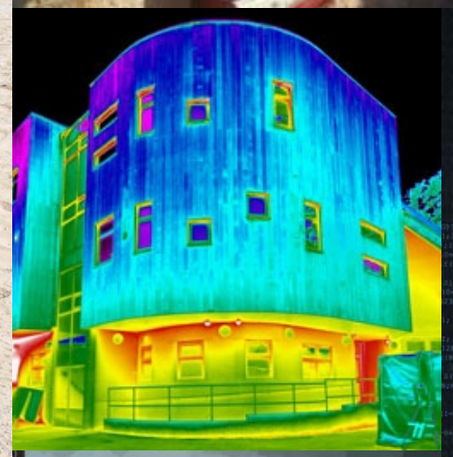
World Institute for Nuclear Security

Autonomous and remotely operated systems: benefits and challenges to nuclear security

2nd – 4th April 2019

Brief Review of Remotely Operated and Autonomous Systems for Security

Pierre Legoux
Head of Programmes



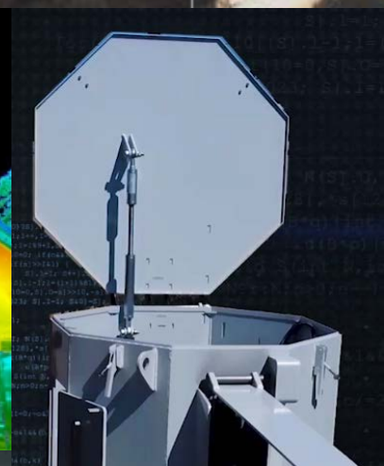


Photo: Sandia National Laboratories

What is important to us?

- What is the need? What security function do we want to achieve?
- What technologies are currently available? What's likely over the next 5-10 years?
- What's our experience to date with these technologies? Do we have enough opportunities for sharing lessons learned?
- What is a thorough process to identify a new technology, assess its possible benefits and effectively integrate it into existing security arrangements?
- What are the incentives for adopting new technologies?
- What are the remaining barriers to effective integration in our security programmes?
- How do we demonstrate these technologies are protected against misuse?

What are the main advanced technologies related to security?

- **Drones** and other unmanned aerial vehicles (UAVs)
- **Automated Access Control and Tracking Systems**
- **Surveillance Robots** and other unmanned ground vehicles (UGV)
- **Remotely Operated Weapons Systems (ROWS)**
- Virtual and Augmented Reality
- Artificial Intelligence (AI)
- Enhanced human performance
- Cyber security
- Advanced Modelling and Simulation Tools
- Etc.

Drones and other UAVs

Benefits?

- Surveillance of perimeter and large areas
- Quick and safe assessment of (outdoor) alarms
- Reduce guard force exposure
- Flexible use: Stationary, pre-programme flights or remotely controlled
- Relatively cheap

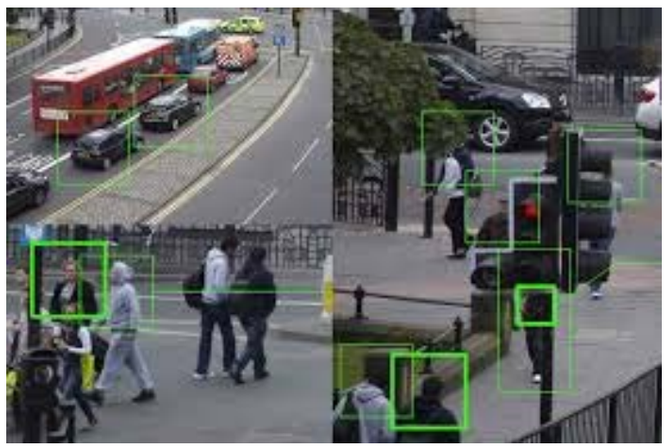
Challenges?

- Limited autonomy
- Sensitive to weather conditions
- Subject to tight regulations
- Subject to countermeasures

Automated Access Control and Tracking Systems

Benefits?

- Multi Biometric based (reliable)
- Reduce number of staff required
- Efficient insider mitigation tool (e.g. support investigation; deterrence effect)



Challenges?

- Increased response time (no human presence)
- Privacy issues
- Data reliability and security
- High tech Alarm Station

Access Control as a Service (AcaaS)

Surveillance Robots

Benefits?

- Mobile sensor platform (multiple; customisable)
- Reduce number of staff required (e.g. patrols)
- Prevent fatigue and boredom
- Reduce exposure of guard force
- “Marketing tool”

Challenges?

- Still very early stages. Is there a need?
- Costs
- Maintenance

Remotely Operated Weapons (RoWs)

Benefits?

- Force multiplication (single operator with near-instant response at multiple points of concern)
- Staff protection
- Increased efficiency (Remote operator removed from “combat situation” stress)
- Reduced operator inaccuracy and fatigue
- Long term Reduction of security cost
- Available Lethal/Non Lethal

Challenges?

- Primarily designed for military applications.
- Not always designed with the safety design basis required to enable its use for other security systems applications
- Liabilities and Regulatory matters
- Human interaction and Public acceptance
- Cybersecurity resilience

Nuclear industry perspective

- Security budgets are under greater scrutiny at the same time as potential new threats and new facility designs might raise new security challenges
- The insider threat is a more important issue than ever and must receive even greater attention
- Regulation must become more agile to allow for responsiveness to changes in threats and benefits brought by advanced security technologies

Will any of these technologies become a game-changer for risk management?

What is important to us?

- What is the need? What security function do we want to achieve?
- What technologies are currently available? What's likely over the next 5–10 years?
- What's our experience to date with these technologies? Do we have enough opportunities for sharing lessons learned?
- What is a thorough process to identify a new technology, assess its possible benefits and effectively integrate it into existing security arrangements?
- What are the incentives for adopting new technologies (performance; cost reduction; deterrence, protection of first responders, others?)
- What are the remaining barriers to effective integration in our security programmes (cost; regulations, staff training, employee acceptance, etc.)?
- How do we demonstrate these technologies are protected against misused (cyber security)?

Thank you!

Learn more at: **www.wins.org**

World Institute for Nuclear Security