IRSN
INSTITUT
DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

Faire avancer la sûreté nucléaire

Learning Lessons from TMI to Fukushima and Other Industrial Accidents: Keys for Assessing Safety Management Practices

Nicolas Dechy, Jean-Marie Rousseau
IRSN (Institute of radiation protection and nuclear safety), France

Yves Dien, Michel Llory, René Montmayeul
CHAOS Association (Heuristic club for organizational analysis), France

IAEA - International Conference on Human and Organizational Aspects of Assuring Nuclear Safety - Exploring 30 Years of Safety Culture

Vienna, 25th February 2016

The key messages

1. There are failures to learn from accidents in all sectors – organizational learning remains difficult

2. We can learn the lessons from all industrial sectors because of the recurring patterns and similarity of the root causes

3. Such as in medicine, we can capitalize the knowledge from accidents "*knowledge and culture of accidents*"

4. We can already use it in prevention when conducting HOF assessment of nuclear safety management provisions

5. Beyond the retrospective bias, the "*gift of failure*" and the "*royal road*"

- **PART 1: WHY, WHAT and HOW can we better CAPITALISE the LESSONS from ACCIDENTS from all industrial sectors?**

- PART 2: HOW can we better USE them in PREVENTION?

1.1 Why should we use the Lessons from Accidents better?

- Some lessons were learned in the nuclear sector:
  - TMI, Chernobyl, Fukushima ➔ official investigations (Kemeny, Rogovin, Diet), lessons were disseminated (IAEA, OECD, WANO) and treated (EU "stress tests")
- But, there are failures to learn in the nuclear sector:
  - Some root causes without deep changes: organizational complexity, production pressures, inter-organizational relationships, regulatory capture, failure to learn
  - Fukushima: "*The regulators also had a negative attitude toward the importation of new advances in knowledge and technology from overseas*"

1.1 Why should we use the Lessons from Accidents better?

- Failures to learn in space industry: **accidents at NASA**
  - *"**Both** Columbia and Challenger were lost also because of the **failure of NASA's organisational system**"*
  - **"echoes"** of Challenger in Columbia
  - *"[…] the causes of the institutional failure responsible for Challenger have not been fixed. […] **if these persistent, systemic flaws are not resolved, the scene is set for another accident**"*

- Failures to learn in process industry: **accidents at BP**
  - ***"striking similarities"** - lessons of Grangemouth (2000)/TC (2005)*
  - ***"striking similarities"** - causes Prudhoe Bay (2006) /* Texas City
  - *"Most if not all of the **seven root causes** that BP consultants identified for the Prudhoe-B incidents have **strong echoes** in TC"*
  - Both reports *"point to **similar cultural factors** within BP, in both its upstream production and downstream refining operations" ; "underscores how safety culture truly is set at the top at a corporation"*

1.1 Why should we use the Lessons from Accidents better?

- Key findings from lessons from industrial accidents:

  ➔Accidents are ***unique*** events with very different technical failures but ***similar*** organisational causes

  ➔The **inability to learn** within an organisation ➔ a **similar accident reoccurs**

  ➔After an accident, in-depth organisational learning in the same organization, in the same industry, **and learning fully from others' hard lessons** remains much more difficult than expected

1.1 Why should we use the Lessons from Accidents better?

- Some barriers to recognize the generic character of others' hard lessons:
  - "It can not happen to us, we are different"
  - Too much differences between technological sectors?
    - Fukushima lessons for aviation sector?
    - Columbia lessons for Process industry in Europe?
    - Texas City lessons for nuclear industry?
  - An accident is
    - a unique event
    - a contingent combination of multiple causes + circumstances
    - that would not repeat itself

1.1 Why should we use the Lessons from Accidents better?

- Generic character and patterns:
  - Beyond technological differences, all sociotechnical systems?
  - Researchers found recurring schemes, generic accident patterns
    - Incubation period (Turner, 1978), weak signals, whistle-blowers, latent errors (Reason, 1990), systemic failure (Bignell and Fortune, 1984), organizational accident (Reason, 1997)
  - Study of >100 of industrial accidents show (Llory et al, 2015)
    - **Similar root causes recur across accidents whatever their occurrence contexts (industrial sector, country, regulation, history, culture)**
    - **"Echoes", "striking similarities" not only in NASA and BP accidents but in most if not all accidents!**

1.1 Why should we use the Lessons from Accidents better?

- Limits of safety improvement:
  - Overall risk reduction for the last 50 years – asymptotic curve
  - But, some limits
    - "*tango on an asymptote*" (Frantzen, 2004)
    - Accidents still occur in all sectors and countries
    - Some similar accidents recur
  - Turner (1978) describes the end of an accident not in technical terms but when there is a "*full cultural readjustment*"

➔ does it occur?

1.2 How can we capitalize and transfer the lessons learned from accidents?

- 2 concepts are proposed:
  - Content issue : *"Knowledge of Accidents"*
  - Transfer issue : *"Culture of Accidents"*
- Goals:
  - Enrich safety analysts, prevention actors and decision-makers with "background knowledge references" [*expert black-box*]
  - Disseminate and make effective this knowledge (as an **alive memory**) for operational actors
  - Enable a paradigm shift

1.2 How can we capitalize and transfer the lessons learned from accidents?

- The medical metaphor:

  - Study of diseases, pathologies, causes of death ➔ develop knowledge based on « anatomy of disaster »
  - Effort of collecting and classifying diseases
  - Library of reference cases in medicine handbook, epidemiologic studies to support (etiology of diseases)
  - Huge effort of memorization for students at medical school

  ➔Analogy n°1: need to develop a capitalized, articulated and actionable knowledge of accidents

  - During the diagnosis, the past knowledge is guiding to infer clinical signs based on symptoms to deduce the syndrome

  ➔Analogy n°2: need for a clinical approach of the organization, « comprehensive approach », guided by the knowledge of accidents

1.2 How can we capitalize and transfer the lessons learned from accidents?

Example of a knowledge of accidents

- "*Pathogenic Organizational Factors*" (Dien 2004, after Reason, 1990)
  - Production pressures;
  - Organizational complexity leading to obscurity and compartmentalization, excessive formalism or proceduralisation;
  - Weaknesses of learning from experience (OPEX) [see in annex]
  - Complacency or deficiency of control authorities
  - Deficiencies of communication or lack of quality of dialogue…

- PART 1: WHY, WHAT and HOW can we better CAPITALISE the LESSONS from ACCIDENTS from all industrial sectors?

- **PART 2: HOW can we better USE them in PREVENTION?**

2. How can we use the lessons learned from accidents for normal operations?

- In assessment of nuclear safety management on NPP

  - IRSN is the public expert to support the French regulator (ASN)

  - "Safety management in a competitiveness context" (IRSN, 2008)
    - *To address:* "priority given to safety" in decision-making
    - *To question:* Production pressures? Safety still meaningful? Counter-measures effective? Continuous improvement?

  - "Safety and radiation protection management during outages" (IRSN, 2013)
    - *To address:* organizational complexity and performances after an organizational change (outage control center)
    - *To question:* interface management (internal, subcontractors)? rhythm and interaction of changes? human resources management (staffing, skills)? learning from events?

2. How can we use the lessons learned from accidents for normal operations?

- In assessment of nuclear safety management on NPP

Use of lessons: to interpret

- Retirement wave ➔ understaffing + loss of skills ←➔NASA in 90's
- Outage Control Centre from USA was not the only change (AP913, subcontractors, spare parts, human performance, IT, procedures) ←➔ NASA: "*not one or two policy changes, but a torrent of changes. This was not evolutionary change, but radical or discontinuous change*" [CAIB, 2003]
- Complexification of organisation in outages ←➔ NASA
- Flawed decision-making ➔reversing the burden of proof ←➔ NASA
- Learning deficiencies ←➔ several accidents with failures to learn

2. How can we use the lessons learned from accidents for normal operations?

In event analysis

- IRSN deals with 1300 significant reportable events per year from French nuclear operators (EDF, AREVA, CEA)

- Goal is to stimulate transverse and inter-organizational learning
  - Short reports with similarities between events across operators
  - Echo with a lesson from accident

- An example:
  - Anomalies not treated/fixed for some time
  ➔ a cause of events
  - Tolerance to persistent deviations echoes "normalization of deviance" identified by Vaughan (1996) in Challenger accident

CONCLUSION

Discussion

- Relying on accident data is a strong assumption: school of thoughts

  - HRO, Resilience engineering advocate for normal operations:
    - too much attention to accident ; reports are second hand data
    - Factors, strategies, “best ways” in daily, adverse conditions

  - “Gift of failure” (Wilpert, 2011):
    - Opportunity to learn, generate discussions

  - “Royal road” (Llory, 1996)
    - Freud metaphor: a way to access the malfunctioning of organizations and hidden phenomena “dark side”
    - Accidents help to better understand the banality of the daily life in organizations (supported by medical metaphor)

Discussion

- Relying on accident data is a strong assumption: validity

  - "Retrospective bias" ; "hindsight"
    - For accident investigator – wisdom (Reason, 1990)
    - Weak signals could not be understood (Vaughan, 1996)

  - But, several accidents show
    - People (operators, managers) had recognized the safety degradation (e.g. Texas City) before the accident
    - Weak and strong signals missed ; whistleblowers not listened

  - Proof of vulnerability in an accident VS in normal operation, proof of reliability/resilience while an accident is waiting to happen?

➔Both knowledge from accidents and normal operations are potentially biased (for different reasons) but complementary

Further challenges

- 37 years after TMI - 30 years after Chernobyl

- Will we take full benefits from Fukushima' lessons and former industrial accident lessons to achieve a "*full cultural readjustment?*"

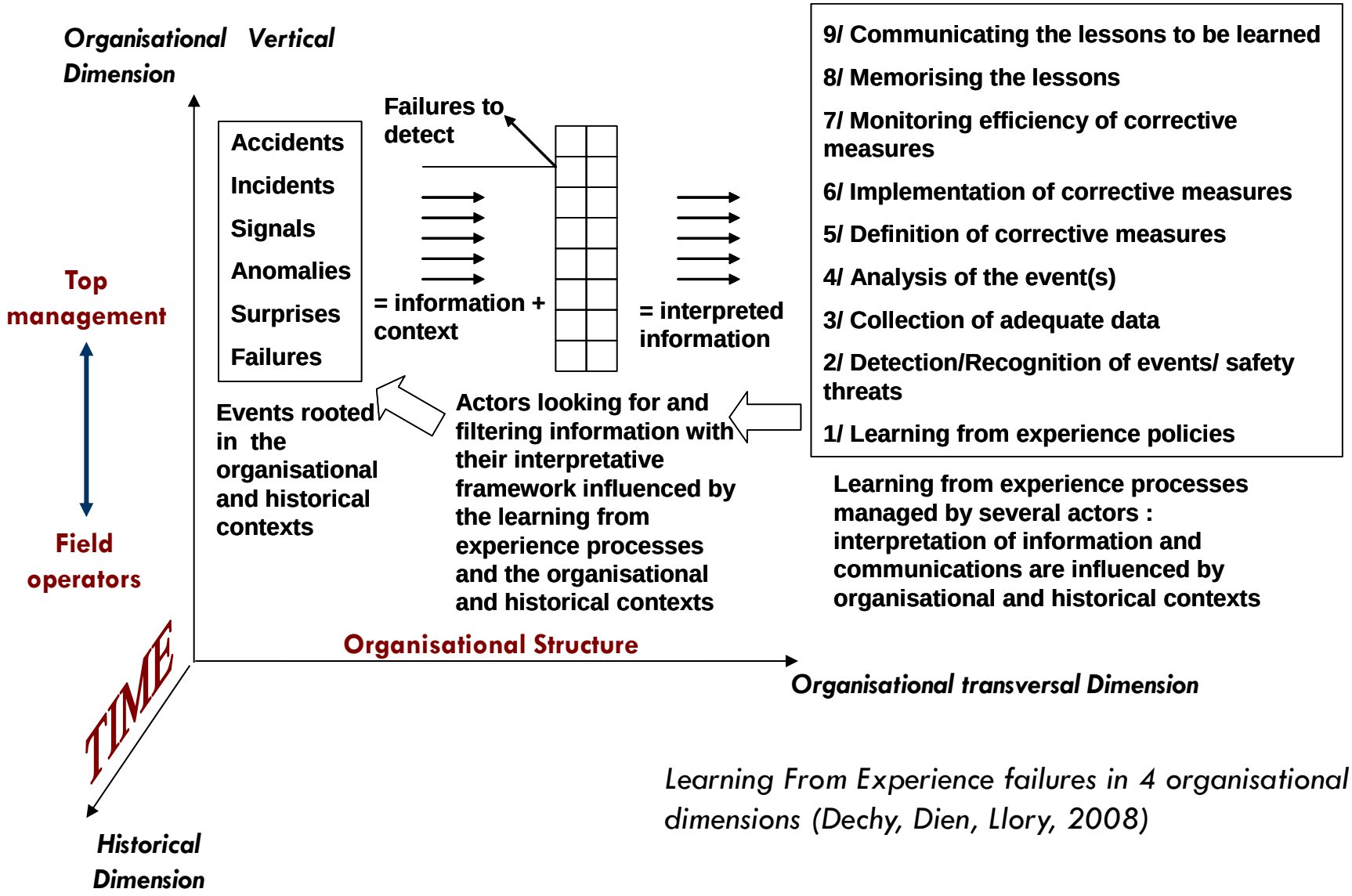
Thank you for your attention

nicolas.dechy@irsn.fr

Differences between weaknesses of incident databases versus « new view » (Knowledge and Culture of Accidents)

Concepts	A few features and weaknesses of present view of incident/accident	A new view on learning from accidents
Learning objectives	Tendency to "symptoms botany" Tendency to capitalise an heterogeneous list of cause, of data/knowledge with poor context	Search for "grammar of signs" and syndromes Search for phenomenological structures relying on sociotechnical (MTO) interaction dynamics
Learning resources	Limits (competencies, budget) for analysing events internally	More resources due to the pressure of internal/ external control authorities and civil society
Depth of analysis of the sociotechni-cal system	Low depth of analysis of incident : direct technical causes and human errors Local view (technical system, operators) Chronology limited to last actions close to the event Describe or explain approach Global analysis on a specific industrial system/sector	Root causes (human, organization, societal) including the deficiencies of vulnerability management Big picture, historical dimension and accident dynamic on longer duration, multiple causes, latent defects, incubation period More comprehensive approach Global analysis, inter-sectorial, regularities
Impact of corrective actions and generic interest	More focused on technical system within technical culture of the industrial sector, best practices, corrective actions with limited impact, local (technical system, procedure, training)	Generic character of recommendations to adapt on the specific context (by comparison and/or mirror effect)

Example of a knowledge of accidents



Learning From Experience failures in 4 organisational dimensions (Dechy, Dien, Llory, 2008)