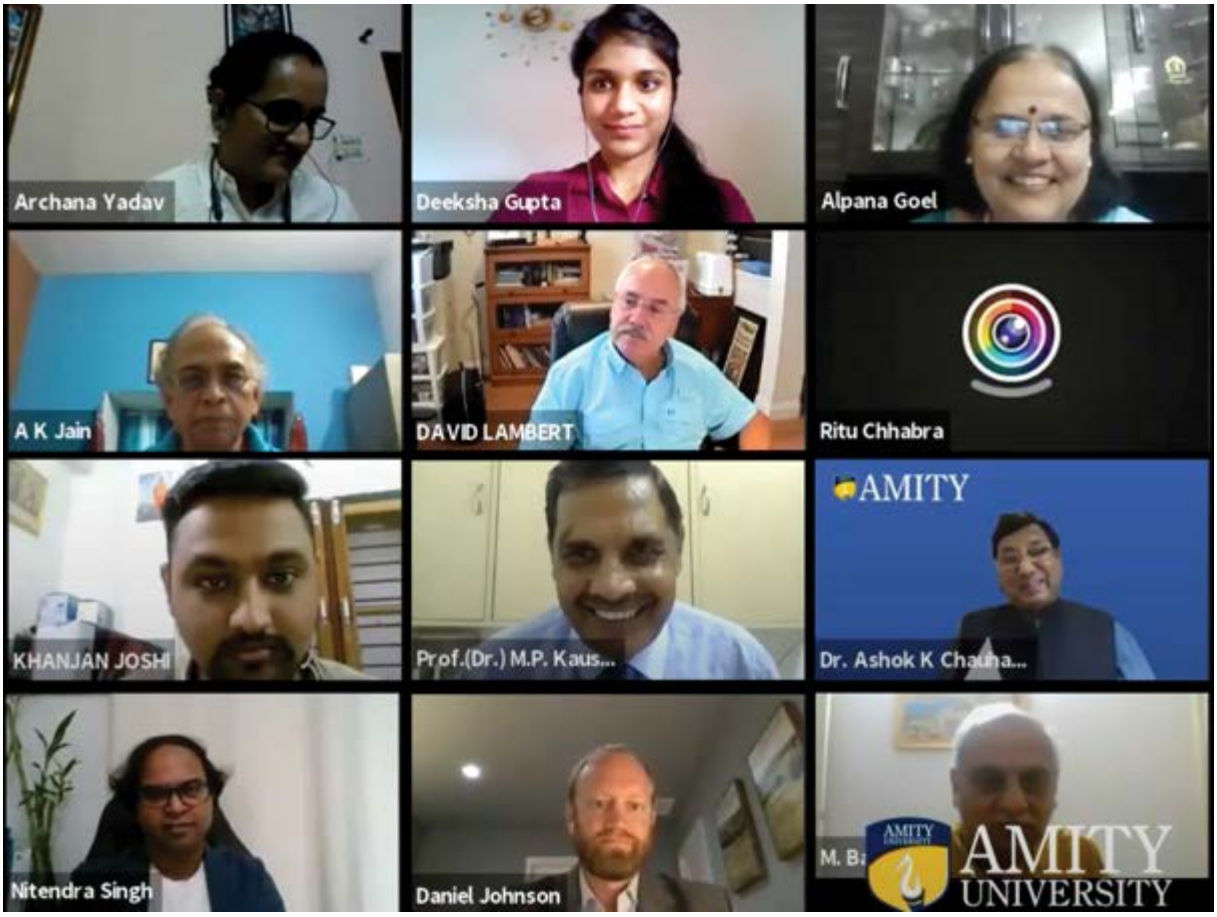
Training Course Report

WINS Academy Training on Integrating Cybersecurity with the Security Programme

In collaboration with the Amity Institute of Nuclear Science & Technology (AINST), AUUP & Indian Youth Nuclear Society

22-26 September 2020



Background

Over the past few years, the World Institute for Nuclear Security (WINS) and Amity University have collaborated to deliver a series of training courses to increase knowledge and skills on security matters for the future nuclear work force in India. From 22-26 September 2020, WINS and Amity continued the collaboration through an online training course for 57 Amity students, alumni, and members of India's existing technical nuclear industry to achieve the following objectives:

- Provide participants with an understanding of the interface between cybersecurity and physical protection and insider threats
- Provide participants with an understanding of real threats from cyberattacks through case studies presented by nuclear security experts and stage an exercise to aid the application of the learning
- Review and evaluate the learning to consider what continued professional development is required for participants to further enhance their understanding of nuclear security
- Help to develop a cohort of professionals with the knowledge, skills and competence to improve the integration and effectiveness of nuclear safety and security across India

Participants learned through online interactive sessions and exercises to consider how threats can be identified and mitigated. Participants considered the topics of cybersecurity and how it connects to physical protection systems and insider threats through the human factor. The training course

reviewed corrective actions and improvements that can make a real difference for mitigation of nuclear security risks.

Participants were encouraged to apply for a funded scholarship to complete a WINS Academy Certification Programme and take the required exams to achieve the status of Certified Nuclear Security Professional (CNSP) and join the WINS Alumni Network.

Introduction Session

The training course was opened by Dr Archana Yadav, Amity University, who served as the host for the event. Dr Yadav introduced Dr Alpana Goel, Amity University, who provided opening remarks to welcome participants to the event and thank all of those who helped with the organisation. Dr Goel invited Dr Ashok Chauhan, founder of Amity University, to provide remarks to the participants. Dr Chauhan stated his strong support for the collaboration between Amity and WINS. He noted that he has established an Amity technical centre in the United States and supported collaboration on nuclear security. He said that the topics covered in the training course are very important for India.

Mr Dan Johnson, WINS, thanked Dr Ashok for joining the event and blessing the proceedings. He thanked all of the Amity staff and alumni who helped with organising the event, which is the third collaboration between Amity and WINS. Mr Johnson stated that the topic for the training course is particularly interesting. To provide context, he said that earlier this year, WINS surveyed its over 6,000 members on the state of nuclear security globally. WINS members said that cybersecurity was the number one security challenge facing the industry. Dan noted there are great opportunities for young professionals to find solutions to the various cybersecurity challenges and identify career opportunities.

Presentations

Fundamentals of cyber security for nuclear facilities Throughout the week, experts provided presentations on topics related to cybersecurity. Dr S.A.V. Satya Murty, Director of the Vinayaka Missions Research Foundation and former Director of the Indira Gandhi Centre for Atomic Research, provided a keynote presentation on the fundamentals of cyber security for nuclear facilities. Dr Murty noted that new digital control systems are vulnerable to cyber threats and that cybersecurity needs to be built into the design.

A robust Q&A session with participants followed Dr Murty's presentation. Dr Murty responded to questions by stating (inter alia):

- Digital systems have lower capital costs and are cheaper to maintain. Although there is a risk, it is like any other risk that we accept and manage in our day-to-day lives.
- Using open source operating systems is better. People are sharing knowledge to improve open source systems and it is possible to have external validation from a knowledgeable third party. In addition, commercial software can come preloaded with malware, whereas open source software is free of this problem.
- Although it adds latency, defence in depth is important to apply for computer systems.
- Reactor operators must have extensive training to ensure that information is securely transferred and controlled. They must pass exams and receive regulatory approval.

Physical protection systems and how they are vulnerable to cyber threats

Mr Dave Lambert, Senior Security Specialist/Nuclear Security Training Manager at Gregg Protection Services, gave a detailed presentation on how physical protection systems (PPS) can become vulnerable to cyber threats. Mr Lambert noted that safety and security are tightly integrated with cybersecurity. He stated that computer systems need some level of physical protection, but the physical protection systems themselves are vulnerable to cyber-attacks. However, there is no particular design basis threat (DBT) for computer systems, although two concepts are found internationally: 1) computers are part of the existing DBT document, or 2) the computer DBT is separate from the existing DBT.

Regardless of the approach, computer systems including PPS must be protected through defence in depth. Systems to be protected include access controls, cameras, detectors, sensors, and alarm systems amongst other components. However, a number of external factors can conspire to defeat computer systems that PPS rely on, including smoke and fire, loss of power and cooling, plumbing leaks and water damage, and structural collapse, amongst other factors.

During the Q&A, participants had a number of excellent questions:

- One question related to the COVID-19 pandemic and how we maintain the same level of cybersecurity and physical protection. Mr Lambert noted that you can have the best technology in the world, but if no one is there to maintain it then systems are subject to fail. The pandemic highlights the importance of recognising that external events can impact the site and there needs to be advanced contingency planning to prepare for unexpected events.
- Questions also revealed that employee data is particularly vulnerable to cyberattacks and is often not as well protected as it should be.
- Access control systems, including key card access and even biometric systems, can be defeated by intercepting employee information and reprogramming configurations. It is important to adopt multifactor authentication.
- The computer DBT and existing DBT should be tightly integrated and considered from an operational perspective.

Cybersecurity insider threats

Ms Karen Kaldenbach, Human Reliability Program Team Lead at Oak Ridge National Laboratory, provided a presentation on cybersecurity and insider threats. Ms Kaldenbach shared a number of real-world case study examples to illustrate the threat. She noted that insiders can be both unintentional (unwitting) and intentional insiders. In both instances, there are a number of mitigation measures that can be implemented to reduce the threat, including trustworthiness and reliability programmes, mandatory ongoing training, defence in depth, systems monitoring, and a variety of procedures to ensure risk reduction. In summary, Ms Kaldenbach stated that protection from insider threats is 20% technology and 80% employee awareness and adherence to procedure.

During the Q&A, Ms Kaldenbach clarified that:

- "Unintentional" insider acts are quite prevalent and related to human error. For example, a nuclear facility was found to have connected its business network with its operating control systems.
- Morality and values differ by culture. Based on your own culture you can develop a set of trustworthiness and reliability criteria.
- Social media monitoring is increasingly used by nuclear organisations to detect threats. In some countries such as the United States this is allowed and appropriate, and there may be staff dedicated to monitoring social media.
- Although the nuclear industry is eager to adopt automation, you still need people to work at these facilities and make judgement calls. The human element is not going away.

Panel Discussion

The training course held a panel discussion with five Indian subject matter experts to explore the relationship of insider threats and physical protection systems to cybersecurity. The five experts were:

1. Dr S.A.V. Satya Murty – Director (Research) of Vinayaka Missions Research Foundation (VMRF)
2. Prof. M. Sai Baba – Outstanding Scientist and formerly Director, RMG, Indira Gandhi Centre for Atomic Research (IGCAR) and Senior Professor, HBNI, Dean (Student Affairs) and Coordinating Dean of HBNI at IGCAR
3. Shri Gyan Prakash Srivastava – Electronics Engineer, Distinguished Scientist and Director, Electronics, Bhabha Atomic Research Centre
4. Shri Ranajit Kumar – Head Nuclear Controls and Planning Wing, Department of Atomic Energy
5. Munish Sharma – Consultant, Institute for Defence Studies and Analyses

The panel was moderated by Professor A K Jain, Advisor at Amity University. The founder of Amity University, Dr Ashok Chauhan, also attended the session and provided remarks to compliment the

agenda and said that this is one of the most important seminars that can be held in India. Dr Chauhan stated that topics covered in the course were very sophisticated and he was glad that the distinguished panellists were able to participate and collaborate with WINS and the Indian Youth Nuclear Society.

The panellists discussed the following key points:

Cyberattacks in India

Fortunately, to date there have been no instances of damage to an Indian nuclear facility from a cyberattack.

GCNEP Engagement

They were calls for greater engagement between the Global Centre for Nuclear Energy Partnership (GCNEP) and the Indian academic community. So far, GCNEP has focused on engagement with technical organisations such as the U.S. laboratories and CEA in France. However, they are starting to open up now for engagement with other institutions including in academia. It was suggested that GCNEP post information about this event and serve as a gateway for future events of this type.

Man/Machine Interface

There is a man and machine interface that must be harmonised. The goal is to use technology to make things easier, not to compromise productivity. We need to use technology to identify insiders rather than restrict technology.

In addition, technology cannot be stopped. We need to focus on security by design rather than trying to keep everything secret. In this respect, the change control management process is an important part of strong cybersecurity, whereby users are not allowed to make changes because of a strong design.

Insiders and Human Reliability

An insider has specialised knowledge and access. An attack can happen suddenly or can take place over a long period of time. Furthermore, employees can make the transition from reliable to unreliable while working at a facility. There needs to be a process for periodic screening of staff, not just when they are hired.

Facilities should focus on access control and surveillance to ensure staff are not going beyond their permitted access. However, too much intrusion and surveillance can lead to employee dissatisfaction. Corrective actions need to be taken with an understanding of acceptable risk. We need to take a helpful rather than a punitive approach.

Furthermore, it is understood that humans are the weakest link in security. We can harness psychology and technology together to come up with next generation security solutions. For example, behavioural analysis can be used to pick up early warning signs and stop an insider before an incident. Existing tools on social media can be leveraged to identify problems and its acceptable for the nuclear industry to use these tools. We can also use language processing tools for workers in different regions. There is a stark difference in behaviour even between different regions.

Quantification of human behaviour and cognition is very challenging. Human behaviour will always be qualitative. You can run experiments and test models to influence behaviours. For reference, IAEA guidance is adapted by member States based on the socio-political and regional environment. Indian nuclear organisations use the IAEA guidelines but follow their own internal standards.

Career Opportunities

There are many career opportunities in cyber. Students are at the best age to take up the challenge. The panellists suggested that participants consider this as an area of specialisation. The scope is everywhere and beyond just nuclear.

Cybersecurity Assessment Exercises

During several days of the training course, participants were organised into five teams to undertake a cybersecurity assessment of the Shapash Nuclear Research Institute (SNRI). The objective of the exercise was to utilise the IAEA documents *NST37 Conducting Computer Security Assessments at Nuclear Facilities* and *NSS17 Computer Security at Nuclear Facilities*. NSS17 is the primary international guidance on establishing a computer security program for a nuclear facility, while NST37 builds upon this

guidance and presents a methodology for conducting a computer security assessment, or peer review, based on NSS17 guidance.

The exercises were facilitated by Mr Johnson of WINS. Participants were presented with a series of four exercises that followed in sequence with each other. In Exercise 1 the teams chose a team leader and organised themselves. They were then given the option to choose from a menu of five areas to undertake a computer security assessment. These five assessment areas were:

1) I&C Security Architecture
2) Removable Media and Mobile Device Management
3) Physical Protection Systems
4) Configuration Management Procedures
5) Nuclear Material Accountancy and Control

In Exercise 2 participants familiarised themselves with documentation developed for the fictional SNRI as well as NSS17 and NST37. During this step they reviewed the SNRI information based on their chosen assessment area and began understanding how to write a recommendation for an assessment of computer security at a nuclear facility. In Exercise 3 they began to further plan out a computer security assessment and chose a number of functional and security domains to explore as part of their review.

Exercise 4 brought all of the previous exercises and learning together. Participants were tasked with writing a series of assessment reports to identify non-compliances at the SNRI and provide recommendation based on IAEA guidance. These recommendations were reported out on the final day of the training course for feedback from Mr Johnson and Mr Lambert. The participants did an excellent job and by going through the exercise were able to better understand the relationship between computer security and the various operational processes at a nuclear facility.

Career Discussions

Ms Deeksha Gupta, Amity alumni who is a PhD candidate in nuclear cybersecurity and currently working as a cybersecurity consultant, organised a session on the last day of the course to discuss career opportunities with participants. Speakers included the following Alumni from Amity:

- Prakharesh Awasthi
- Aayush Sinha
- Samyak Munot
- Abhyuday Sharma
- Siddharth Sinha
- Rishika Singh

Speakers encouraged students to pursue additional career opportunities in this area and to take advantage of the WINS Academy for their professional development.

Dr Nitendra Singh also gave a presentation to encourage participants to join the Indian Youth Nuclear Society (IYNS). IYNS is a non-profit organisation with the aim to spread awareness about the benefits of nuclear energy among the general public and encourage youth to learn and contribute to the nuclear energy programme.

Conclusion

The training course concluded with remarks from Dr Goel and Mr Johnson to thank Dr Yadav, Dr Jain, Ms Gupta, the presenting experts, alumni, and the entire Amity team for supporting the event. It was agreed that this was a great topic, very important for Indian nuclear facilities and worthy of additional exploration for future events.

In sum, Mr Johnson noted that the training course covered the many potential vulnerabilities in computer systems. These vulnerabilities can be mitigated through defence in depth, security by design, training, and adherence to policies and procedures that align with standards and guidance. However, mitigation measures can be quickly overcome. You can have the best technology and systems in the world, but those systems are still subject to fail. There is a particular danger from insiders, whether it's intentional or unintentional, and the vast majority of instances occur because of human error.

Students were advised to explore career opportunities in this area. To start, they were encouraged to take advantage of scholarship opportunities with the WINS Academy and earn a certificate from WINS.