Senior Regulators' meeting

19 September 2013

Chairperson's Summary

Session 1 was on *Benefits and Future Development of the Integrated Regulatory Review Service (IRRS) Programme*

In summarising the first session, is first of all very pleasing to note that the number of completed missions is now approaching 50 and that 25-odd missions are planned for the next couple of years. An increasing fraction of the missions are follow-up missions. This is expected as it will take some time to establish a steady state, but the importance of a follow-up mission cannot be overstated, as this is the confirmation of host countries actually being serious about their self-assessment and action plan.

A second point, which has been made many times also in many other fora, is that IRRSs are not beauty contests. The number of recommendations, suggestions and good practices is not a quantitative assessment of the state of safety in the host country, and it is not a reflection of resources and/or maturity. In my experience there isn't a mature programme where there isn't room for recommendations; nor is there a programme so small and under-resourced that there aren't any good practices that can be identified. Maybe the constraints themselves have even stimulated innovative approaches, for others to take note of. There should be no hesitation for a country to embark on an IRRS out of fear of not "looking good". IRRS plays an important role no matter the level of maturity. It should be noted though that for a small country with constrained resources, the work load, even with the support of the new SARIS tool for self-assessment, can be daunting. The Agency's support for IRRS missions to such countries is vital.

A third point is that a peer review is about getting good advice from colleagues. Good advice happens only when *the host country* is forthcoming and honest in the self-assessment and in their interaction with the review team, and through developing a robust action plan and implementing it. *The review team* also needs to go about their review seriously and be clear with its advice, focussing on strategic actions that are implementable. Long lists of detailed advice are not helpful, nor is advice against which you cannot measure improvement. Also, although a peer review is about getting good advice from colleagues, the review needs to have 'teeth'. If a problem arises or in the worst case scenario, an *accident* happens, and it turns out that a systemic issue was there but was not identified during the mission, or that actions recommended by the mission were not implemented, the credibility of the peer review system could be seriously undermined – just as the global framework for safety itself.

The question is how the observations from peer reviews can be picked up in other fora to support actions to reinforce the global nuclear safety framework. One of the easiest ways is to be fully transparent and publish the full reports, not only the executive summary, which is the case for about half of the missions. Also, only few countries publish their action plans. Mandatory reporting of IRRS findings to the review meetings of the Convention of Nuclear Safety is favoured by many Member States as well as Contracting Parties to the Convention. The EU has already made mandatory, through the Nuclear Safety Directive, that peer reviews should be performed every 10 years and have agreed internally that IRRS is the most suitable mechanism. The IAEA could potentially have a role in advising governments if there are concerns over the national implementation of the safety infrastructure.
Clearly, the IAEA has a role in aggregating and analysing the results of all IRRSs to evaluate trends and shortfalls in the global nuclear safety infrastructure. The aggregated information from IRRSs might be the best indicator we have of the progress in improving nuclear safety internationally.

Session 2 concerned *cyber and information security from a regulatory viewpoint*.

The rapid growth in the global reliance on cyber systems to aid our daily undertakings has created new and emerging threats and vulnerabilities which have implications for Governments. The threat of a cyber-attack has implications for a wide number of industries within Member States including national defence, financial sectors, and Government - and the nuclear industry is not alone in this regard. Member States have assessed and envisaged that the impact associated with a cyber-attack for nuclear installations, nuclear and radiological sources and their associated facilities could vary widely, ranging from the disruption of normal day to day activities and, for the more severe considerations, potentially result in on-site, off-site and trans-boundary nuclear incidents or accidents.

Clearly, regulators, along with other government agencies and facility operators have a central role to play in the challenge of strengthening cyber security and minimising the impacts (and where possible ensuring the prevention) of cyber-attacks.

Cyber and information security should make sure that the information is protected, that it is correct (i.e. has not been tampered with), and is available to the right client at the right time. The objective is no different from radiation protection, safety, security and safeguards: to protect people and the environment from harmful effects of ionising radiation. The approach is one of defence-in-depth.

One particular issue is the safety-security interface, causing much debate and sometimes frustration inasmuch as timely actions to promote safety can at least sometimes be perceived as being hindered by security measures, or *vice versa*. This is an important debate but one that can only be approached by further exploring the interface and establishing the appropriate balance. A few years back, the then Chairs of AdSec and of CSS wrote to the IAEA DG establishing their vision of a holistic approach. There is movement in this direction

but progress is slow. Module 12 of the IRRS discusses the interface of nuclear and radiation safety with nuclear security.

In conclusion, cyber and information security is an important area for all States, where clear strategies and flexibility are needed to meet the growing threat of cyber-attacks. The IAEA has a strong, central role to play in assisting States and in issuing recommendations and guidance to support States in developing their national regulations.

Session 3 was about *establishing and strengthening the regulatory infrastructure in States without nuclear power plants; the constraint of limited resources* and was followed by a panel discussion: *effective mechanisms for supporting regulatory infrastructure*.

Currently as many as 134 countries receive Agency assistance and this number is still growing although at a slow rate. The Agency is being informed of the status in the Member States through information held in the Radiation Safety Information Management System (RASIMS). Over the last few years we have seen the number of countries where there essentially was no infrastructure drop by about a third – still, the infrastructure in some 20 countries remains very poor. This is an impediment to the technical assistance to such countries; e.g. the introduction of radiotherapy with clear health benefits to the population will be delayed until such time it can be considered safe (from the radiation safety point of view) to introduce such techniques.

Notably, radiation safety is not only about the technique as such; it is about the culture, i.e. the approach, training, awareness, priorities, resourcing (human and otherwise) and other factors that are commonly captured under the umbrella term *safety (and security) culture*.

The deliberations during the session and panel discussion clearly demonstrated that although it is a prerequisite for receiving TC assistance, many States continue to face major challenges in establishing adequate radiation safety infrastructure. This is most acute in the area of patient protection, where the regulatory infrastructure needs to be put into place as quickly as possible, in order to receive assistance that saves lives.

All cooperation levels must be exploited: bilateral, regional and international. Mentoring between countries and permanent/optimized networking are also efficient mechanisms to be developed. On a positive note, however there is a variety of mechanisms for support, noting that ‘one size does not fit all’ and substantial financial support (€128M in the last 10 years) has been made available for improving the regulatory infrastructure. Yet more efforts need to be made to ensure that the support provided actually leads to significant, sustainable improvements. We heard a variety of suggestions for possible ways of doing this, for example through raising awareness of decision makers in government, focussing more on enhancing safety culture, reassessing how groups of countries are clustered in the TC programme, conducting peer reviews and workshops on the safety and security of sources at a regional level so as to capture the movement of sources across shared borders,

and providing training to younger individuals who are expected remain within an organization for many years to come. In general, it seems that the further improvements would involve continuous improvement of the efficiency and effectiveness of the current system rather than seeking to explore completely new approaches.