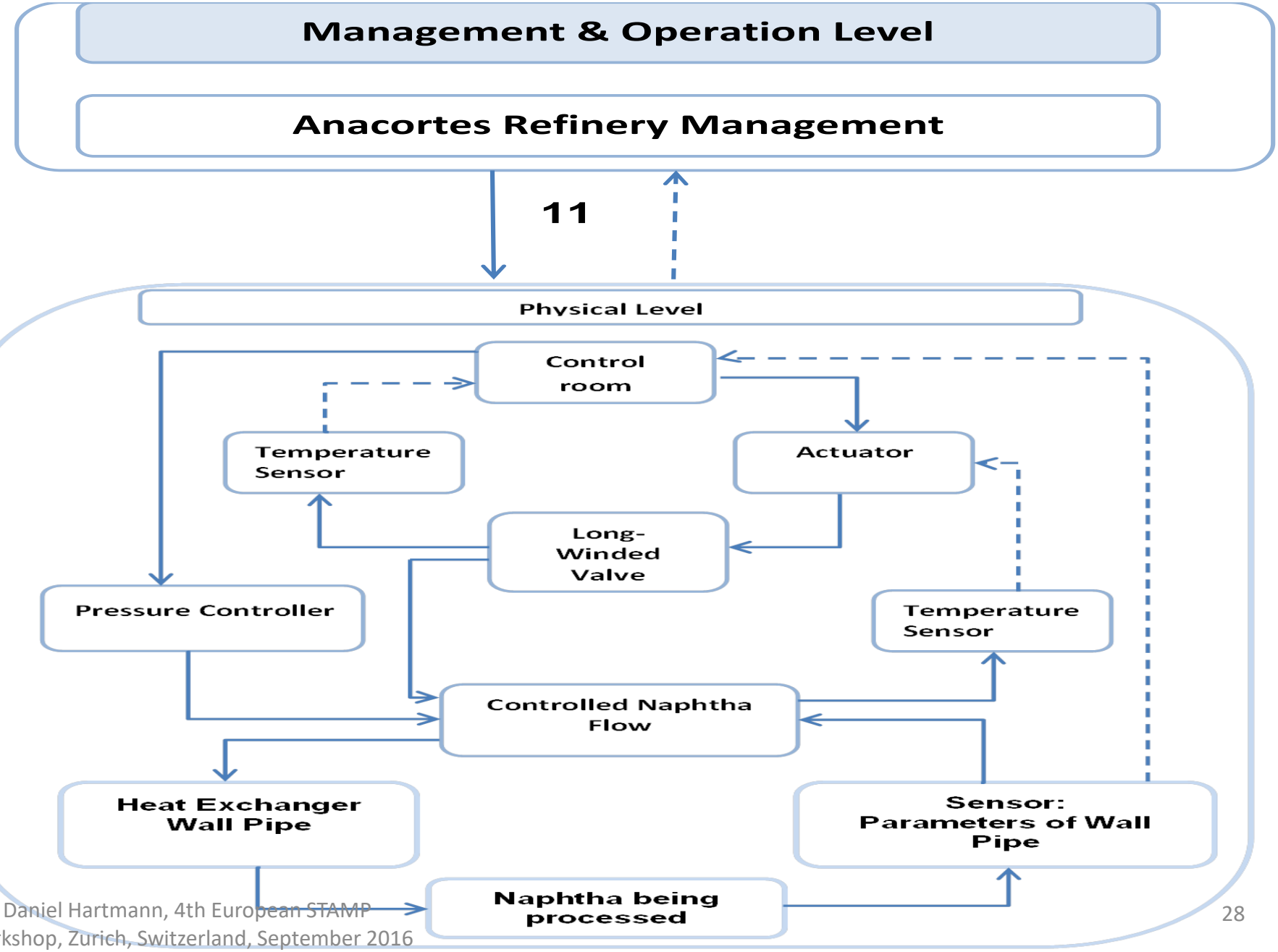
Anacortes, Washington (State), April 2, 2010

# Post-Incident View of D/E/F NHT Heat Exchanger Bank

# Sociotechnical Hierarchical control Structure – Anacortes Accident



# Sociotechnical Hierarchical control Structure – Anacortes Accident



# 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% |

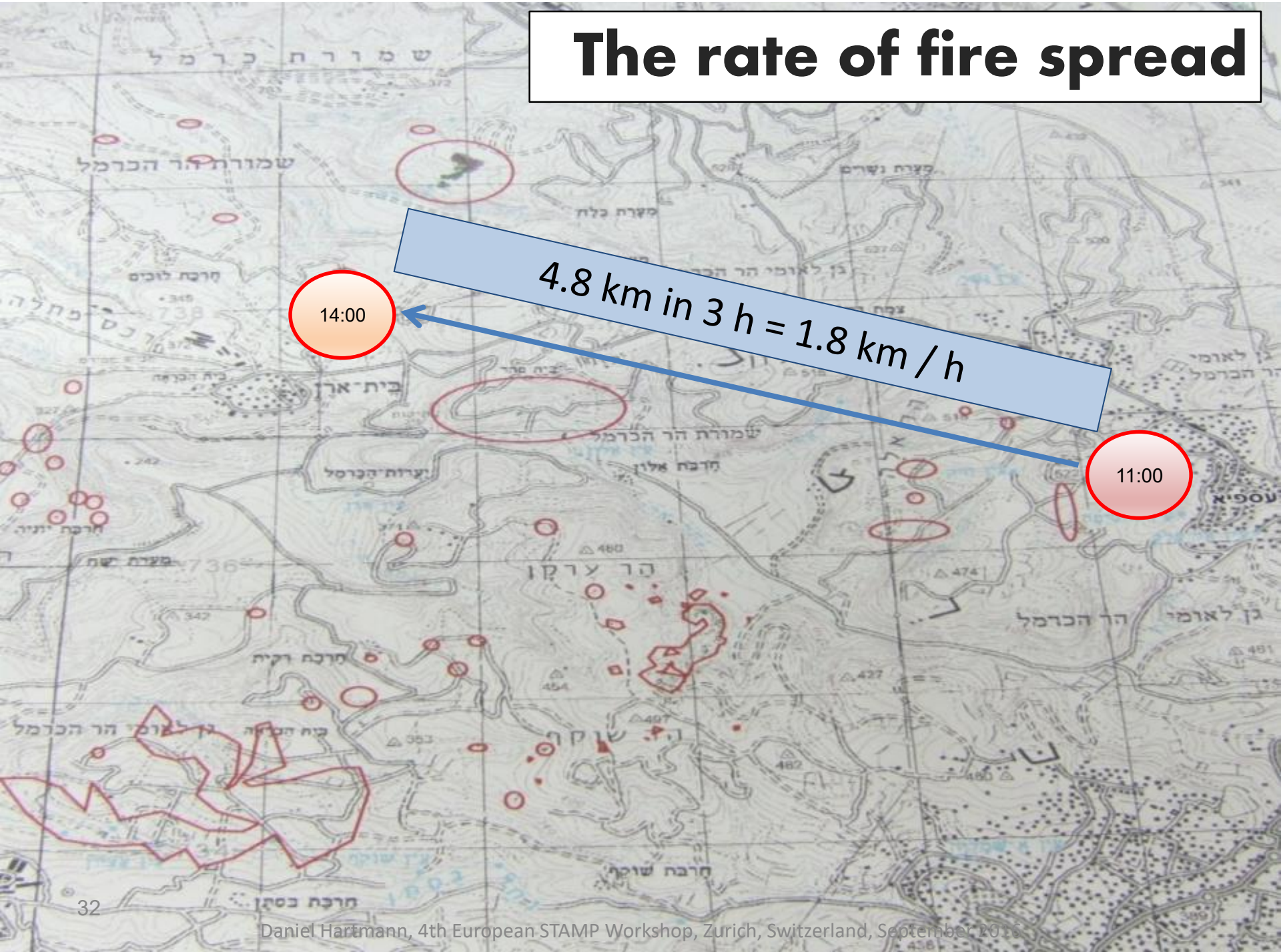
# Accident's Dimensions

- **Time**:
  - Proximal Event: Seconds – Minutes
  - t Δ between Design and Accident: ~ 40 years
- **Space**: few hundred square meters
- **Severity**
  - Tangible & Direct: **Seven** fatalities
  - Intangible & Indirect: mainly financial
- **Complexity**
  - Internal (PE): very Simple
  - External (SOCS): Simple
- **Response:** Simple

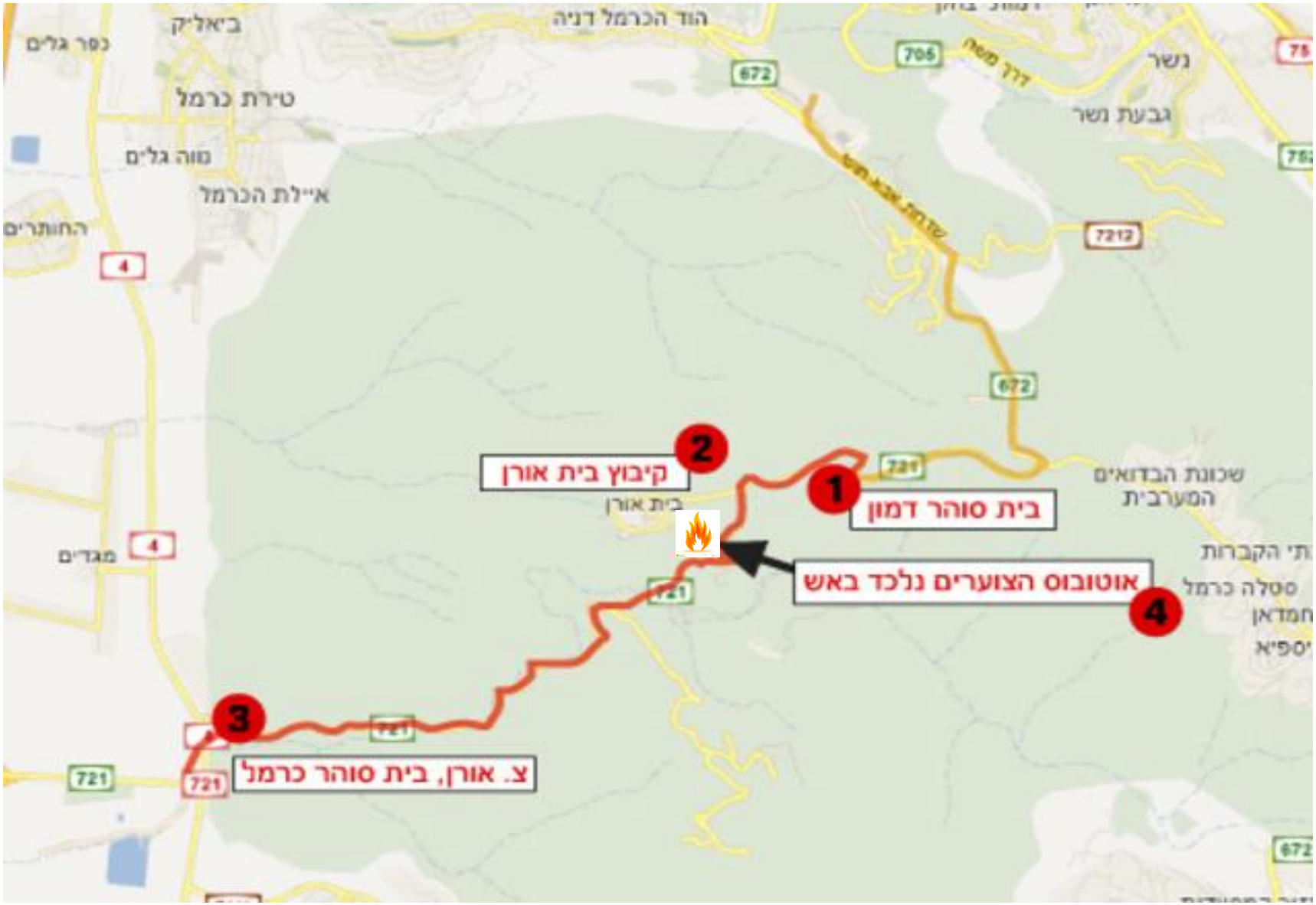
# The Carmel Forest Fire Disaster (CFFD), Israel (2010)

## An Accident in a System Response Control Structure (SRCS)

# The rate of fire spread



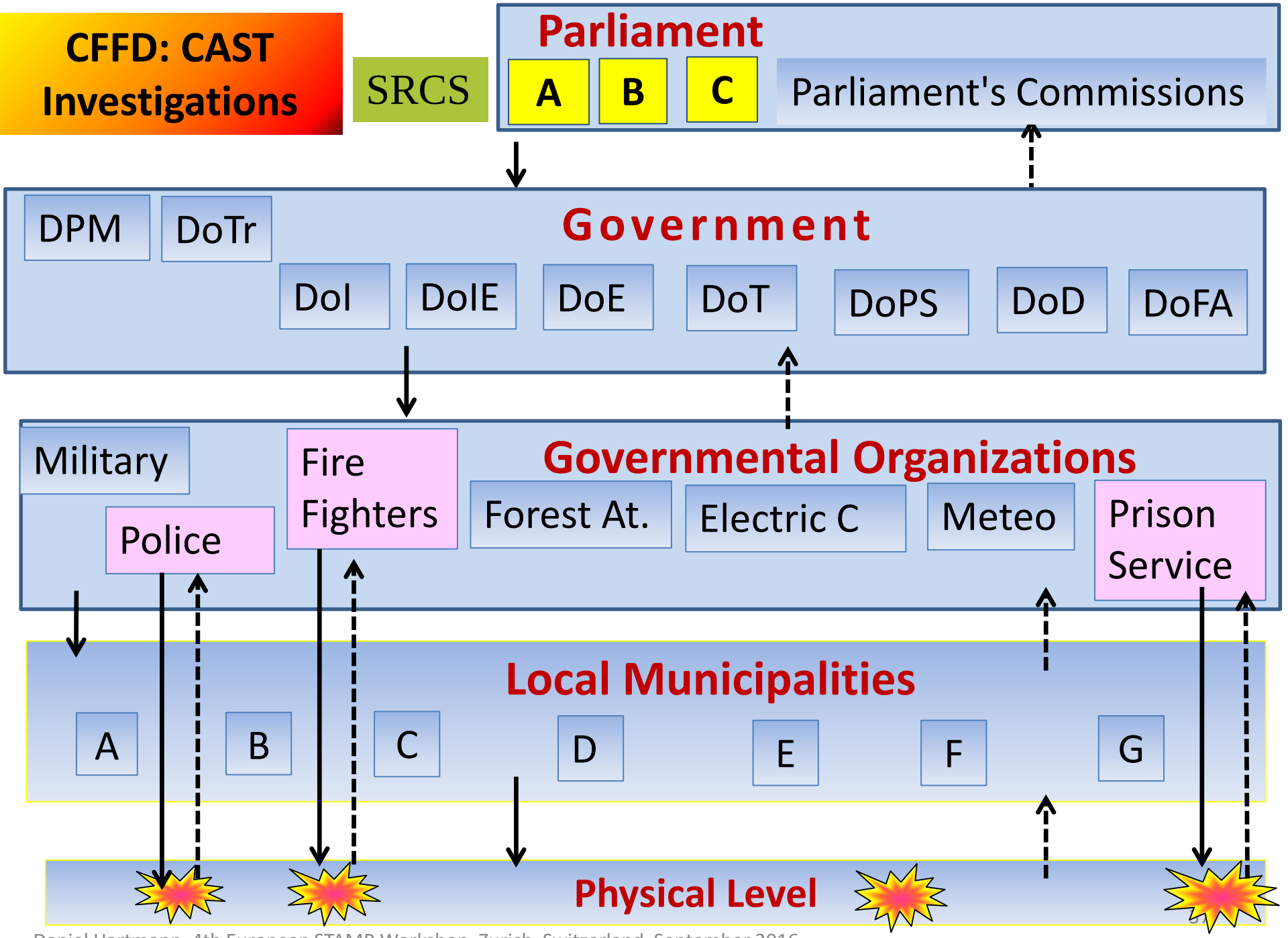
# Carmel Mountains – Road 721



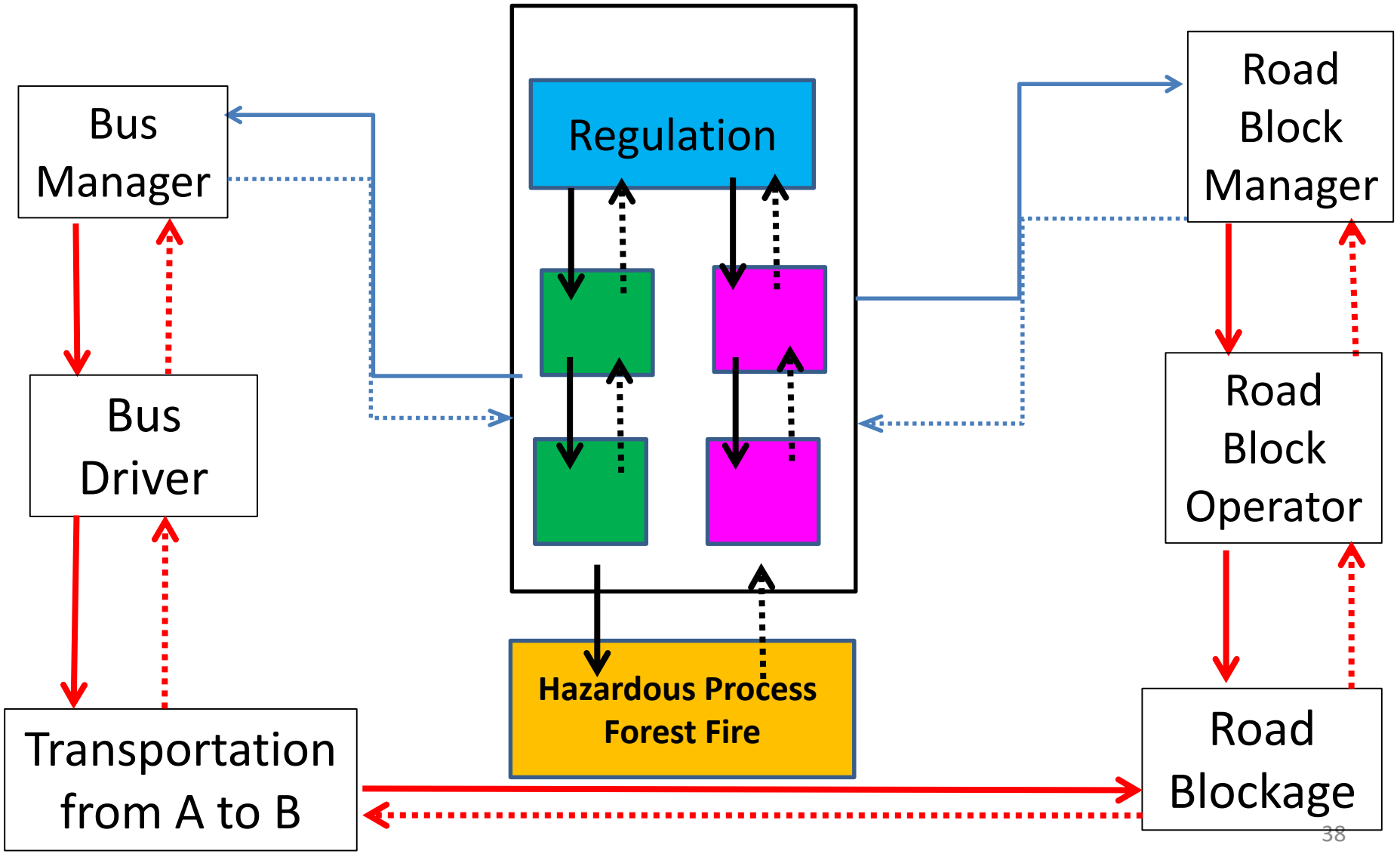

# The Carmel Forest Fire Disaster (CFFD), Israel (2010)


# The Carmel Forest Fire Disaster (CFFD), Israel (2010)

# Mount Carmel [Israel] forest fire (2010): a very expensive lesson in risk management and safety


CFFD: CAST Investigations
SRCS
Parliament
A
B
C
Parliament's Commissions
DPM
DoTr
Government
DoI
DoIE
DoE
DoT
DoPS
DoD
DoFA
Military
Police
Fire Fighters
Governmental Organizations
Forest At.
Electric C
Meteo
Prison Service
Local Municipalities
A
B
C
D
E
F
G
Physical Level

# CFFD partial S-T System Response Control Structure



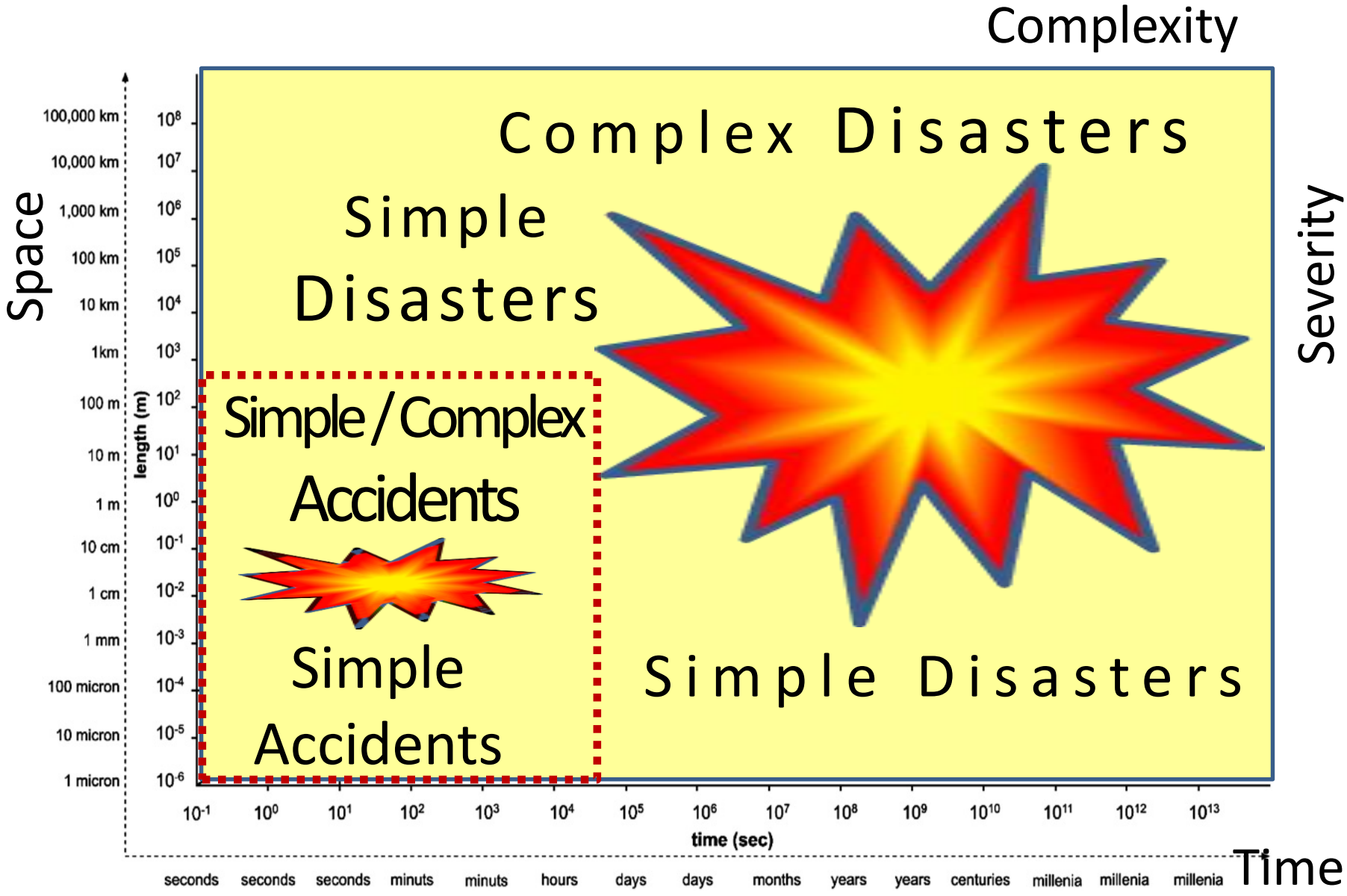
# CFFD Accident's Dimensions

- **Time**:
  - Proximal Event: many hours – few days
  - t Δ between Design and Accident: ~ 50 years
- **Space**: many dozens square kilometers
- **Severity**
  - Tangible & Direct: **forty four** fatalities
  - Intangible & Indirect: immense
- **Complexity**
  - Internal (PE): very Complex
  - External (SRCS): very Complex
- **Response:** very Complex

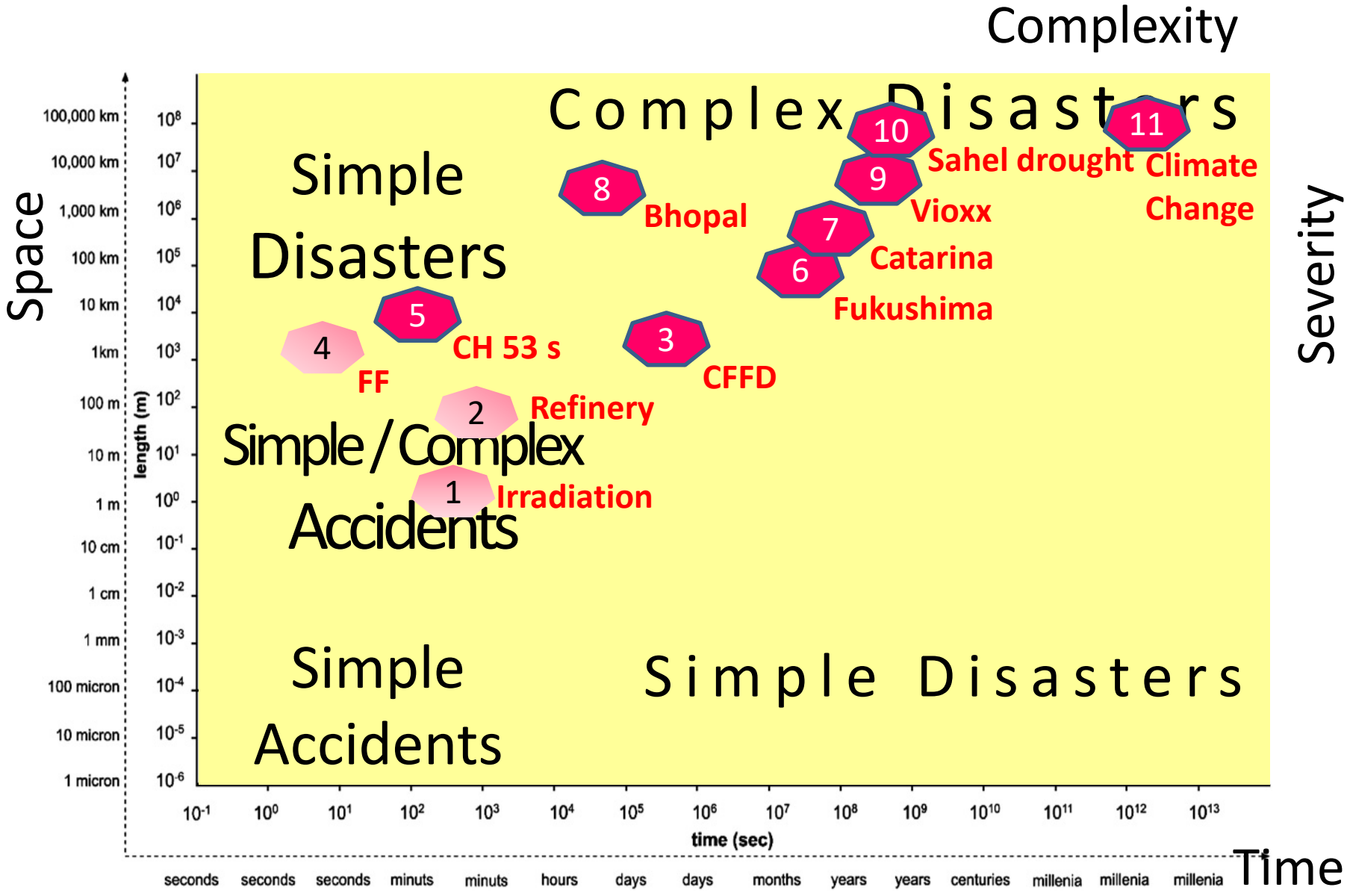
# Outline

- ✓ Short Introduction to “my ideas”
- ✓ Short Description of Accidents
- ✓ Some Preliminary Thoughts and Ideas

# Classification of Loss Events [Accidents and Disasters]



# Mapping of Loss Events [Accidents and Disasters]



# Some Preliminary Conclusions

- The key parameters building STAMP, CAST & STPA should be defined in a more precise scientific way.
- To avoid “spaghetti problems”, one should be strict with the division between SDCS, SOCS, SRCS and their sub-divisions.
- Large scale and numerous CAST analysis are needed to understand the variability and the patterns of loss events in various STSs.
- For most existing STSs, CAST analysis has to be the precursor for any STPA analysis.


Daniel Hartmann
danielh@bgu.ac.il


Daniel Hartmann
danielh@bgu.ac.il