25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

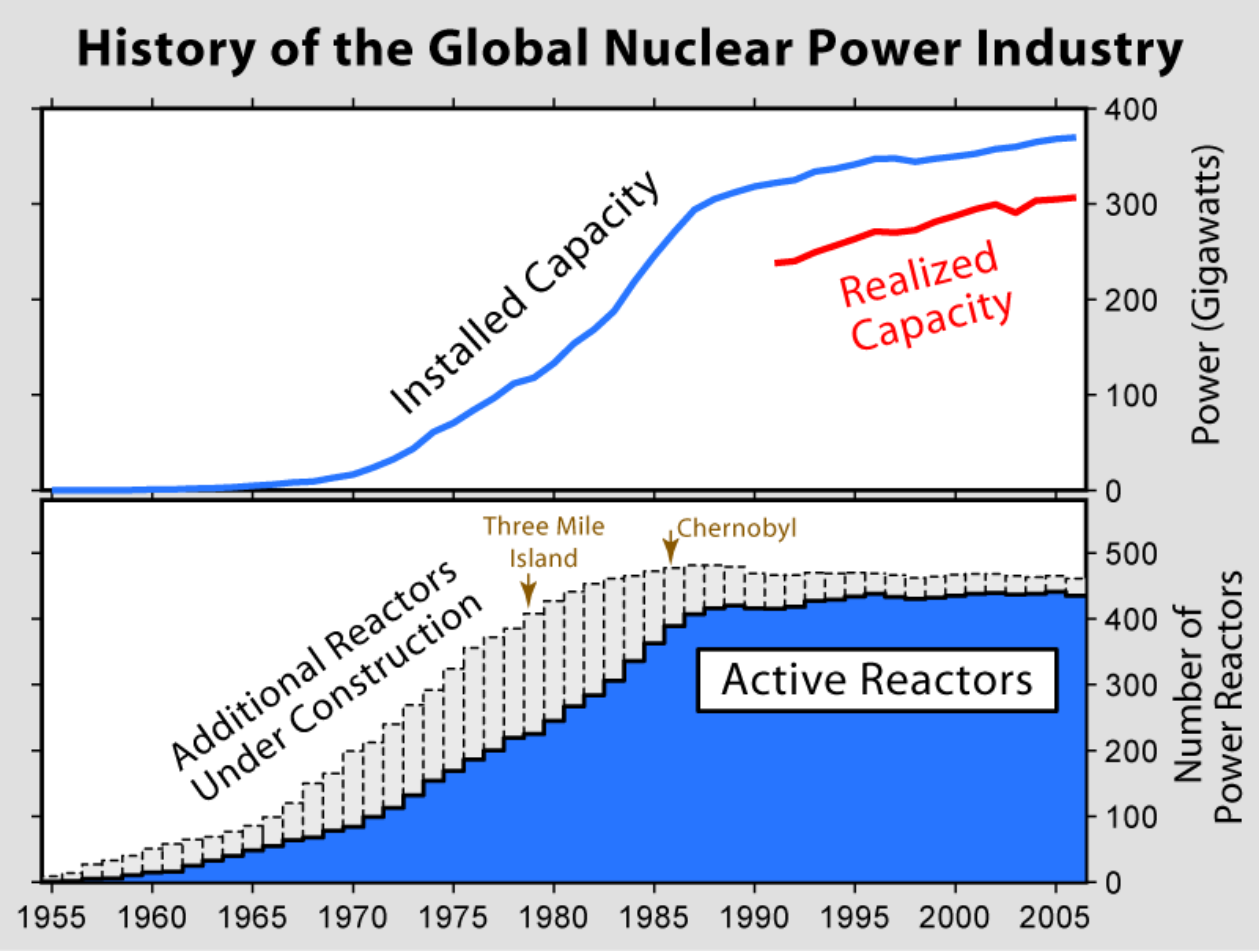
A practical guide to assuring the system resilience to operational errors

Dr. Avigdor Zonnenshain – Technion
Avi Harel – Ergolight
Gordon Center for System Engineering – Technion

TMI 2– 1979 – Three Mile Island

- New station – 40 days only
- Core melted for 5 days
- Operators fail to understand the situation.

Effect on Industry



What did the operators need to learn in 13 seconds?

- **The pumps stopped**
- The turbines shut down
- **The emergency pipes were blocked for two days, following a maintenance procedure**
- The steam generator boiled dry
- SCRAM
- **The PORV did not close after pressure**

- The pressure indicator did not reflect the water temperature properly.

How could they know it?

- 3 audible alarms
- Many of the 1600 lights blinking
- Printed messages hours behind schedule
- Radiation alarms coming in
- Control room filled with experts
- Phones ringing constantly
- Wrong indication about the PORV status

The need for this guide

- 90% of Industry accidents
- 75% of transportation accidents
- 50% of human productivity
- Consumer products
- Public-operated systems

To err is human.

Cicero 106-43 BC

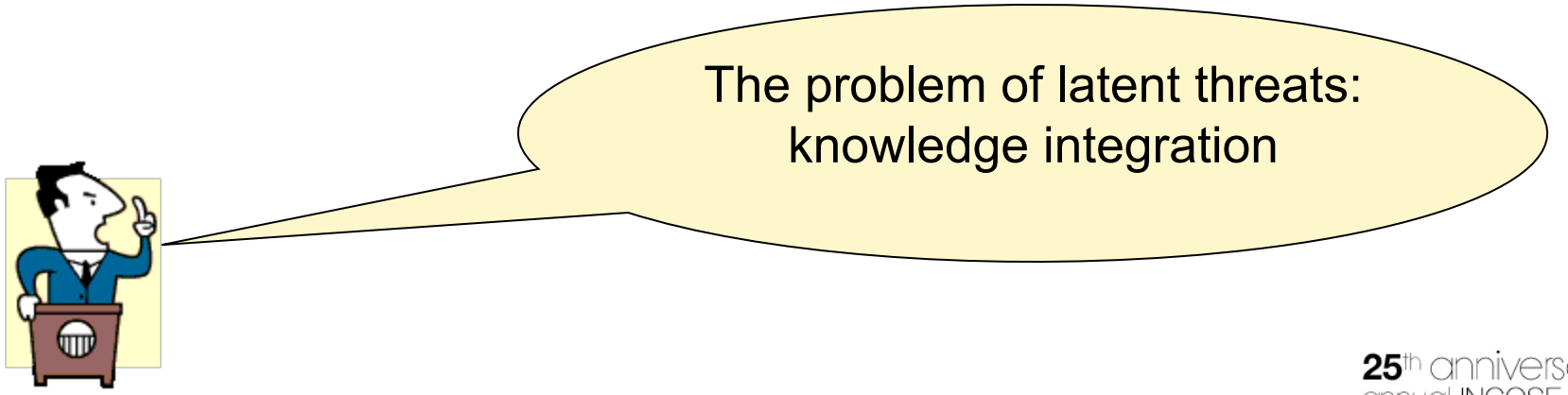
Analysis of the TMI accident

- System was under threats for days before
- The operators were not aware of it
- Operators' awareness of the threats should prevent the accident

The key issue in resilience assurance - **latent threats**

Do we need a new guide? Related disciplines

- Safety engineering
- Human factors engineering
- Risk Management



What is a human error?

The result?

The situation?

The trigger?

Hollnagel, 1980

A trigger is considered an error only if the results are undesired

Sources of human error?

Results

Condition

Trigger

Hollnagel, 2011

An error is the result of extreme conditions

Human error vs. negligence

No need to double check. I did it 100 times before

We should not look for the bad apple. Rather we should focus on preventing the next accident

Dekker, 2007

Application of Murphy's Law

If the design enables the human operators to fail, eventually they will!

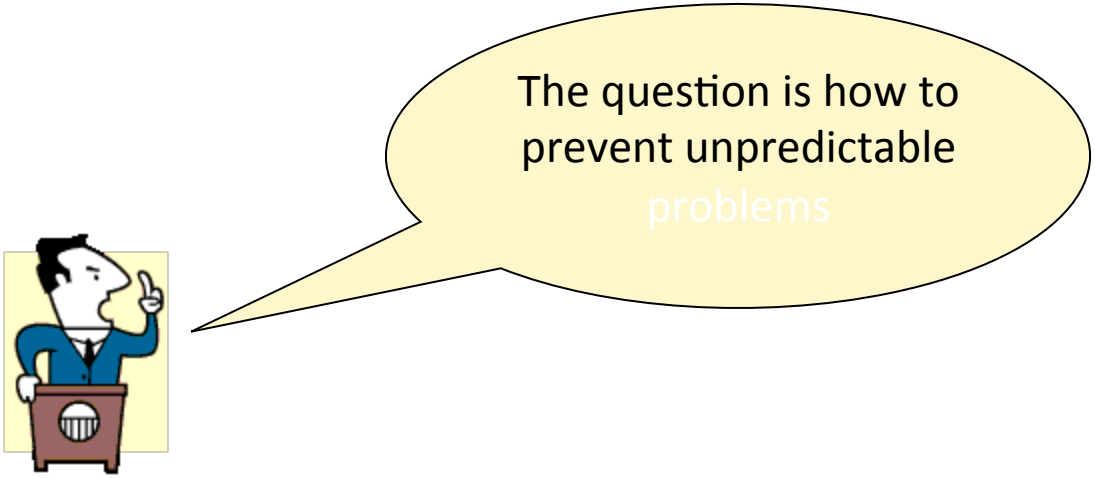
Weinberg 1971

Instead of accusing the operator, we should focus on analyzing the designers' attitude to user errors

Engineerable definition

A human error is

"*the absence of a best practice or the failure to apply knowledge that would have prevented a problem*."

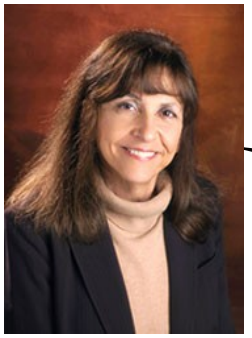


Mark Paradies - TapRoot

State of the art

Situation-oriented:
- 1997 Ergolight UPI
- 2004 STAMP

Trigger-oriented:
ETA, FTA, FMEA,
HAZOP,
Poka-yoke,
Etc.



Nancy Leveson

The design should constrain the system behavior according to **explicit rules**

Goals of this guide

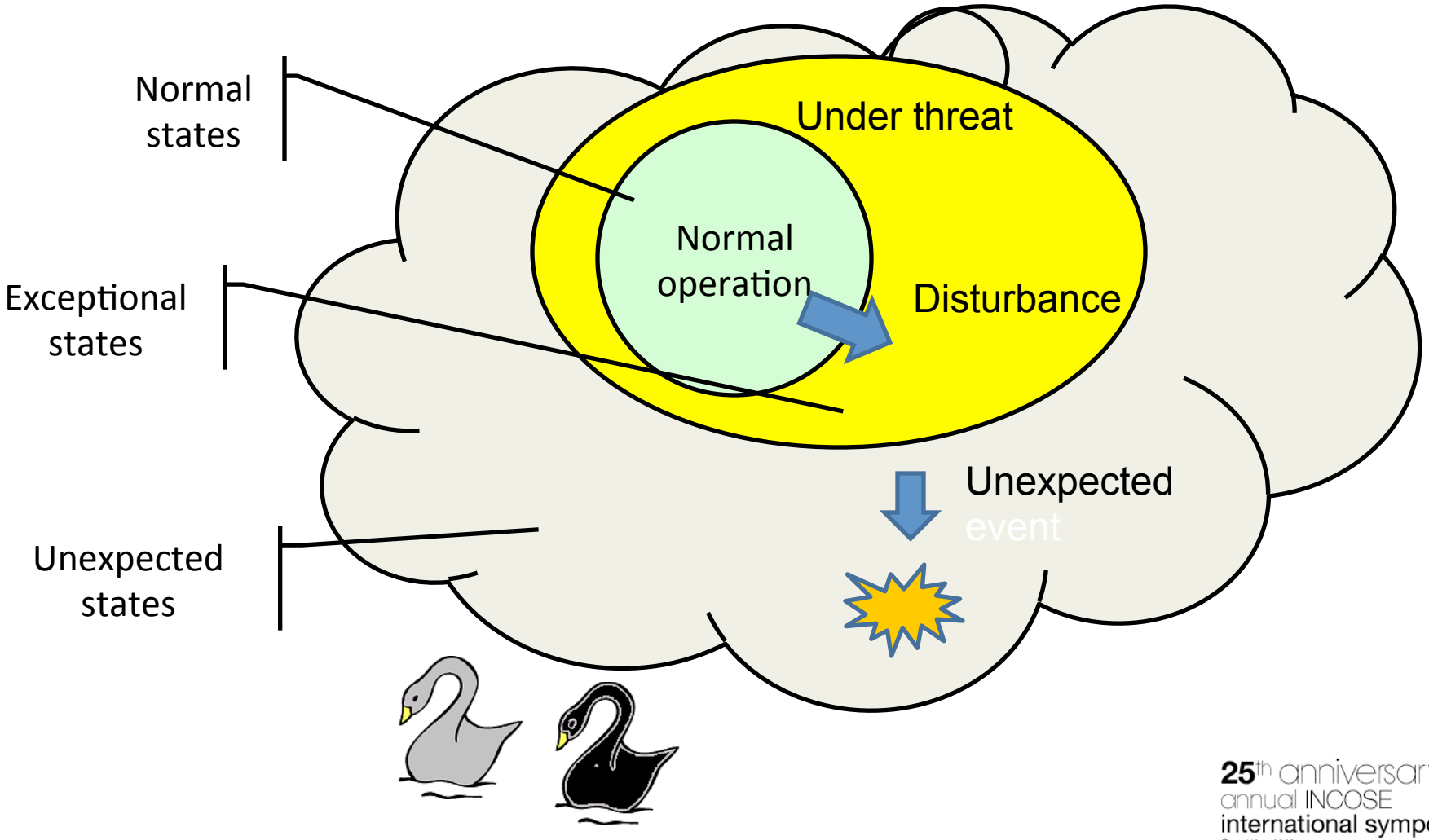
- Propose ways to **identify failure modes** early at the design stage
- Present methods to **prevent these failure modes**
- Evaluate the **risks of safety means**

It is surprising that such a guide was not proposed before

Prior studies

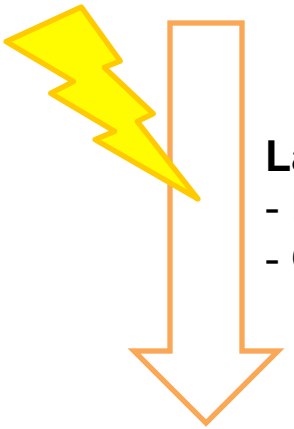
- 2009 – Task-oriented system analysis
  - A. Zonnenshain, A. Harel – INCOSE conference
- 2009 – Initial version of the guide
  - M. Weiler, A. Harel – Resilience WG report. (Hebrew)
- 2010 – tackling unexpected events
  - A. Harel, M. Weiss – INCOSE-IL conference
- 2010 – managing operational risks – driving
  - M. Weiler, A. Harel – INCOSE-IL conference
- 2013 – Resilience-oriented design
  - A. Zonnenshain, A. Harel – INCOSE-IL conference

Model of operational failure



Types of triggers

Normal Conditions

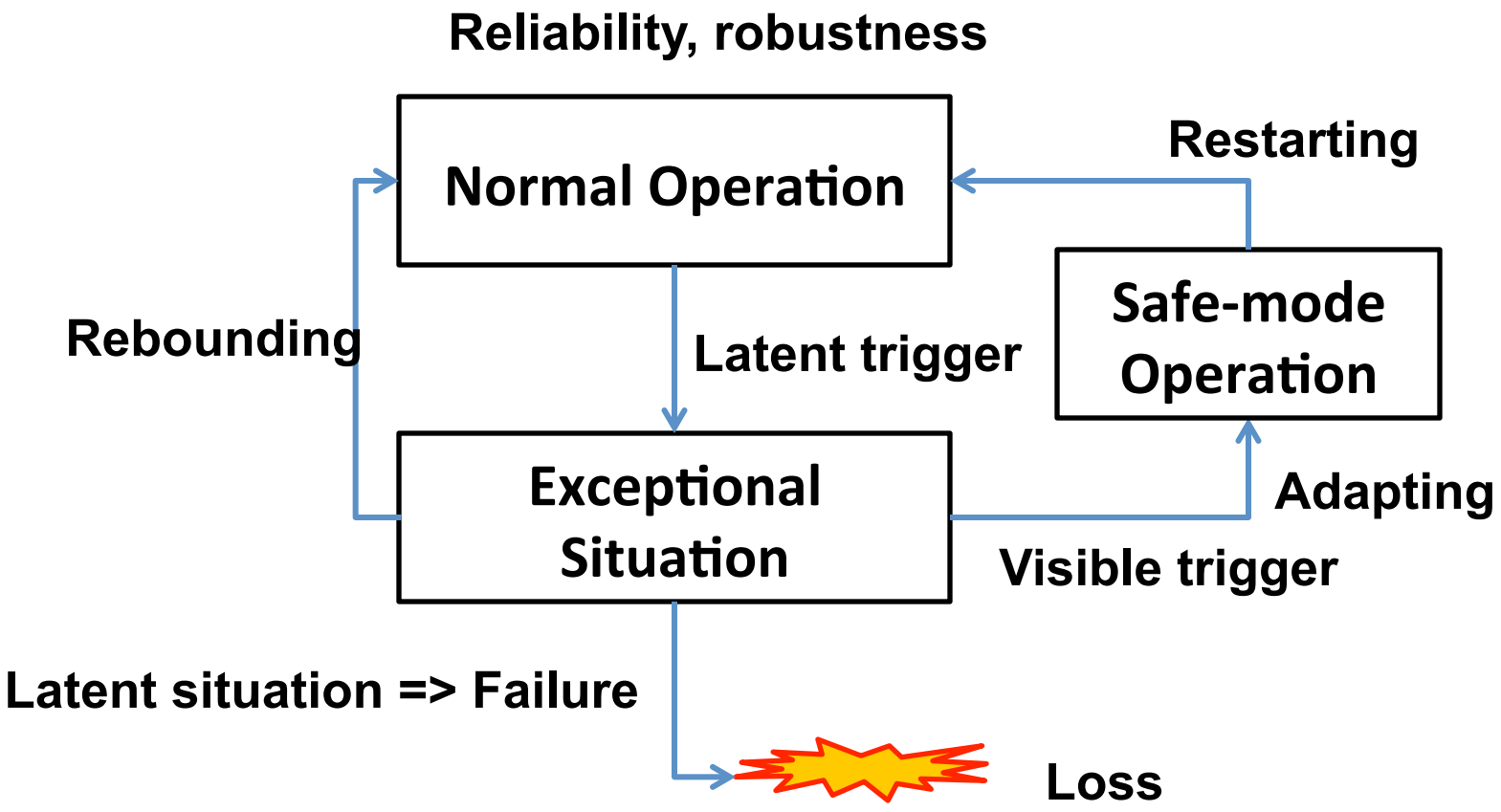


Latent trigger:
- Fault: HW, SW
- Operator's input

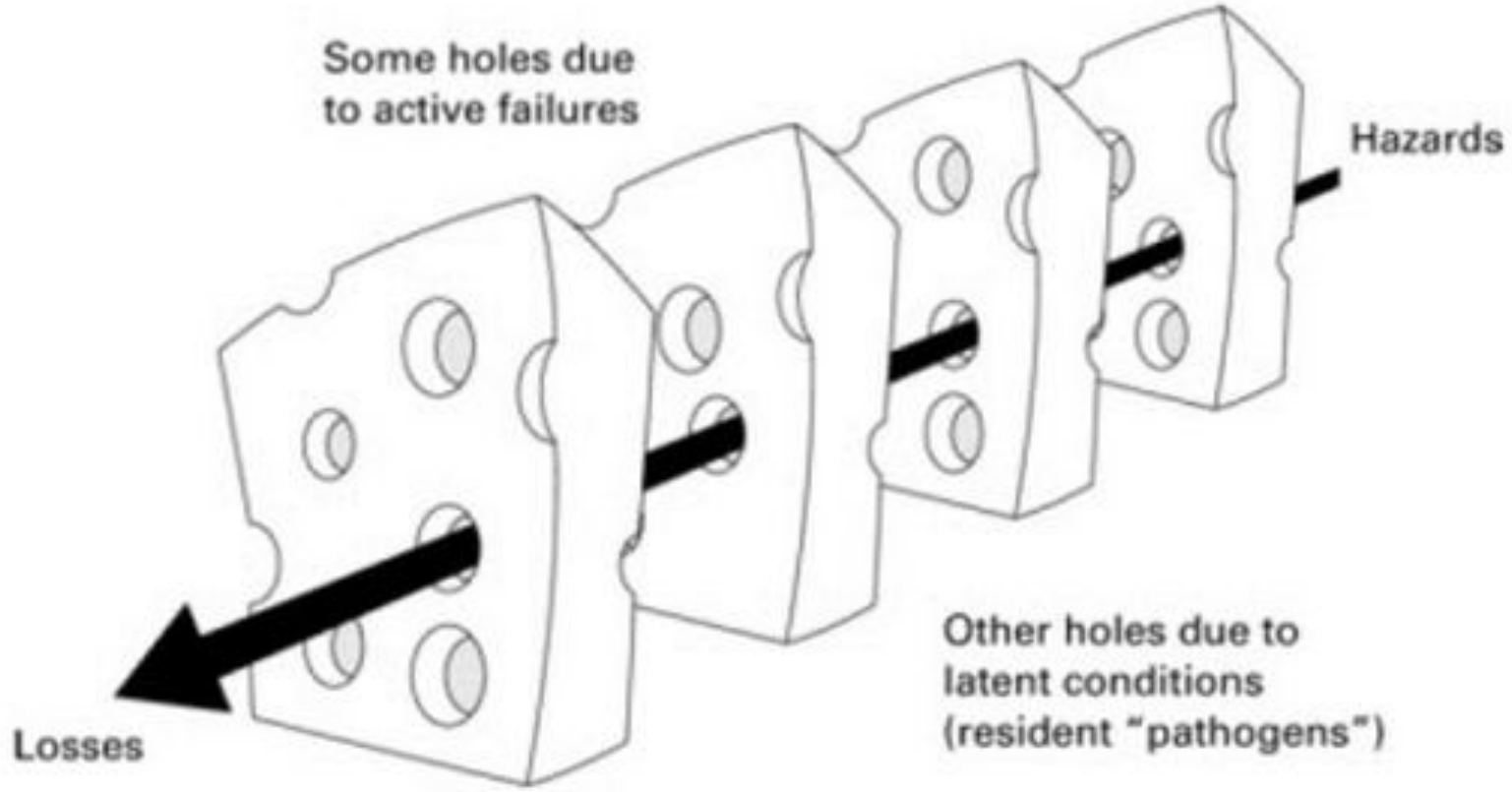
Latent Exceptional Conditions

Visible trigger:
- **Normal event**
- Derived fault
- Coinciding fault

Resilient Operation



Failure and Defenses

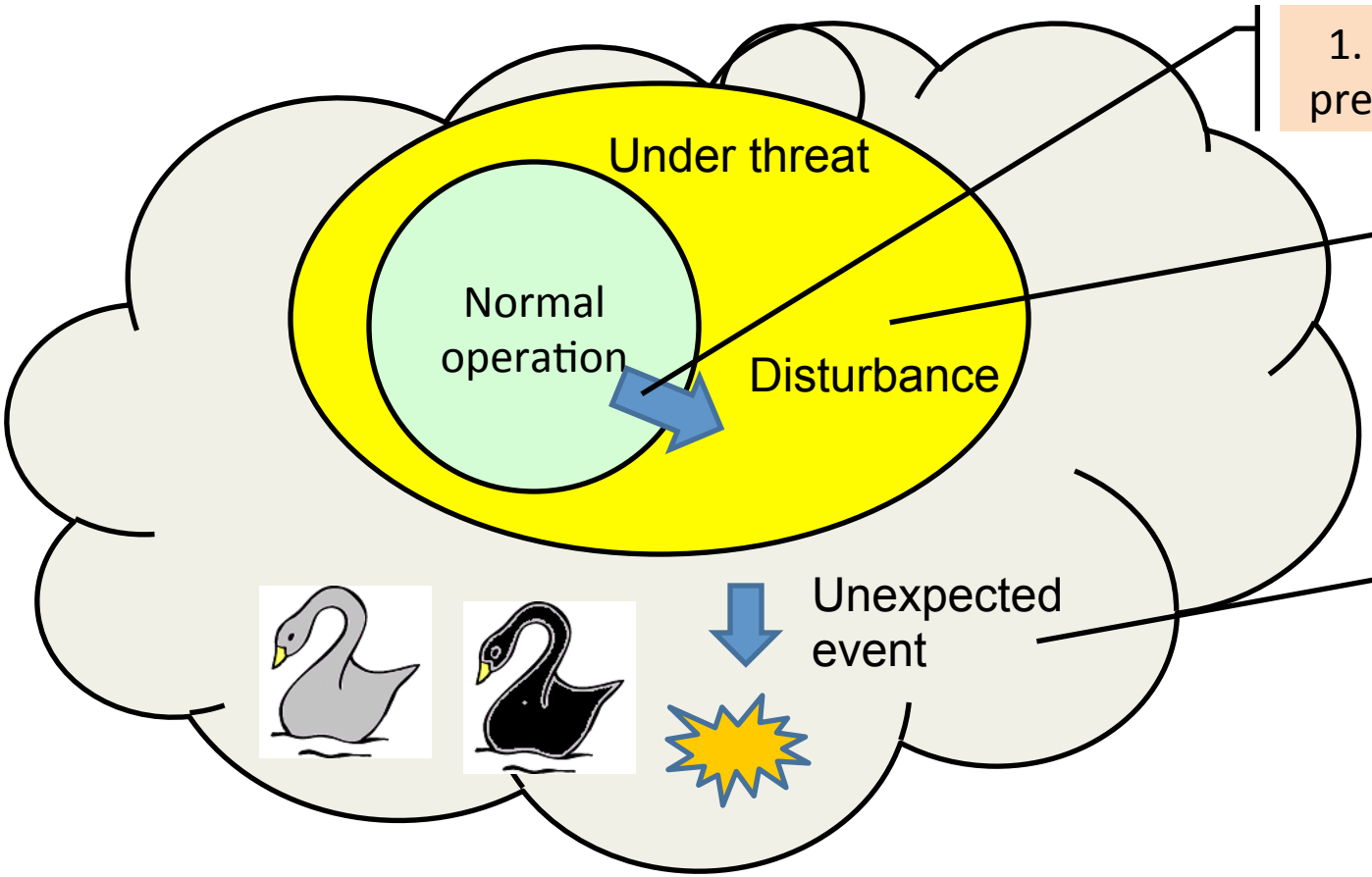


Swiss cheese model by James Reason published in 2000.

Defense Strategies - firewalls

- Prevent threats
- Manage the exceptional situation
- Resilience management

3 Firewalls


Under threat
Normal operation
Disturbance
Unexpected event
1. Threat prevention
2. Manage Exceptional states
3. Resilience management

Firewall break down

- Prevent threats
  - Automation management
- Manage the exceptional situation
  - Detect latent conditions
  - Alert
  - Prevent escalation (safe mode operation)
  - Rebound
- Resilience management
  - Verification and validation
  - Learn from mishaps

1. Automation Management

- Dilemmas
  - Who controls?
  - Who controls the control?
- Depending on the situation:
  - Bainbridge (1983) The Irony of Automation

2. Detect latent condition Rule-based operation

Alain Colmerauer

Rule-based programming Prolog, 1967

Ergolight

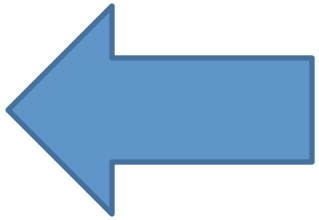
Rule-based Usability testing UPI, 1999

Nancy Leveson

Principle of **Explicit rules**, 2004

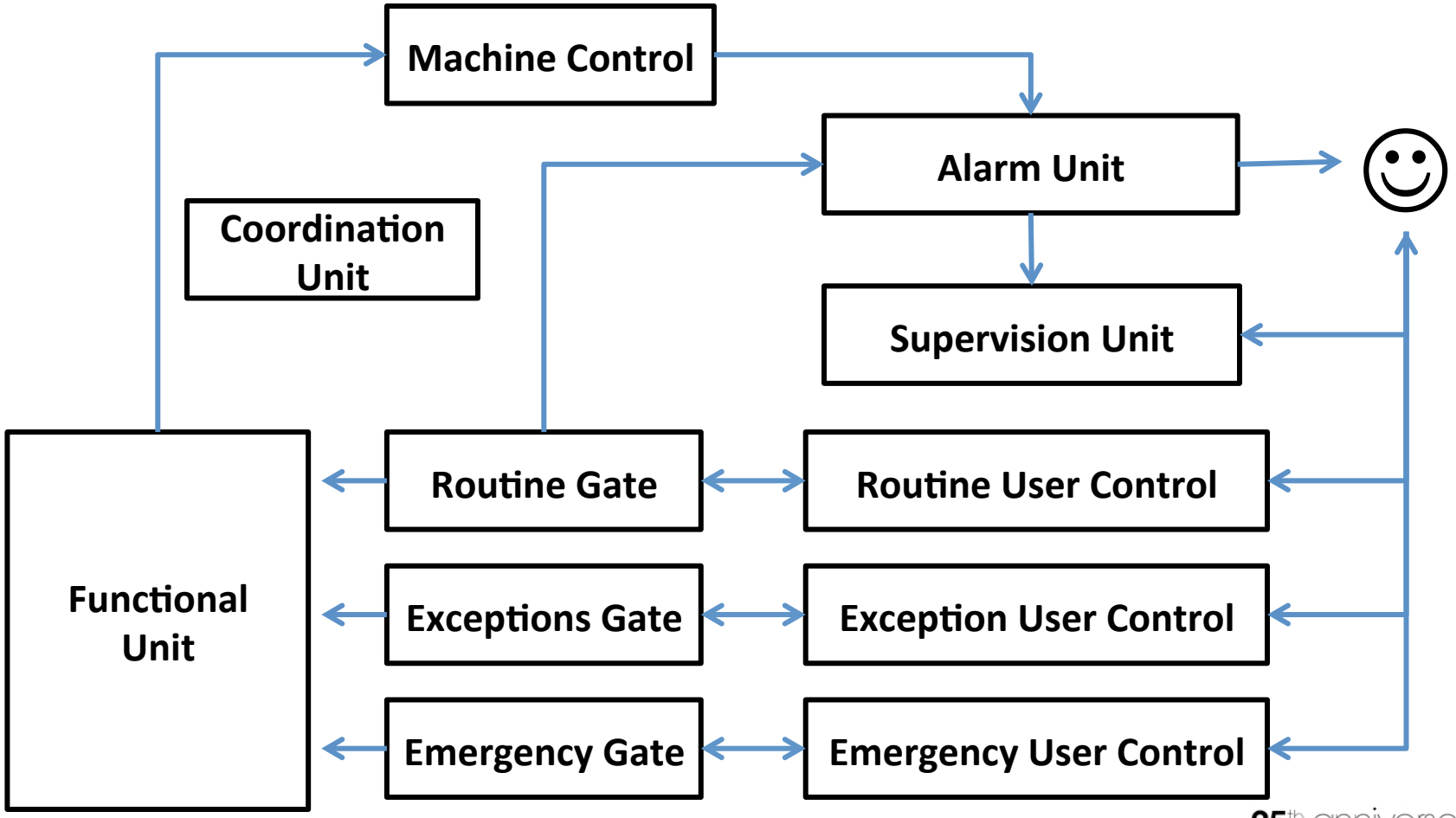
Principles of rule-based operation

1. Scenario-dependent rules
2. Scenario-based Human-Machine Coordination

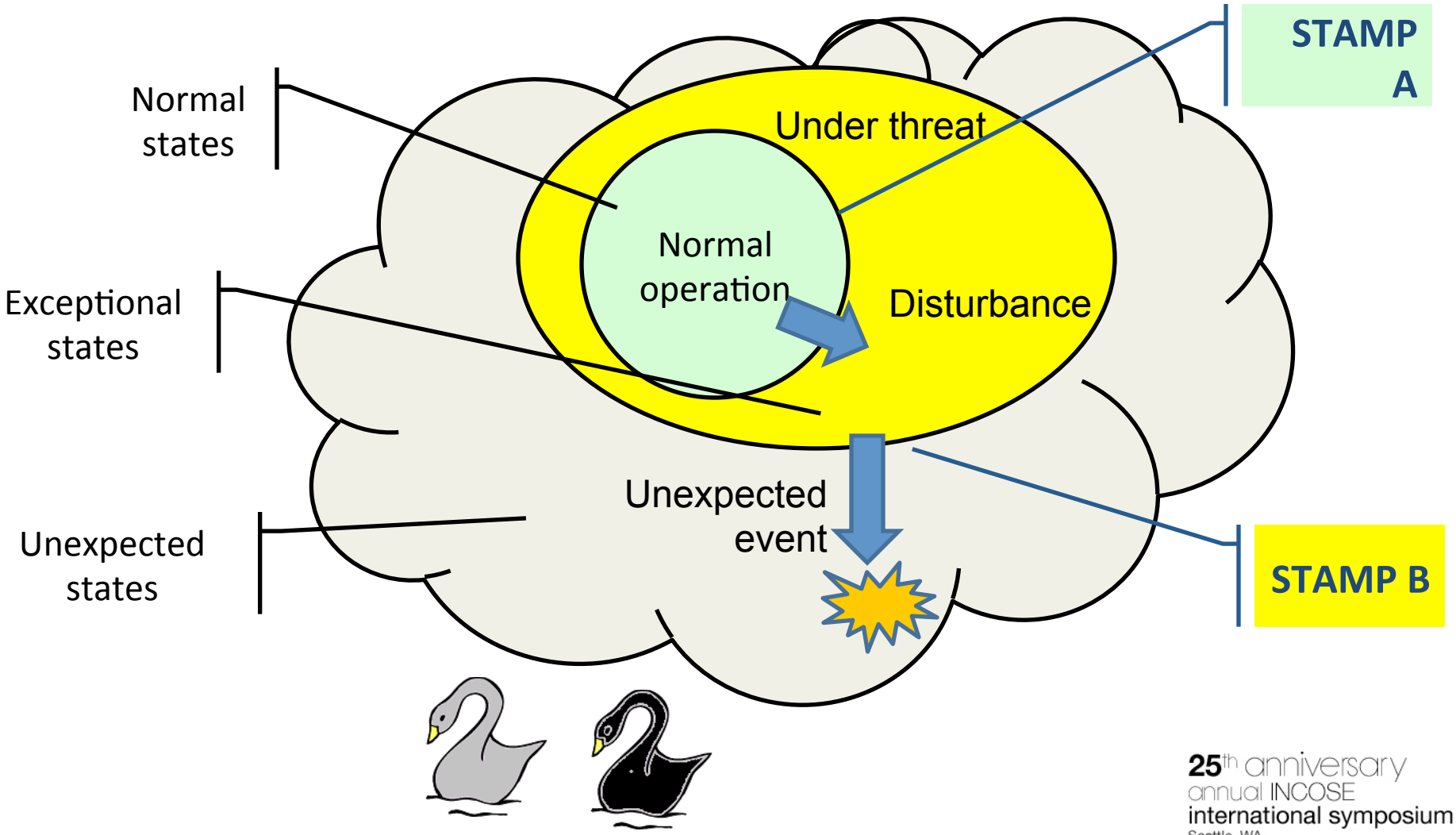


Principle of
explicit scenarios

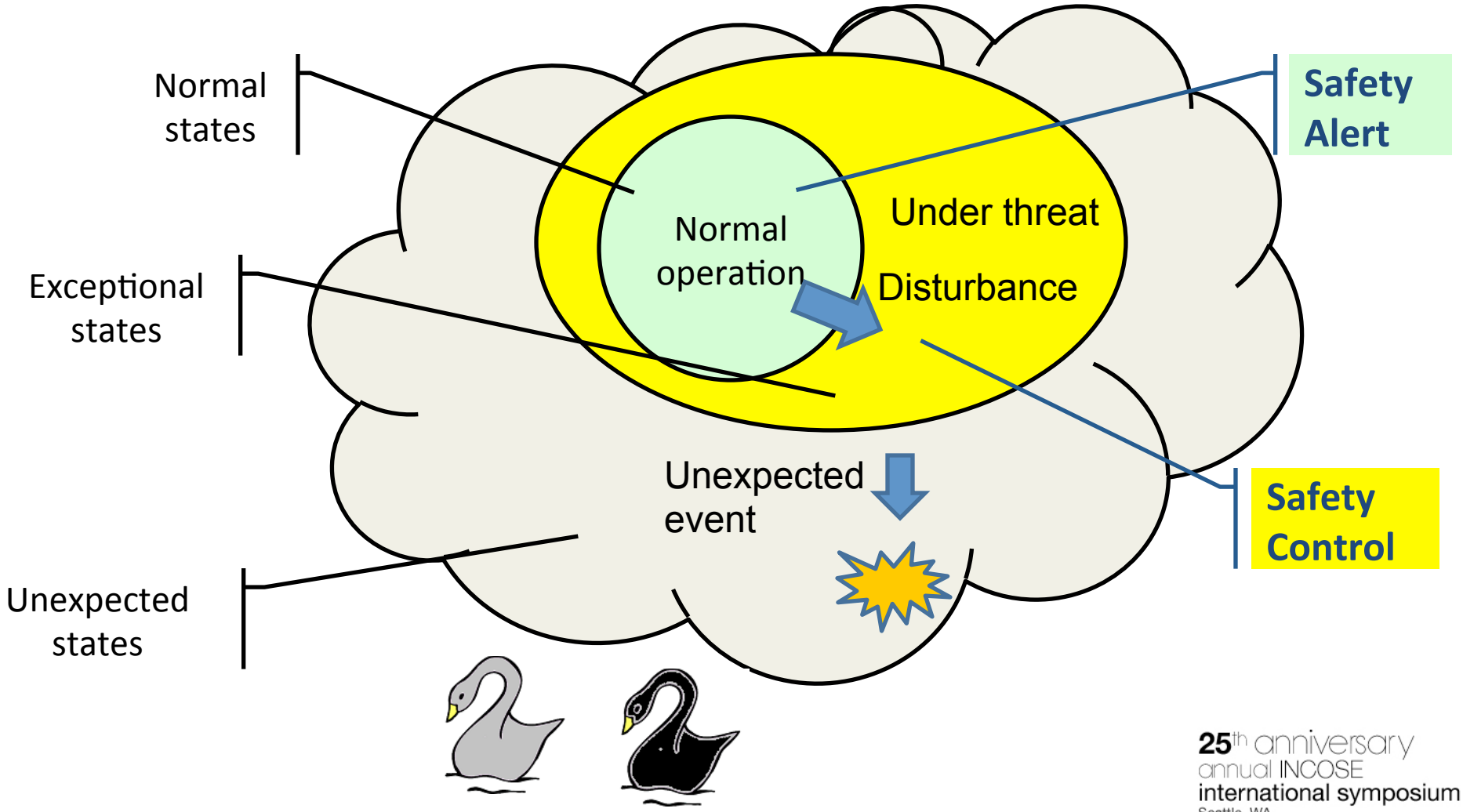
Managing exceptional situations



Escalation Prevention



Automation design



Validation method

- Event Database: 67 events
- Experts – members of Resilience WG
- Resilience score: guidelines per event
- Statistics of resilience scores

Event Database

- Sources
  - Published accidents
  - Published usability issues
  - Iltam/Incose-il Resilience working group.
- Event structure
  - Event description
  - Failure modes
  - Reference to the guide (version 8).

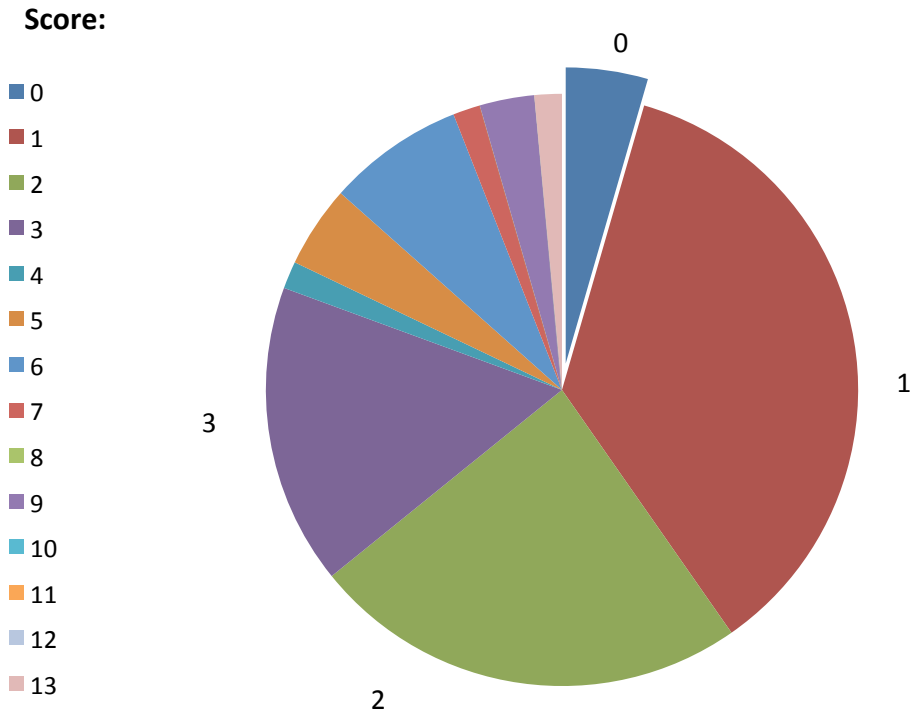
Pilot study – 11 events

- Gilad Segal – M.Sc. student
- Version 7- July 2014
- Reference from events to guide
- Event resilience score = # referred guidelines
- Get statistics of resilience scores

Final study – full database

- 67 events
- Version 8 – January 2015
- Reference from events to guide
- Cross reference from guide to events
- Event resilience score = # referred guidelines
- Get statistics of resilience scores

Statistics of resilence scores



Resilience score: 2.6
Coverage: 96%

Next goals

- Validating the particular instructions
- Integrating the guidelines in common development procedures
- Procedure for fine-tuning the constraints
- Tools for resilience-oriented development
  - Constraint definition and tuning
  - Incident identification and reporting
- Pilot real projects
- Education: industry and academy

General availability

resilience.ergolight-sw.com