INTERNATIONAL EVENT ON

INCIDENT PLANNING AND EMERGENCY RESPONSE

VIENNA, AUSTRIA

12-15 FEBRUARY 2018

BACKGROUND

Planning for and managing the response to major security incidents at nuclear facilities can be extremely challenging if the wrong approach is used. How are command, control and communication among different departments or organisations best designed and implemented? Why is interoperability important? What happens if it fails? Who has the controlling mind for nuclear safety and security? What are some common challenges in managing this critical interface? What specialised safety training do armed response forces require in order to discharge their responsibilities without compromising nuclear safety?

In order to discuss these issues, World Institute for Nuclear Security (WINS) and Bruce Power (Canada) jointly held an international event on Incident Planning and Emergency Response drawing on experiences and best practices from managers and specialists from the nuclear and emergency response communities, and other governmental organisations.

During the first two days of the workshop, discussions focused on the experiences and lessons learned by those who have designed and implemented frameworks and strategies to achieve effective nuclear security programme and security incident management. Day 3 consisted of a table-top exercise (TTX) that gave participants the opportunity to identify and address some of the potentially complex issues that could arise when responding to incidents. The hypothetical scenario allowed participants to react in real time to a situation, discuss how they would approach it, and ultimately identify possible improvements they could make in their existing response arrangements.

OBJECTIVES OF THE TRAINING

WINS and Bruce Power jointly conducted an international event on Incident Planning and Emergency Response from 12 to 15 February in Vienna, Austria. The event was built upon the successes of related workshops held in Pretoria in October 2017 and Toronto in December 2016.

The content was based on the WINS Academy Elective on Nuclear Security Incident Management, supplemented by the opportunity to interact with highly experienced emergency management experts from Bruce Power and other nuclear organisations. The 3-day programme gave participants the opportunity to identify and address potentially complex issues that can arise when responding to security incidents (including command, control and communications) and to translate concepts and principles into relevant and effective planning tools and deployment in an operational context. Participants took part in a fast-moving security scenario where they were able to test their knowledge and decision-making. Participants enrolled on the WINS Academy course had the opportunity to take the examination immediately after the course finished.

TRAINING PROCESS

The event, which was moderated by **Mr Carl Reynolds**, focused on issues such as:

1. Identifying how command, control and communication among different departments or organisations are best designed and implemented;
2. Exploring the importance of interoperability and what happens if it fails;
3. Describing and understanding responsibilities for approving the plans and how the planning documentation is structured
4. Understanding competencies of the guard force and rules of engagement;
5. Identifying and addressing common challenges in managing the critical interface between nuclear safety and nuclear security.

International experts gave a variety of presentations during the sessions, setting the scene for the discussions that followed. Mr Reynolds guided the discussions using such methods as plenary sessions, table and breakout discussions, and expert panels. An instant electronic voting system (e-voting) was used during the workshop to learn more about participants' opinions and concerns. Some results of these votes are illustrated in this report.

EXPECTED OUTCOMES

The expected outcomes of the training were that participants would better understand:

- The importance of having a national nuclear security strategy and challenges when implementing such a strategy.
- The information on existing guidance for emergency response and incident management.
- Who internal and external stakeholders involved in nuclear security incident management are.
- What we can learn from real-life examples.
- Onsite emergency planning and arrangements, and structure of planning documentation.
- The relationship between the operator and offsite responders and arrangements for the information sharing.
- Best practices for the interface between emergency programmes and the security department.
- The complexity of command, control and coordination in a multiagency environment of a nuclear security emergency.
- The principles of interoperability and range of arrangements that need to be put in place.
- The rules of engagement and competencies of the guard force.
- Effective exercises and tools that can be used to exercise the guard force.
- How to ensure that "lessons identified" from security exercises are translated into "lessons learned" in order to improve operational effectiveness.

DAY 1

OPENING SESSION

Dr Roger Howsley, WINS Executive Director, welcomed the participants, provided a preliminary overview of the importance of incident planning and arrangements for emergency response, and introduced the scope, objectives and agenda of the workshop.

In addition, the opening session gave organisers the opportunity to explain how the training would be conducted, highlight the expected outcomes, and briefly introduce the key topics for discussion.

Participants' introduction and expectations

Participants were first asked to introduce themselves; they were then asked to use the e-voting system to indicate which sector they represent. Following are the results.

Prior to the training, participants were asked to take a survey about what they hoped to achieve by attending the training. Mr Reynolds presented the key outcomes of their responses and asked them to reflect on these key outcomes with the other participants at their table and to identify new outcomes if appropriate. Following is a summary of their responses.

- ❑ Share knowledge and experience
- ❑ Learn how to overcome communication challenges when coordinating during an emergency or crisis
- ❑ Share the best security practices in case of emergency or incidents
- ❑ Learn about practices and security systems in other countries
- ❑ Understand how to clearly define roles in emergency response arrangements
- ❑ Understand better how the effective emergency response coordination is managed and controlled

SESSION I: SETTING THE SCENE

The purpose of the 1st session was to introduce participants to the topic of nuclear security strategy and achieving an effective nuclear security programme. Another purpose was to describe

some challenges when implementing such a strategy. The third was to discuss information on existing guidance for emergency response and incident management.

Presentation

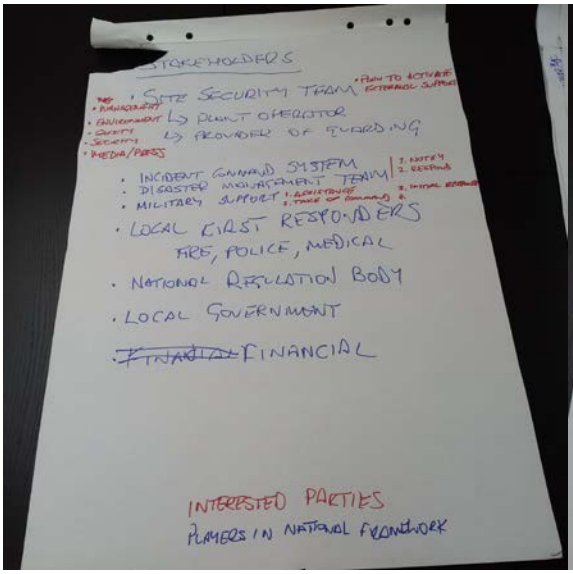
Mr Nigel Tottie, International Atomic Energy Agency (IAEA), opened the Session I with the presentation titled *"Developing a National Framework for Managing the Response to a Nuclear Security Event"*. He provided an overview of how an effective national response framework can support States in managing their response to nuclear security events. He also discussed how nuclear security is addressed at the international level, predominantly by Convention on the Physical Protection of Nuclear Material (CPPNM) through obligation on reporting of nuclear security events with trans-boundary implications. He talked about the IAEA publications which provide guidance on the developing and implementing a national framework, its design and infrastructure. Mr Tottie concluded his presentation by mentioning some common challenges, lessons and recommendations for developing the national framework and emphasized the importance of multi-agency cooperation.

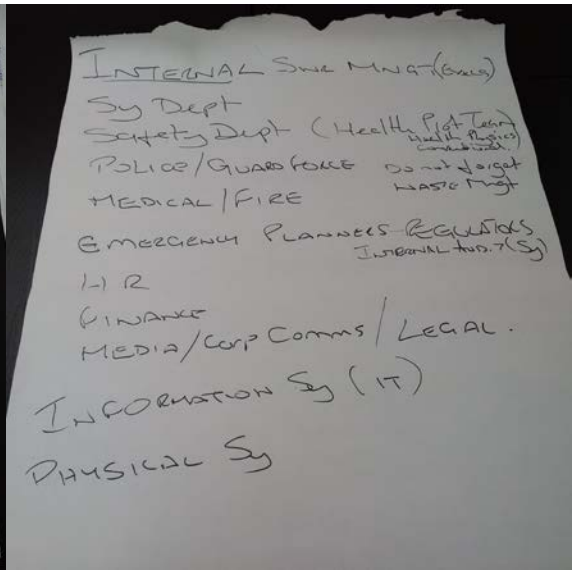
E-voting

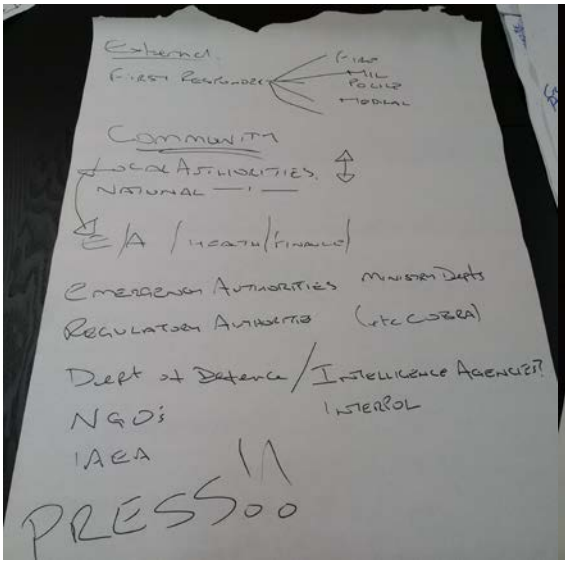
An e-vote was taken to elicit participants' opinions on whether all stakeholders have been identified and properly involved in the development of the incident management strategy in their countries. One third of the audience indicated that all stakeholders have been identified and involved in the incident management strategy, while the other third said that is done only partially. The rest of the audience replied that the stakeholders have not been identified and involved or that they did not know if that had been done.

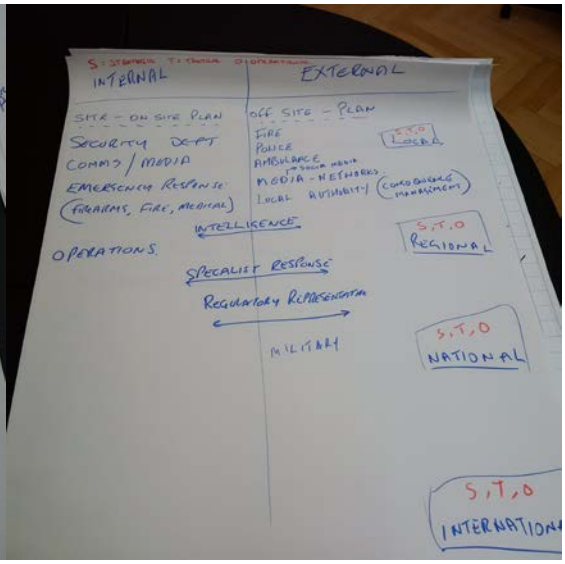
Group discussion

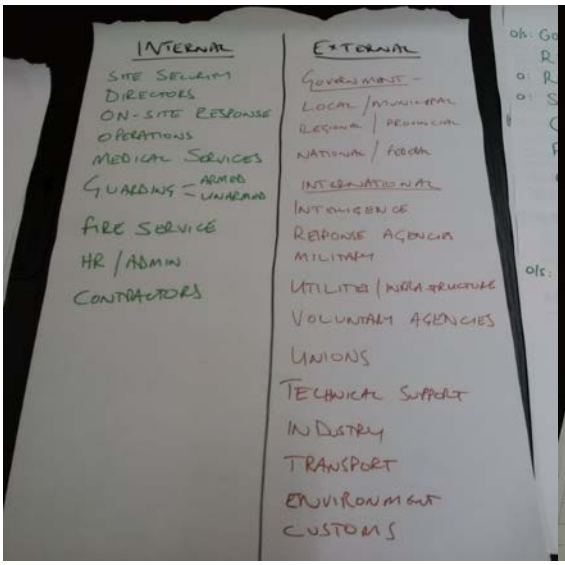
As a follow-up to the presentation, participants were asked to identify and discuss internal and external stakeholders involved in nuclear security incident management and to identify their respective roles and responsibilities. Participants agreed that stakeholders can be identified on different levels: local, regional, national and international, and that it is vital to define the lines of command and communication as the decisions made at different levels have different impacts. Following are some key findings:

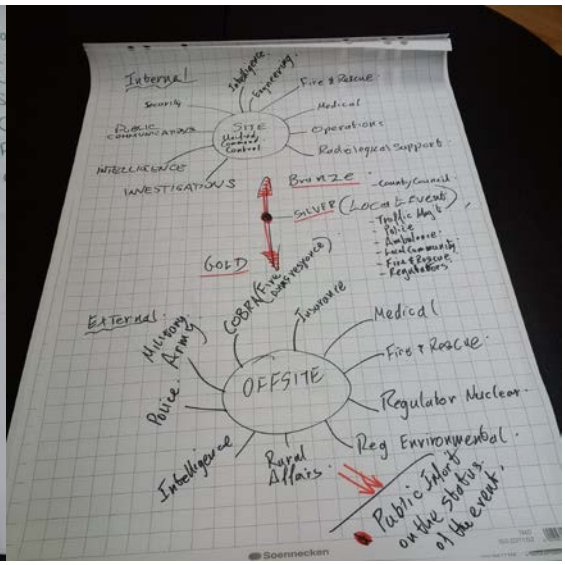

STAKEHOLDERS
SITE SECURITY TEAM
PLANT OPERATOR
PROVIDER OF GUARDING
INCIDENT COMMAND SYSTEM
DISASTER MANAGEMENT TEAM
MILITARY SUPPORT
LOCAL FIRST RESPONDERS
FIRE, POLICE, MEDICAL
NATIONAL REGULATION BODY
LOCAL GOVERNMENT
FINANCIAL
INTERESTED PARTIES
PLAYERS IN NATIONAL FRAMEWORK


INTERNAL
Sy Dept
Safety Dept
POLICE/GUARD FORCE
MEDICAL/FIRE
EMERGENCY PLANNERS
L-I-R
FINANCE
MEDIA/CORP COMMS/LEGAL.
INFORMATION Sy (IT)
PHYSICAL Sy


External
FIRST RESPONDERS
FIRE
AMB
POLICE
MEDICAL
COMMUNITY
LOCAL AUTHORITIES
NATIONAL
EMERGENCY AUTHORITIES
REGULATORY AUTHORITIES
(ie COBRA)
Dept of Defence/INTELLIGENCE AGENCIES?
NGO's
INTERPOL
IAEA
PRESS

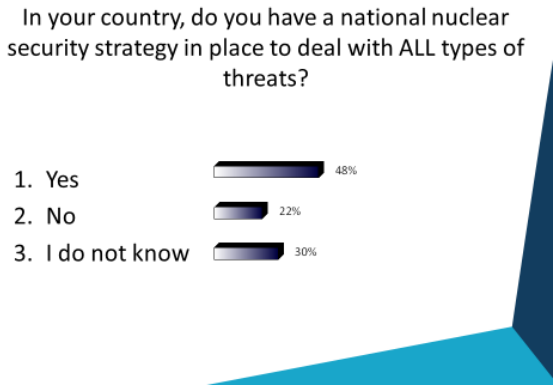

INTERNAL
EXTERNAL
SITE - ON SITE PLAN
OFF SITE - PLAN
SECURITY DEPT
COMMS/MEDIA
EMERGENCY RESPONSE
(FIREARMS, FIRE, MEDICAL)
FIRE
POLICE
AMBULANCE
MEDIA - METHODS
LOCAL AUTHORITY
OPERATIONS
INTELLIGENCE
SPECIALIST RESPONSE
REGULATORY REPRESENTATIVE
MILITARY
S.T.O LOCAL
S.T.O REGIONAL
S.T.O NATIONAL
S.T.O INTERNATIONAL


INTERNAL
SITE SECURITY DIRECTORS
ON-SITE RESPONSE
OPERATIONS
MEDICAL SERVICES
GUARDING - ARMED - UNARMED
FIRE SERVICE
HR/ADMIN
CONTRACTORS
EXTERNAL
GOVERNMENT -
LOCAL/MUNICIPAL
REGIONAL/PROVINCIAL
NATIONAL/FEDERAL
INTERNATIONAL
INTELLIGENCE
RESPONSE AGENCIES
MILITARY
UTILITIES/INFRASTRUCTURE
VOLUNTARY AGENCIES
UNIONS
TECHNICAL SUPPORT
INDUSTRY
TRANSPORT
ENVIRONMENT
CUSTOMS


Internal
Intelligence
Engineering
Fire & Rescue
Medical
Security
Public Communications
SITE
Operations
Radiological Support
INTELLIGENCE
INVESTIGATIONS
BRONZE
SILVER
GOLD
External
Military/Army
COBRA
Insurance
Police
OFFSITE
Medical
Fire & Rescue
Regulator Nuclear
Reg Environmental
Intelligence
Rural Affairs
Public Info on the Status of the event.

Evoting

As an introduction to the part of the session focussing on national arrangements, participants were asked if their countries have a national nuclear security strategy in place to deal with all types of threats. The majority said that such strategies exist in their countries, but some participants pointed out the inability of any strategy to address and deal with all types of threats.



Presentation

Alex Zapotoczny, Canadian Nuclear Safety Commission (CNSC), Canada, provided the overview of Canada's nuclear emergency management regime, addressing issues such as Canada's commitment to nuclear security, who the competent authorities are, legislative and regulatory framework, contingency planning, and stakeholders' responsibilities. He explained how Canada's commitment to comply with the CPPNMNF is the key in establishing regulatory framework for nuclear security. Mr. Zapotoczny also described different tiers of regulatory and legislative framework, competent authorities and their responsibilities, with a particular focus on the division of responsibility in case of a security incident and documents outlining the arrangements between different institutions. He noted that, although Canada has extensive response plans, there were many challenges in building the nuclear emergency partnership and there is still a lot of room for improvement.

Group discussion

As a follow-up to the presentation, participants were asked to form sub-groups and select a spokesperson who should draw up their national schematic and share it with the other members of the group. Other members of the group then pointed out similarities and differences to their national arrangements. As participants pointed out differences in their national emergency management regimes, they agreed on some common issues, such as the importance of procedures in place identifying responsibilities of each stakeholder and ability to exercise those responsibilities jointly with other competent institutions in order to integrate the procedures effectively.

DAY 2

SESSION II: ONSITE EMERGENCY PLANNING AND SECURITY INCIDENT MANAGEMENT

The objectives of Session II were to describe emergency planning and security incident management arrangements, understand responsibilities for approving the plans, and describe how the planning documentations is structured. Group discussions provided an opportunity to further explore the roles of different stakeholders, importance of information sharing, and common challenges facing the cooperation between different stakeholders.

Presentation

Mr. Kevin Slater, Sellafield Ltd, United Kingdom, opened Session II with a presentation titled *"Sellafield Ltd. Security Preparedness/Response*". He began by giving an overview of serious threats the UK is facing and then focused on security challenges at Sellafield and how the security competence and capability are built and improved. Dividing the control of Sellafield emergency situation in strategic, tactical and operational, he explained how the responsibilities are divided among the stakeholders and relevant departments, and how configuration of site emergency control centre looks like. Mr. Slater also explained how Sellafield ensures a measured performance through a consequence-based approach, exercises, competency assessments, and exercise evaluations. In addition, he presented Sellafield's Main Site Command Facility and emphasised the benefits of co-location delivered through enhancements in processes, organisation, technology and information flows.

Group discussion

Participants were then asked to identify the information the operator needs to know about offsite responders and the information the offsite responders need to know about the operator, and how this information is communicated to one another. Following are some key findings.

What does the operator need to know about the offsite responders:

- Response time
- Standard entry procedures, what happens when they are no longer in effect, and how to understand what alternatives are available
- Identification protocols for offsite response
- Tactics, training, equipment
- Legislation
- Knowledge sharing and planning

What do offsite responders need to know about the operator:

- What hazards are on the site
- Operator's emergency procedures
- Risk exposure
- Access arrangements
- Layout of the facilities
- Environmental impacts and surroundings

How is this information communicated to one another:

- Creating a memorandum of understanding
- Regular reviews of MOU
- Complying to the MOU and building the trust and confidence
- Communication

- Regular exercises
- Working groups and interoperability meetings

Presentation

Shaima Al Mulla, Nawah, UAE, presented the Nawah emergency preparedness and security response program, which focuses on Barakah Nuclear Power Plant and its offsite stakeholders. She gave an overview of different types of emergencies and responses required for each type, explained how the flow of information, command and control is established, and what the main responsibilities of the site plant security are when responding to a hostile action. Concluding the presentation, she pointed out the importance of a comprehensive all-hazards programme and the importance of commitment to protect the health and safety of the public and environment from a potential radiological event in the area surrounding the power plant.

Presentation

Dave Maloney, Bruce Power, Canada, gave an overview of how to plan for a nuclear security incident/crisis at Bruce Power, which included the differentiation between incident and crisis, explanation of incident management hierarchy and incident management team. He also described the response to a nuclear security incident/crisis, security incident command, and decision making process. He briefly showed how security at Bruce Power changed in the last 17 years and how the current command framework combines strategic, tactical and operational levels and what their responsibilities are. He discussed different notions that are part of the decision-making process in the event of a security incident and presented the decision-making model used by Bruce Power, which outlines a set of question which help to make an informed decision.

Group discussion

Participants were given a draft Memorandum of Understanding and divided into four groups. Using the draft MOU and based on their professional experience, they were asked to identify where the major problems would occur in developing and agreeing the MOU. Each group was given one aspect of the MOU where they needed to identify what could go wrong and how to solve it. Group 1 focused their discussion on rules of engagement. They pointed out that the major challenge is setting the scope and limits of force used by onsite and offsite response teams. Onsite response force responds to theft or sabotage and is authorised up to lethal force; offsite teams might respond with lethal force in order to protect life, not against theft or sabotage. Group 2 discussed the problems and possible solution regarding the control of site access and egress. They concluded that the procedures needed to be pre-defined, but the possible challenges might be the broken, corrupted or unstable communication flow, information not reaching the relevant groups/individuals, or equipment failure causing communication problems. The third group discussed information handling and stated that this particular aspect is the largest bit of the MOU and the most difficult to achieve. In order to overcome the challenges facing the information handling, the same level of information should be shared, secure lines set up for transmission of information, equipment integration checked and resources invested in exercises and drills. Group 4 discussed communications and identified possible challenges including classification, differences in terminologies, silo mentality and blame culture. They concluded that these challenges need to be dealt with in order for the communications to be improved and the relevant stakeholders to learn and grow as a team.

SESSION III: COMMAND; CONTROL; AND COORDINATION

The final session of day 2 was designed to broaden the understanding of terms command, control and coordination in the context of nuclear security and how complex they have become in the multiagency environment of a nuclear security emergency. Other objectives of this session were to understand the principles of interoperability and joint working and the range of arrangements that need to be put in place.

Presentation

Mr Brian Welsh, Joint Emergency Services Interoperability Programme (JESIP), United Kingdom, provided the group with a UK view of interoperable working, challenges the UK institutions have been facing over time, such as lack of communication between commanders and responders, lack of understanding or proper sharing of risks and information, inadequate training and lack of audit process. He then described the joint approach taken by the relevant stakeholders and communications and engagement strategy which included the joint doctrine, training, testing and exercise and joint organisational learning. He concluded by emphasising the need for common systems and appropriate standards for establishing and maintaining interoperability and the importance of team work and team effort, open, honest relationship and focusing on the same goal.

Presentation

Ms Dana Early, Ontario Provincial Police, Canada, gave a presentation titled *"A Collaborative Approach to Critical Incident Management"*. She described the obligations and responsibilities of the OPP, focusing on the specialty units within the organisation. Talking about the critical incident management, she pointed out that the key to successful planning is thoughtful preparation and that in order to succeed during a major or critical incident there must first be a solid relationship built on trust and an understanding of each party's role, responsibilities and capacities. She discussed the major points of the MOU and its role in solidifying the relationship, encouraging ongoing communication and information sharing, and defining a critical incident and critical incident command.

Group discussion

As a follow-up to the presentations, the participants were asked to assess the level of coordination and cooperation amongst the key stakeholders and identify factors that that are making coordination and cooperation more difficult with some of these stakeholders, basing their conclusion on their experience as much as possible. They were also asked to discuss opportunities to generate collaborative working relationships and mutual understanding "difficult stakeholders" and provide real life examples where possible.

Some of the key issues with proper engagement with stakeholders are summarised below:

- Local Municipalities: complexity of keeping plans and Point of Contacts up-to-date; Some security concerns associated with disclosure of information
- Bringing safety and security disciplines together: Two different mind sets/cultures. Timing/dynamics of the safety and security incidents might differ a lot. A possible solution is to create mixed teams. Developing an all hazard approach may help;
- Media communication: Communication plans during normal time are usually effectively in place; the challenge is to handle media pressure during crisis. Ability to control social media?

- Legal basis is often still missing. Difficult to demonstrate that required security measures are effective. The distribution of responsibilities amongst stakeholders may need to be clarified. The decision making process for the deployment of the armed response adequate could be improved. PR plans are missing. Many of these things already exist but need to be raised to international best practice level.
- Political level: Political cycles lead to extended discussions, delay in decisions and funding; short term interest of the political decision makers vs. Long term perspective of the nuclear industry.
- Regulators: Demonstrating the competence of regulators (especially for the policing component) is sometimes an issue. Proper selection of the regulatory team can increase credibility and expertise. It is important to balance the workforce with various background. Financial component might be a challenge to attracting best experts.

Presentation

Col. Mapotsane Francina Moloi, South African Police Service, South Africa, gave a general overview of physical security management at national key points and strategic installations. She discussed the differences in the roles of the SAPS in protecting the national key points and strategic installations, including the development of minimum physical security and training standards, issuing physical security directives and regulations, and roles of the institutions (NKPs and strategic installations) including, among others, complying with the regulations, resourcing physical security improvement and ensure maintenance.

Presentation

Col. Etheresa du Plooy, South African Police Service, South Africa, discussed further and in more detail the actual incident management procedures and specific duties and responsibilities that both SAPS and NKPs have in such situations. She also talked about the symptom based incident management model used by the SAPS, its components and steps for its realisation. She concluded the presentation by addressing some common challenges SAPS is faced with in terms of the NKP security and the role the regulator has in meeting (and posing!) the challenges.

Group discussion

As a conclusion to the Session III, the participants were provided with some scenarios and asked to discuss the manner in which the situation impacts the relationship between the armed police and the licensee, what factors need to be taken into account, and what potential impact the answers have on the model MOU. The participants pointed out that good relationship between senior management and guard force commanders is critical to an effective security regime. Regulations or codes of conduct may help and spirit of collaboration is vital. Also, the relationship between armed/response force and the staff is important and should be based on mutual respect. Rules should be designed and implemented but taking into account the human factor.

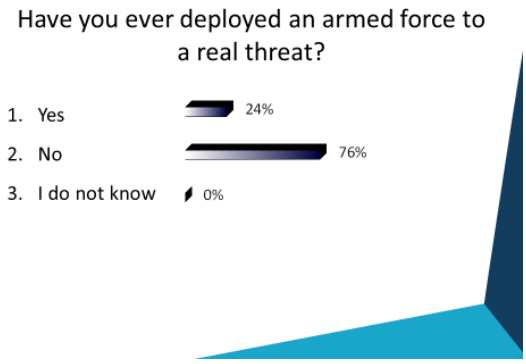
DAY 3

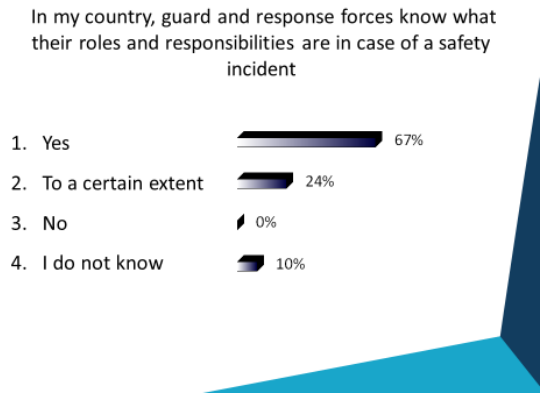
SESSION IV: GUARD FORCE DEPLOYMENT

The objective of Session IV was to discuss the competencies of the guard force, both armed and unarmed, discuss some effective exercises and tools that can be used to train and exercise the guard force, and understand the issues around the rules of engagement, including the use of deadly force.

Evoting

As an introduction to the presentations and group discussions, participants were asked a series of questions regarding the response and guard forces.





The majority of the participants answered positively to the question whether the security plans and procedures are exercised regularly in their organisation. When asked if they ever deployed an armed force to a real threat, majority of participants replied that they did not. The participants were also asked if the guards and response forces in their country knew what their roles and responsibilities were in case of a safety incident. Majority of participants replied positively to this question.

Presentation

Mr Greg Briggs, Bruce Power, Canada, gave a presentation titled *"Nuclear Security Training and Exercises"*. He discussed the objectives and impact of the exercises, their key components and the basis for conducting them. By presenting the examples from his organisation, he discussed the types of exercises and their purpose, highlighting the importance of development of candidates through the exercises in order to maximise the resources and support the needs of the organisation. He concluded by pointing out some key factors to consider while developing security exercises, such as regulatory requirements, safety, impact to operations and stakeholder engagement.

Group Discussion

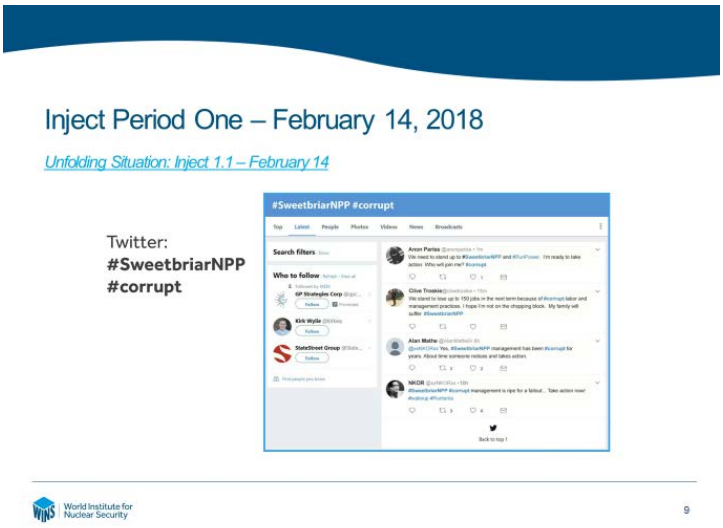
As a follow up to the presentation, the participants were asked to discuss the types of exercises their organisations use and which exercises they think are effective and why. They were also asked to discuss how to ensure that "lessons identified" from security exercises are translated into "lessons learned" and improve operational effectiveness. The participants pointed out that their organisations use modelling and simulation, table-top exercises, and force on force exercises, discussing in more detail the cost effectiveness of modelling and simulation tools when preparing for security exercises or the simplicity of conducting table-top exercises with very little means. The discussion on force-on-force focused around the challenges the participants faced in their individual countries both in terms of the budget of such exercises and the necessary man-power / impact such exercises have on day to day operations. The discussion on lessons learnt revolved around performing vulnerability assessments, validating training methods, validating equipment, and validating the team response – both the individual response and the operational plans. These factors when performed properly can improve operational effectiveness.

SESSION V: TABLE-TOP EXERCISE – SWEETBRIAR NUCLEAR POWER PLANT

The purpose of this session was to put the workshop discussions into practice by having participants work through a scenario that takes place in the hypothetical country of *Ruritania*. Moderated by Mr Reynolds, the TTX gave participants the opportunity to identify and address potentially complex issues that could arise when responding to incidents, further explore the respective roles of on-site and off-site stakeholders in responding to a security incident, review best practices for developing effective communication, coordination and cooperation amongst key stakeholders, identify and discuss usual challenges with respect to the response, management and recovery from such an event, and review some aspects of crisis planning and response processes.

Inject 1

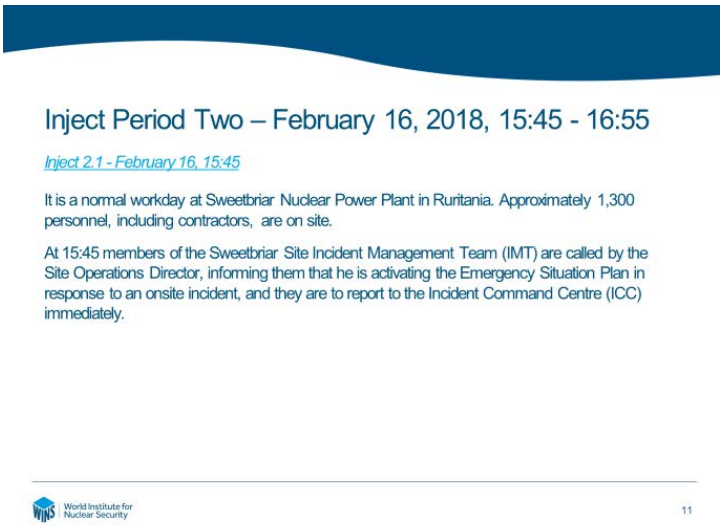
The simulation began with some background information pertaining to the location and type of facility involved; it then presented the first inject of information.

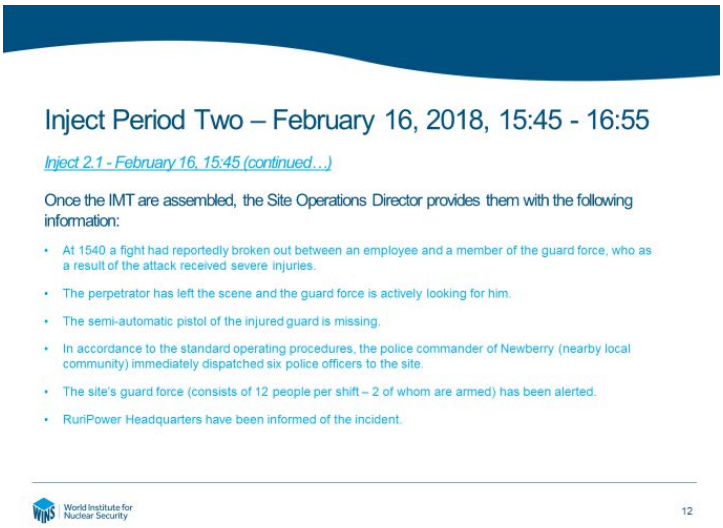


The first inject shows a social media feed. Users are commenting on rumours of poor and corrupt management practices at the Sweetbriar nuclear power plant which might cause more than a 100 people to lose their jobs.

Inject 2

Mr Reynolds then presented the second set of injects, describing a fight between an employee and a member of the guard force and providing some formation of the Incident Management Team. The injects also illustrate how quickly social media can pick up on an incident.





Inject Period Two – February 16, 2018, 15:45 - 16:55

Inject 2.2 - February 16, 15:55

Twelve Newberry police officers arrive on site. None of them are familiar with the detailed layout of the site.

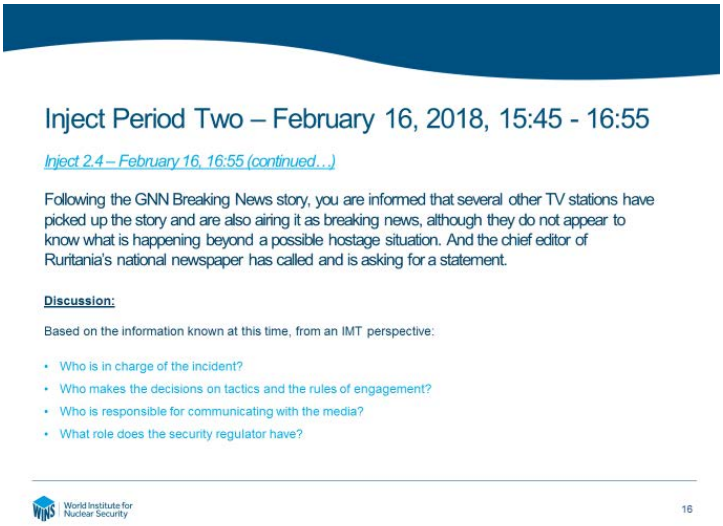
Inject Period Two – February 16, 2018, 15:45 - 16:55

Inject 2.3 – February 16, 15:57

Twitter:
#SweetbriarNPP

Inject Period Two – February 16, 2018, 15:45 - 16:55

Inject 2.4 – February 16, 16:55



The participants were then asked to discuss the following questions:

- Who is in charge of the accident?
- Who makes the decisions on tactics and rules of engagement?
- Who is responsible for communicating with the media?
- What role does the security regulator have?
- Consider the sequence of events described above by the Site Operations Director. Would your site handle such a situation in the same way?
- As members of the IMT, what other information do you need?
- Are the Site Operations Director's actions appropriate? How do you know?
- As the external response organisation, would you dispatch officers to the site? Why or why not? What indicators do you need to take such a decision?

Some key findings are:

- We need more information. For example, is the event taking place inside or outside the high security area?
- We should assume the worst case scenario!

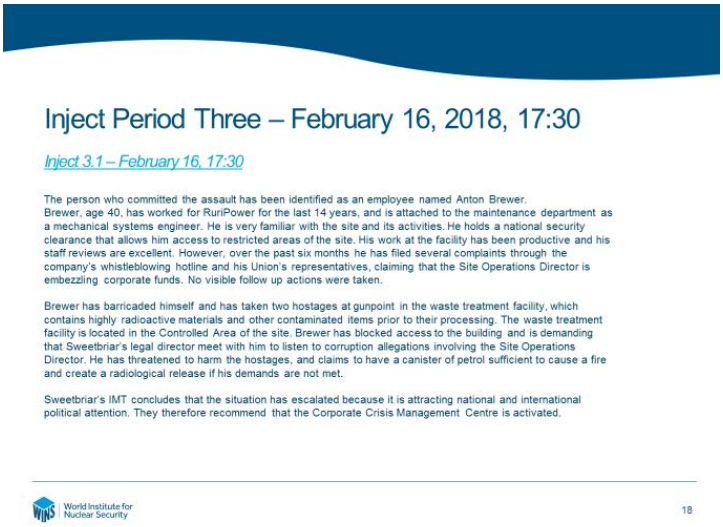
Actions:

1. Lock down the site.
2. Request a site emergency via the EMS (intercom).
3. Find out what the trend is in reporting incidents.
4. Try to identify who this person is so he or she can be locked down from the security side and electronically denied access permissions. Begin by asking all department heads to do a head count of their personnel.

5. Have any problems occurred recently? Has any maintenance been conducted in the last six months?
6. Implement emergency and security plans.
7. Check the operational plan. (Is there ample electricity and water?)
8. Conduct an internal search of the site.
9. Prepare internal communications to make a statement to the public.
10. Lock down internet and mobile signals (signal jamming).
11. Contact the media and brief them on the event.
12. Activate high alerts at HQ to safeguard the building and management.

Inject 3

Mr Reynolds then presented the next inject, which gave participants more details about the perpetrator and his current whereabouts.



Participants were asked to briefly discuss the mechanisms their organisations have in place to ensure effective communication, coordination and cooperation, and they pointed out that it is vital to use the mechanisms that already exist in the communication policy, current structures, such as the JPC (Joint Planning Committee), and operational procedures.

Inject 4

Mr Reynolds then presented Inject 4, which provided more details on the how the situation was playing out.

Inject Period Four – February 16, 2018, 17:45 – 20:00

Inject 4.1 – February 16, 17:45

At 17:45, Incident Command Centre receives a call informing IMT that:

- Brewer has started a fire in the waste facility.
- The environmental radiation detection monitoring system has measured a small increase in the on-site radiation background but there are no measuring stations near the building with the hostages.

Based on site emergency procedures, the IMT orders an evacuation of all non-essential personnel.

Inject Period Four – February 16, 2018, 17:45 – 20:00

Inject 4.1 – February 16, 17:45 (continued…)

Discussions *(for various stakeholders - IMT / Police Commander / HQ Corporate Crisis Communication Centre):*

1. Who is accountable for nuclear Safety on the site?
2. Do you issue a public statement simultaneous to the order to evacuate non-essential personnel?
3. How do you think the employees and public will interpret the order to evacuate? How do you ensure your message is interpreted correctly?
4. How do these new developments affect your decision-making?
5. What should the response teams do? Who is in charge?
6. What additional information do you need?
7. Do you need to consult anyone else? If so, whom?
8. What are your top priorities over the next 30 minutes? Over the next 24 hours?

Inject Period Four – February 16, 2018, 17:45 – 20:00

Inject 4.3 – February 16, 19:00

In view of the situation and possibility of a radiation release, thirty minutes later the police decided to take control of the situation and a CBRN unit rushed into the waste facility, neutralised Anton Brewer, freed the hostages, and circumvented the fire before any radiological release occurred.

One of the hostages was slightly injured during the assault and taken to the local area hospital.

Inject Period Four – February 16, 2018, 17:45 – 20:00

Inject 4.4 – February 16, 20:00

Inject Period Four – February 16, 2018, 17:45 – 20:00

Inject 4.2 – February 16, 18:30

Twitter:
#SweetbriarNPP
#explosion

Inject Period Four – February 16, 2018, 17:45 – 20:00

Discussion:

1. What happens now?
2. Who are the primary stakeholders? Who coordinates communications with each?
3. What were the primary "lessons to be learned?"
4. Who is in charge of the post-incident inquiry?
5. What information needs to be gathered?
6. If an inquiry were to take place, who is liable for what has happened? What are the potential criminal and civil penalties?

The highlights of the discussion that followed are captured below:

1. Issues with access control

2. Security systems failed (both equipment & personnel)
3. Vulnerability assessments
4. Random screening / mental screening /physical screening
5. Training, implementation and understanding
6. Integration of different systems
7. Emergency plan includes the public
8. Evacuation plan activation
9. Operator is in charge
10. Additional information needed:
    a. check building management systems (BMS)
    b. transport
    c. weather (wind)
11. Top priorities:
    a. safety of the personnel
    b. safety of the public
    c. safety of environment
    d. return to normal activities (24h to two weeks)
12. Employees' expectations:
    a. provide assurances to employees
    b. provide assurances to the public

Participants highlighted some of the common crisis management challenges. These include:

1. Not having a clearly defined organizational policy and senior leadership approval
2. Lack of a well-established crisis management system
3. Indecisive leadership
4. Not engaging all stakeholders
5. Not having a risk communication plan
6. Not having an issues management capability
7. Limited external relationships (reputational capital)
8. Lack of situational awareness
9. Lack of a situational reporting system
10. Not having a master events log (MEL)
11. Lack of defined roles and responsibilities of crisis team members (who's responsible for what?)
12. Addressing assumptions

13. Lack of forethought when transitioning into recovery
14. Not having a pre-determined decision-making process
15. Briefing cycle discipline
16. Not having a fully equipped EOC
17. Not having access to an alternate Emergency Operations Centre (EOC)

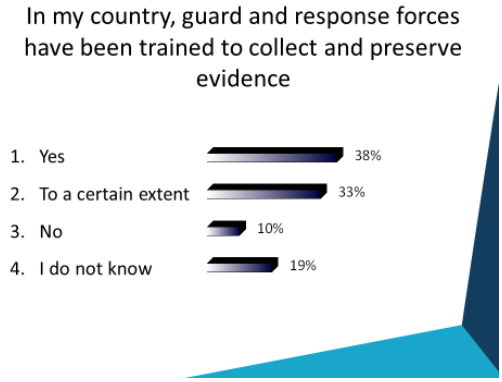
DAY 4

SESSION VI: POST-INCIDENT MANAGEMENT

Session VI was designed to discuss post-incident management, define entities responsible for conducting post incident reviews, define key elements of conducting a post incident review.

E-voting

The Session VI discussion started with e-voting questions on training of guard and response forces on collecting and preserving evidence and improvement process supporting an effective learning from actual incidents.



The results clearly showed that post-incident management still needs to be improved and defined. Participants had mixed opinions about the capability of the guard and response forces to collect and preserve evidence. A part of the audience expressed their trust and confidence in the response forces management whereas others indicated that the training has been sufficient only to a certain extent. When asked about the improvement process and effective learning from incidents, majority of participants said that such processes exist in their countries/organisations, although a large group of participant said that the effective learning is conducted only to a certain extent or they weren't actually sure if such learning and improvement processes exist in their countries/organisations.

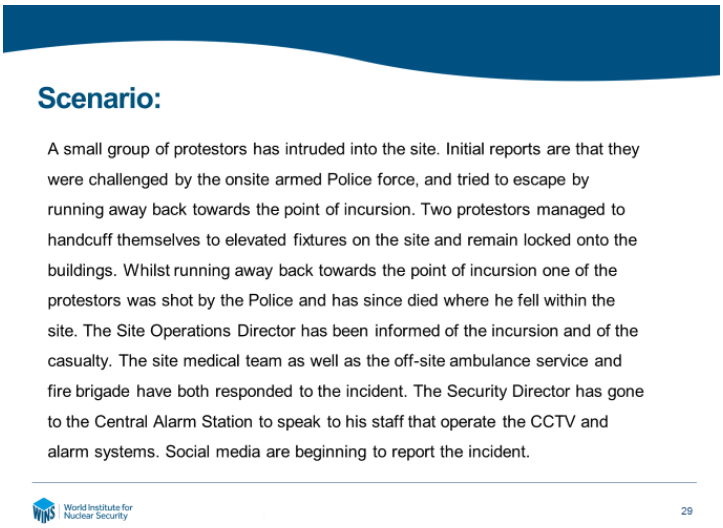
Presentation

Mr Nigel Tottie, International Atomic Energy Agency (IAEA), provided the participants with some perspectives on post-incident management, including the response, radiological crime scene management, and nuclear forensics. He outlined the spectrum of nuclear security activities, from prevention, to detection and ultimately to response, and explained why radiological crime scene management has such an important role in post-incident management, what objectives it aims to

fulfil, and how it is different from other crime scenes. He also pointed out the importance of nuclear forensics and its role in State's national response plan for security events.

Group Discussion

Participants were then presented with a scenario and were asked to discuss and summarise the most important and urgent post-incident actions that need to be taken by the Site Operations Director and the Commander of the onsite, armed Police force.



Some of the main findings of the discussions are highlighted below:

- Regardless of where the incident happens, including sensitive areas or materials, the investigation process should be the same;
- Handling media can be very intense and reputation damaging. Media would dig to know everything; they would be very intrusive. Organisations must be prepared and selected staff trained to communicate with media. Dedicated point of contacts for media should be identified and integrated within comprehensive communication plans. Some organisations have prepared media report templates, including a statement indicating that an update would be provided within an hour;
- The first incident report is important but might be impacted by the "psychological mind" of the staff involved in the incident. Part of the initial training for armed officers should include preparation to trauma. Psychologists and health professionals should be available for further support and assistance to staff involved in serious incidents;
- In many cases, investigations would be run in parallel by the police and by the nuclear regulator;
- It is sometimes difficult to effectively learn from an incident. It might take years to get a comprehensive report. Intermediate steps need to be established to support short and medium-term improvements.

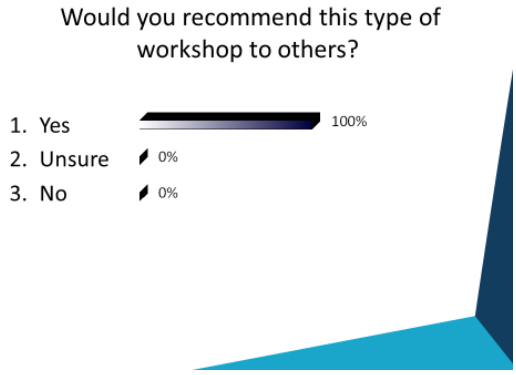
SESSION VII: WAY FORWARD AND CONCLUSION

At the conclusion of the event, Dr Roger Howsley, WINS, gave an overview of the WINS generic protocol for emergency planning and security incident management. The presentation was part of the discussion on the protocol. Following are some additional issues that a protocol needs to address:

- Conventional safety risks and hazards
- Evidentiary procedures which the licensee needs to know and understand
- Sharing sensitive information/intelligence
- Building relationships and trust through joint operations/exercises
- Detention policy
- Pursuit of individuals beyond the site borders
- Identification of places on the site where weapons should not be discharged
- Areas of site access for off-site response forces
- Communication within the facility and what happens if certain areas do not have signal

Evaluation and concluding remarks

The e-voting system was used to obtain a final evaluation. Participants indicated that they were very satisfied with the event, that it had been an excellent and useful learning experience, that Mr Reynolds had been an effective facilitator, and that they would recommend the event to others.



In their closing remarks, representatives from WINS and Bruce Power, and Mr Reynolds emphasised that the success of the workshop was largely due to the active contributions of all participants. They praised the willingness of the group to learn from the speakers' team and from each other despite a challenging topic. They added that the discussions had shown that participants (and likely the stakeholders they were representing) had a strong appetite for learning tools and techniques for increasing their capabilities to strengthen their already existing incident

management programmes. Participants committed to building on this success and to increasing opportunities in which stakeholders can exchange with national and international partners on their experiences in ensuring nuclear security, especially in regard to the challenges from in incident management and emergency response planning.