Working Group RS I 3
RS I 3 13042/9

Bonn, 16 March 2011
Extension: 2850

Initial reflections on the consequences of Fukushima

Safety check of German nuclear power plants and reassessment
As of: 16 March 2011

The ongoing nuclear power plant crisis that began in Japan on 11 March 2011 has made it necessary for Germany to review the safety of its own reactors. This applies as much to Fukushima scenarios (I) and similar damage scenarios (II) as it does to a general reassessment of risks (III). The checks must go beyond simply reproducing old results (IV). The safety checks and measures called for here must exploit state-of-the-art science and technology and be implemented at all plants in the near term and as *prerequisites* for using additional electricity produced as a result of the statutory extension of reactor lifetimes.

The following list is based on initial reflections in accordance with the current state of knowledge. It will be adapted as necessary, primarily on the basis of how the situation at Japan's nuclear plants develops, and the interim results that the safety checks produce.

I. Fukushima scenario – implications for German nuclear power plants

1. Seismic design and soil dynamics

a) A reassessment of the seismic design of plants is to be carried out in the near term. The reassessment must take account of current seismic loads and exploit state-of-the art science and technology. Any retrofitting measures necessary are to be implemented immediately.

b) The reassessment of seismic design will also take account of the effects of processes related to soil dynamics, such as sinkholes, subsurface erosion, landslides and all other types of mass wasting – as actions in themselves and as events triggered by earthquakes. Any retrofitting measures necessary are to be implemented immediately.

c) In particular, all components of all four safety levels involved in ensuring safe operation during and after an earthquake are to be checked and replaced or reinforced where necessary.

2. Flood design

a) A reassessment of flood design is to be carried out in the near term. The reassessment must take account of climate change and exploit state-of-the-art science and technology. Any retrofitting measures necessary are to be implemented immediately. Flood assessments will also consider tsunamis (in the North Sea) and large surges in neighbouring bodies of water brought about by, e.g. earthquakes or storms occurring in conjunction with flooding.

b) In particular, all components of all four safety levels involved in ensuring safe operation during a flood are to be checked and replaced or reinforced where necessary.

3. Other external occurrences

a) Plant design and operating regulations are to be checked to establish their ability to withstand other external occurrences. The checks must exploit state-of-the-art science and technology and take climate change into account. Such occurrences may include extreme weather conditions, plane crashes, cyber attacks and pandemics. Any retrofitting measures necessary are to be implemented immediately. The checks will also involve assessing the extent to which design assumptions (e.g. for earthquakes and floods) influence system design and whether the possible impacts of the failure of other systems and components (e.g. backup systems) are sufficiently taken into account.

4. Combined effects of external occurrences

Checks will be carried out to establish what combination of occurrences (e.g. earthquake plus widespread power failure) should be taken into account in reactor design according to state-of-the-art science and technology. Any retrofitting measures necessary are to be implemented immediately.

5. Specific measures

a) Checks that exploit state-of-the-art science and technology are to be carried out on plant earthquake safety, particularly with regard to emergency power supply systems and all backup and supply facilities involved in their operation.

b) The auxiliary cooling water supply necessary for ensuring plant safety must also be checked and reinforced if necessary with regard to occurrences, e.g. the presence of foreign substances like hay, molluscs and jellyfish, which may bring about a common-cause failure.

c) To make it possible to establish plant condition, checks must establish whether the control room and the emergency control are measuring system-relevant operational, fault and accident data. It is also necessary to ensure that these data are continuously communicated to the regulatory authorities (review of emergency plans). This requires redundant measurements that are transmitted via geographically separate routes.

d) Checks that exploit state-of-the-art science and technology must be performed on plant instrumentation and accident monitoring systems to ensure that meaningful data is provided even in beyond design basis scenarios.

e) Each reactor must have an emergency control room that is appropriately reinforced with concrete and designed in such a way as to allow it to be continuously manned, even during large-scale release of radioactive material on the plant site.

f) The emergency power supply must be capable of remaining self-sufficient for 72 hours.

g) Checks that exploit state-of-the-art science and technology are to be carried out on the emergency system for flooding the reactor pressure vessel (external RPV cooling). Any retrofitting measures necessary are to be implemented immediately.

h) Plants must have recirculation systems from the reactor building (BWR) or the annulus (PWR) to deal with leaks from the containment building.

i) Measures must be taken that limit the impact of hydrogen explosions – caused by malfunctioning or an accident – to such an extent that the failsafe and emergency systems remain functional.

j) For BWRs: increase the feed-in systems in a pressurized (>10 bar) RPV in addition to TJ and TM in order to reduce dependency on pressure relief and use of low-pressure systems.

k) For PWRs: increase the feed-in systems in the primary coolant loop by using a steam-powered pump, of the kind found in BWRs, that depends solely on control current, not on conduction current.

II. Similar damage scenarios

a) Checks will be carried out to establish whether, in the case of a plane crash (accidental or terrorist), it is possible to avoid a malfunction in emergency cooling or emergency power supply systems.

b) The robustness and functional duration of the emergency cooling and emergency power supply systems (emergency diesel generator, batteries) are to be checked to establish their ability to handle long-term infrastructure failure (e.g. of the external power supply).

c) All emergency diesel generators must be contained in concrete.

d) Pipelines for cooling the safety systems must be laid in concrete-reinforced, accessible channels.

e) Emergency cooling and residual heat removal systems are to be fully upgraded to include four trains, each with 100% residual heat removal capacity. The four trains should feature 2+2 diversity. All trains must be fully protected from external influences and, where necessary, set up in separate areas.

f) Every plant should also be retrofitted with a steam-powered, battery-backed high-pressure feed-in system similar to the relevant systems at German "construction line 69" boiling water reactors and the Biblis A pressurized water reactor. These systems are designed to withstand a station blackout.

g) To cool spent-fuel storage pools, plants should, in addition to the two emergency cooling and residual heat removal trains leading to them, be equipped with two additional cooling trains with 2 x 100% capacity. At least one of these trains must be fully encased in concrete and flood-protected.

h) Emergency power systems that supply power to the emergency cooling systems must be fully upgraded to 4 x 100% emergency power capacity. The four trains must be constructed diversely. Two pairs of 100%-capacity trains in which the active emergency power components are constructed using a different design.

i) Mobile emergency power generators must be set up and the necessary feed-in points installed to ensure that they can be connected immediately and supply devices that are important to plant safety.

j) All plants should be retrofitted with additional emergency systems. These are standard in pre-Konvoi and Konvoi plants. The retrofitted emergency systems should be consistent with the emergency cooling and residual heat removal systems and the emergency power systems. This means that, instead of 4x50% capacity like in Konvoi plants, the plants should be retrofitted with diverse systems of 4x100% capacity – divided into 2x100% + 2x100% with differently designed active components. The emergency systems must be encased in concrete.

k) The coolant inventory in boiling water reactors is to be increased by using larger coolant containers, which must feature a fail-safe design. The capacity of flood tanks in pressurized water reactors must be increased.

l) In pressurized water reactors, to guarantee the third barrier in secondary cooling through steam relief via the roof, pressurized water reactors should be retrofitted with a secondary condensation chamber. This chamber should have a water inventory that serves as a receiver tank for steam relief, as is the case with boiling water reactors. It should also be possible to feed the water back into the steam generators. A heat transport system must be installed for the secondary condensation chambers in PWRs.

m) The spent-fuel storage pool must either be installed inside the containment building, or equipped with a similar barrier that will prevent radioactive material escaping.

n) Plants should be equipped with on-site, separated water wells that are earthquake and flood-protected and have boron storage tanks, mobile emergency power generators and pumps.

III. General reassessment of risks

a) The new nuclear regulations *(Sicherheitskriterien für Kernkraftwerke – Safety Criteria for Nuclear Power Plants)* must be implemented immediately.

b) The individual defect plan must be checked, also according to the assumption that several individual defects may occur at once.

c) Proof must be obtained that the plant can contain design-basis accidents which can be assumed to occur according to current scientific and technological standards (Module 3 of the *Security Criteria*).

d) An effective IT security concept must be implemented in the near term in all German plants. This will ensure that attacks on IT systems will not compromise the safe operation of plants.

e) Digital reactor protection systems should only be introduced if they can offer the same protection against tampering as the analogue technology currently in use.

f) Power failure (e.g. in the case of simultaneous IT attacks on facilities involved in the power supply infrastructure) must not impact on the safety of a nuclear power plant.

g) Checks must be carried out to establish whether IT attacks on several plants at once can trigger simultaneous emergency shutdowns.

h) Improvements to plant safety based on the *Nachrüstungsliste* (retrofitting list) of the Federal Ministry for Nuclear Safety should be carried out in the near term, without subjecting retrofitting requirements to considerations of probability (P2 points), as a prerequisite for using additional power produced as a result of the extension of reactor lifetimes.

i) The quality of facilities and measures for containing occurrences that were previously assigned as rare occurrences to Safety Level 4a, should be moved up to Safety Level 3.

j) Checks that exploit state-of-the-art science and technology should be carried out to establish the quality and efficacy of the facilities and measures in Safety Levels 4b and c.

k) The design of reactor pressure vessels and their components in "construction line 69" boiling water reactors must be assessed for all weak spots arising from fatigue and embrittlement. The assessment must be based on procedures that reflect state-of-the-art science and technology and take into account all possible stresses (relevant core loading, enrichments, burn-up situations, vibrations). Limitations to the ability to identify cracks and possible corrosion should be taken into account in the process.

l) Checks must be carried out to ascertain whether containers and pipelines in pressure boundaries can withstand, for the foreseen operating time, all possible stresses assumed possible according to state-of-the-art science and technology (plane crashes, earthquakes, malfunctions, ATWS). Conditions (fatigue, displacement, vibrations, distensions) must be constantly monitored and evaluated.

m) For all containers and pipelines, proof must be provided that the fixing elements (e.g. wall plugs) of the systems involved in plant safety comply with state-of-the-art technology and can withstand all possible stresses.

n) Switching off safety cooling systems for precautionary maintenance during operation is not permitted. These systems should only be switched off during general inspections.

IV. Checking procedures

a) A team of expert assessors will be set up for each plant. Members will come exclusively from specialist organisations that have not served as the main assessors at the respective reactors, i.e. other branches of the organisations TÜV, GRS, Öko-Institut, Physikerbüro, ESN, etc.

b) The federal supervisory authority must receive all requested documents, without limitation, and shall consult with the Reactor Safety Commission (RSK) on superordinate issues.

c) All plants must implement the measures called for here in the near term and as a prerequisite for using additional power produced as a result of the extension of reactor lifetimes.