ROSATOM

STATE ATOMIC ENERGY CORPORATION "ROSATOM"
ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

# Managing the Unexpected

**IAEA International Experts' Meeting on**
**Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant**
**Vienna, May 21-24, 2013**

**Jukka Laaksonen**
**Vice President**
**Rusatom Overseas**

**May 22, 2013**

# Outline

- Generic lessons from severe accidents
- Tangible targets for managing unexpected events
- Pre-requisites for success in managing unexpected events
- Principles and rules for managing unexpected events

# Generic lessons from severe accidents (1)

- Generic lessons can be drawn from all three severe accidents: TMI, Chernobyl, and Fukushima Daiihci
- In each case, the accident scenario was unexpected to the operators and also to the operating organization as a whole
- However, the hazards that led to severe consequences in these cases were not unknown in advance
  - when the events were analyzed afterwards, precursors for each could be identified from earlier records
  - safety measures to manage the respective risks had been suggested earlier
- One could conclude that in each case the risk of the accident was known but not properly appreciated and addressed

# Generic lessons from severe accidents (2)

- It seems that at each plant where the accident took place the risk of a severe nuclear accident was generally under-estimated
  - evidently, it was not believed that a severe accident at the nuclear power plant in question is possible
  - this general attitude influenced the safety culture in the licensee organization
  - at the management level of the licensee, the priority was clearly in profitable production rather than in safety: strong leadership for promoting safety culture was missing

# Generic lessons from severe accidents (3)

- It seems that also the leaders of the respective societies had high trust on the adequacy of nuclear safety arrangements – including both organizational and technical – and these were not seriously questioned by the political leadership.

# Generic lessons from severe accidents (4)

- In the TMI accident in 1979, the operators were not properly trained and not equipped with necessary instructions to handle the event they faced: from operators' point of view the event was therefore unexpected.
  - the response of a PWR primary circuit to a stuck open relief valve was evidently known to experts familiar with thermo-hydraulics and there had also been a similar precursor event, but the operators were not able to diagnose the state of the plant before it was too late,
  - throughout the 1970's the emergency operating procedures were based on deterministic DBA sequences, with implicit thought that abnormal events could be well predicted in advance
  - serious development of new type of procedures, which were based on addressing symptoms seen by the operators, started only after TMI accident

# Generic lessons from severe accidents (5)

- Before the Chernobyl accident in 1986, the reactor designers knew the inherent risks involved in the RBMK-type reactor design
  - clear instructions and rules on how to avoid driving the reactor into a hazardous state were given in the operating procedures that were available in the main control room
  - however, the purpose and the importance of limits set for controlling the risks had not been communicated to the operators
  - the operating culture did not give priority to safety and the production pressure caused the operators to overlook the hazards and ignore the rules written in the procedures

# Generic lessons from severe accidents (6)

- Before the Fukushima Daiichi accident in 2011, the historical data from tsunamis was known in the society but the need for tsunami protection was not properly addressed in siting and design of the plant units
  - safety authorities expressed their concerns after some large tsunamis had earlier caused devastation around the Pacific Ocean but they did not have the necessary legal power to enforce changes
  - the management of licensee organization overlooked the concerns by the safety authorities and did not believe that correcting of the initial shortcomings in siting and tsunami protection would have been worthwhile

# Generic lessons from severe accidents (7)

- We can conclude that an important root cause of each severe accident was inadequate preparation
  - the hazardous phenomena that initiated the accident sequence were known among experts
  - unfortunately, the communication between the scientific community and the operating organizations was not effective
  - this demonstrated the need to bring the research knowledge to the attention of the licensee management and to transfer the knowledge to the operator training and to the emergency operating procedures
  - **we should ask whether we have learned this lesson:**
    - **is there any better knowledge transfer organized today?**
    - **does the research community understand there responsibility to bring their knowledge to the operators?**
    - **are the operators ready to take the advice?**

# Tangible targets for managing unexpected events (1)

- For managing properly any unexpected event, it is necessary to keep the main safety target clear
- If the main safety target is so abstract that it cannot be addressed with straightforward measures, one has to specify a set of mandatory sub-targets that are necessary and adequate conditions to meet the main target
- Focus can then be on each sub-target and on the tangible measures to meet it

# Concrete targets for managing unexpected events (2)

- As stated in the IAEA Safety Standard SF-1, Fundamental Safety Principles, the fundamental safety objective is to *protect people and the environment from harmful effects of ionizing radiation*.
- The experience from nuclear power plant operation has shown that the safety objective could be achieved by eliminating the severe accidents that cause large radioactive release to the environment.
- A necessary and adequate condition for eliminating such accidents is continued provision of three fundamental safety functions: 1) control of reactivity, 2) decay heat removal from the reactor and spent fuel to the ultimate heat sink, 3) confinement of radioactive materials inside the plant
- Provision of each  fundamental safety task is a clearly specified sub-target, and meeting all of them together ensures that fundamental safety objective will be met

# Concrete targets for managing unexpected events (3)

- Two first fundamental safety functions, reactivity control and decay heat removal, are adequate to prevent severe damages to the fuel in the reactor and in the spent fuel storage. Thus the main fundamental target is met in all type of scenarios if the sub-target of ensuring these two functions is met.
- Third function, confinement of radioactive material is needed to prevent large radioactive releases in case that severe fuel damage takes place.
- Ensuring the third function should be planned to be independent of the scenario that caused loss of one of the two other fundamental safety functions. The target should be protection against any physical phenomena that is connected with severe fuel damage, no matter what was the initial event.

# Concrete targets for managing unexpected events (4)

- We can conclude that the concrete safety target to manage unexpected events at nuclear power plants is the same as the target to manage expected events: to provide the three fundamental safety functions with high reliability.
- The operating staff should thus focus on each of the fundamental safety functions and the tasks that are common to any abnormal event, whether the event is initiated by an internal hazard such as fire, an external hazard such as flood, or a malevolent act such as a large plane crash.

# Pre-requisites for success in managing unexpected events (1)

- The practical approach to provide reliable safety functions is to design and install redundant and diverse safety systems that the operators can use in flexible manner, depending on the initiating event and the event scenario.
  - For achieving the high reliability, each plant should have a proper choice of active and passive permanently installed systems, as well as transportable systems that are stored in a location from which they can be made available within a specified time.
- The operators also need robust monitoring instruments that give reliable and adequate diagnostic data from the state of each safety function, in order to be able to make an intelligent choice on using the available systems.

# Pre-requisites for success in managing unexpected events (2)

- In order to be able to use all equipment in the right situations and in the right way, the operating staff needs good basic education to understand the nature of physical phenomena and the respective risks they could possibly face in connection with an unexpected event.
- The operating staff also needs regular training to maintain its in-depth knowledge on the purpose and structure of each system that they are not using in normal operation. Training must be combined with regular exercises where use of all available equipment can be practiced.
- The skills and knowledge of the operating staff needs to be verified in connection with proper examinations [observations from examination results have shown that retraining and requalification of operators is necessary].

# Pre-requisites for success in managing unexpected events (3)

- Symptom oriented procedures and guidelines that were developed already in the aftermath of TMI accident for a number of different plant types to ensure safe management of complicated accidents are a powerful tool for managing unexpected events.
  - such procedures are valid for any scenario and are intended to ensure provision of the fundamental safety functions both in expected and in unexpected events
  - each nuclear power plant should confirm that its operators have such scenario-neutral procedures

# Pre-requisites for success in managing unexpected events (4)

- In order to ensure that adequate systems for providing fundamental safety functions are available and redundant systems are not lost due to a common cause, it is necessary to assess all internal and external hazards that could threaten the safety systems operation
  - the primary target is effective elimination of known hazards by siting of the plant or by reliable passive protection that withstands all hazards that are found physically possible on that site
  - passive protection could be provided by robust structures and/or by distance between redundant systems

# Pre-requisites for success in managing unexpected events (5)

- The licensee organizations must be ready to accept that very rare events can happen if they are physically possible and that adequate protection against such events has to be provided as part of siting and design

- External support based on use of transportable equipment should be considered if reliable and fast enough availability can be demonstrated and tested in practice.

# Principles and rules for managing unexpected events (1)

- According to IAEA's Fundamental Safety Principles "*the prime responsibility for safety must rest with the person or organization responsible for facilities or activities that give rise to radiation risks*".
  - the responsibility must remain unchanged in all operating situations and it is even more important to emphasize it during unexpected events
  - indeed, the main principle is that decision power in acute/transient phase must remain with people who have adequate basic knowledge on the plant safety features and real time knowledge on the ongoing events

# Principles and rules for managing unexpected events (2)

- In unexpected accident events the plant management and operating shift must have an opportunity to decide on actions that are aimed to reduce the radioactive releases in the long term, i.e. to prevent severe core/spent fuel damage and to protect the containment integrity, even if that would require temporary limited radioactive releases
  - strict observance on rules intended to regulate normal operation may be counterproductive for overall long term safety in unexpected situations
  - for instance, if large releases are considered unavoidable, the management should have an opportunity to make the releases in a controlled manner and to decide their optimum timing rather than wait for the release to happen as a consequence of structural failure in confinement

# Conclusions

- Managing unexpected events safely at nuclear power plants is possible if the basic targets of nuclear safety are clearly understood and addressed by those who are responsible for management decisions in advance and during the event and by those who are implementing the decided actions.
- Flexible pre-requisites, both in hardware and in human and organizational area, need to be available in nuclear power plants to manage unexpected events.
- Clear principles and rules for management of unexpected events are needed for success.