WORLD INSTITUTE FOR
NUCLEAR SECURITY

Data Analytics for Nuclear Security

HOW REAL-TIME INTEGRATED DATA MANAGEMENT COULD SUPPORT NUCLEAR SECURITY

January 2015

Revision 1.0

A Word on Definitions

The purpose of this paper is to provide a perspective on whether combining information that is traditionally "owned" by the security department with other information held by the organisation could provide better security for the overall organisation.

We recognise there is a wide variety of definitions and terminology being used by the business, risk and IT communities to describe risk management and data analysis and that the definitions vary from one vendor to another, from one implementer to another. They will certainly vary from one country to another.

We have chosen to use the terms "Integrated Data Management" and "Integrated Data Analytics" to describe the following; an approach to managing organisations that is led from the top and where all information and data are used to generate value and support the success of the organisation. Within this context, we believe that security must be viewed and operated as an enterprise-wide activity and be fully integrated into other business processes and objectives.

So the important concepts are that security is *integrated*. That information and *data* (the evidence) drive risk and business decisions. And the process of doing this needs both *management* and *analysis (analytics).*

ISBN 978-3-903031-66-1

I. ABOUT THIS PAPER

During 2014 WINS conducted research on the status of integrated data management systems and how they are currently being used to support nuclear security and associated functions such as material control and accountancy, the tracking of nuclear transport operations, etc. The full report[1] is available at *www.wins.org*.

The conclusions drawn from the research were that integrated data management and associated analytic software tools are not being used extensively for security applications in the nuclear sector but would seem to provide immense potential for improving what is commonly referred to as "situational awareness", or as the Information Security Forum describes it, "going from Hindsight to Insight".

To build on the research, WINS hosted a 2-day roundtable in Vienna in December 2014 and invited leading academics, vendors and experts from different sectors to provide guidance on the current application of integrated data analytics in commerce and government, and the benefits and obstacles to its use for achieving enhanced security. We also discussed the emerging technology commonly referred to as "Big Data Analytics" and whether this has a place in the nuclear sector, now or in the future.

Underlying all this work is a belief, borne out by real life experience, that information and data of all types are frequently managed in silos both within and between organisations and that many of the current data management systems for nuclear security are suboptimal. For example, it is common practice to intentionally separate responsibility (and associated information) for physical security, cyber security, nuclear materials control and accountancy (NMCA), and operations in order to prevent collusion by insiders. The question is whether this intentional subdivision of responsibility leads to better nuclear material protection or just the opposite because of the information silos that commonly result.

This paper sets out the key issues that were identified by the expert group; it does not provide definitive answers to the very many questions that were discussed but strongly recommends that integrated data management and analytics be considered seriously for implementation in the nuclear sector, perhaps through collaborative pilot programmes. We will continue to review the status of research and implementation in our subsequent activities, including relevant WINS workshops.

[1] Big Data in Motion; How Real-Time Integrated Data Management Could Support Nuclear Security, August 2014

II. WHAT IS THE ISSUE THAT WE ARE TRYING TO ADDRESS?

Examples of nuclear materials being stolen or nuclear facilities being sabotaged are very rare across the world; either because of the extensive measures used to deter or prevent such incidents or because there are very few real attempts being made to do so by either terrorist or criminal entities. The evidence points more towards the latter because reports of failed attempts are also very rare. This being the case, it raises the question of security preparedness; if an individual or group decided to attempt theft or sabotage, would the security (and related) systems provide sufficient warning and resistance to thwart the attempt? Or would we be in the realm of realising ex post facto that there was ample information and data that could have used to prevent the successfully executed malicious action if only they had been shared and analysed more quickly?

Think about this simple scenario:

- Insiders decide to steal small but significant amounts of nuclear material from a processing line over a protracted period of time - how confident would you be that the NMCA systems would detect the theft?
- How confident would you be that one or more of the physical protection systems would prevent the theft?
- Suppose one or more of the insiders had grievance issues of which the HR department was aware; would the operations managers be told about this or would it be confidential?
- Suppose one or more of the insiders had medical issues involving drug abuse known to the Chief Medical Officer; would operations managers be told about this or would it be confidential?
- Suppose the theft also resulted in the compromise of a number of computer-based control systems on the processing line under the management of the Engineering Department; would the relationship between this compromise and the other indicators be detected and actioned before the situation became any worse?
- Suppose that personnel data on the access control systems to the processing lines didn’t match with other work attendance records maintained by the Administration Department – how long might it take to discover these anomalies?

Of course, in real life, the scenario might be much more complex but it is intended to highlight how information might be available to different parts of the organisation, which if appropriately shared and analysed in a timely manner, would increase the chances of detecting the planned theft and preventing it.

And there are two related factors that are making security management much more challenging than ever before:

1. The first is *the evolution of the design basis threat*; which should now take into account the increasingly sophisticated threats from cyber attacks, insiders and combinations of threats that might be deployed simultaneously, and

2. Secondly, *the sheer growth in technology*: there has been an enormous increase in the number and type of computer-based detector systems used for all sorts of process, control, safety and security applications over the last 10-15 years (see Box 1). The volume of data being generated is huge and growing every year, and there is a serious risk of data overload; organisations being unable to see and make sense of the information they generate. We also need to recognise that in "traditional organisations" the operation, maintenance and control of these systems are likely to be the responsibility of different management groups, quite possibly with limited knowledge of one another's activities, issues and concerns.

Neither of these trends is special to the nuclear industry or the management of security; they are simply reflections of the growth in and deployment of technology in all fields, and many organisations are struggling with how to address the complex challenges of information management and data overload. Instead, organisations need to identify how to derive benefits from the technology and the data, and how they can be used for maximum benefit within the organisation.

Significant results are already being achieved in a wide variety of business and government sectors, from understanding and targeting customers, to political polling, business process optimisation, financial trading, healthcare and law enforcement. Video analytics are now routinely used for sporting events to track and analyse individual and team performance and strategies.

How should the security community address these challenges in the nuclear sector? Is it sufficient to install more sophisticated technology and have it relayed back to dedicated security control rooms that are isolated from all other business processes? Is the sensitivity of the security-related information sufficient to justify that it is always kept separate? How do we develop and test the effectiveness of our security arrangements in the face of sophisticated attacks on the organisation that could involve simultaneous cyber and physical attacks? How does the Security Department "protect" the reputation of the Executives and Board Directors and is it any longer an appropriate role or reasonable expectation for one Department?

BOX 1: TYPICAL EXAMPLES OF DETECTOR-GENERATED DATA THAT SUPPORT SECURITY OBJECTIVES

- Biometric identification of personnel including:
  - Finger print/palm readers,
  - Facial recognition,
  - Voice analysis,
- Security access passes for personnel including SMART technology,
- Digital Surveillance Cameras that can automatically detect and alarm if objects in the field of view change beyond pre-set limits (intruder detection or if items move or appear),
- Radiation/neutron detectors either in portal monitors or to monitor radiation/neutron fields in specific areas/zones of a facility to detect if materials are moving or if levels change beyond acceptable amounts,
- Sound detectors (e.g. fibre optics using interferometric sensors) to help detect unauthorised intrusion and other activity,
- Volumetric/pressure sensors that detect changes in air-pressure,
- Radio Frequency Identity Devices (RFIDs) and related technologies to detect the movement of personnel, materials and other items,
- Infrared detectors to detect temperature changes.
- Plant operating equipment, including Instrument Control (IC) systems, that provide information about the location and status of plant equipment such as specialised vault loading equipment or interlocks,
- Criticality detection systems and radiation monitoring for activity in air or leak detection,
- Inventory monitoring equipment; automatic readers and proximity devices to assist with inventory control,
- The location of transit and transport containers, and
- The location and status of other equipment relevant to production including glove box pressures, production assembly items, etc.

III. ENTERPRISE-WIDE RISK MANAGEMENT AND INTEGRATED DATA ANALYSIS

More and more organisations understand that the only effective way to manage their risks is by making an assessment of all risks that might affect their future success and prioritising them across the organisation. This is more commonly referred to as Enterprise-wide Risk Management. One reason for this is that the scope and range of threats can be very broad and could materialise in many different parts of the organisation or its supply chain – leading to significant financial consequences or reputational damage. Examples include major information security breaches, the theft of assets or the sabotage of systems.

In many organisations there will be arrangements in place that help manage individual groups of risks, perhaps the penetration testing of cyber-systems, or determining how quickly guard forces can respond to alarms generated by intruders. But how do you go about detecting and understanding those threats that are much more complex and where the indicators of a serious problem might appear in a range of different departments or functions within the organisation? And how do you test the effectiveness of the overall security strategy including human reliability, personnel, physical and cyber-security?

We believe that the only way to achieve this (and manage all Enterprise-wide Risks) is by having an Enterprise-wide integrated data analytics capability; i.e. systems that look quickly and effectively for cross-functional and operational trends and indicators that could give an early warning of the emergence of complex threats.

In considering moving to this Integrated Data Analytics capability what are the questions that an organisation would need to consider? Integrated Data Analytics is not some kind of bolt-on panacea that will identify previously invisible problems and compensate for poorly managed security arrangements. But under the right circumstances we believe it can bring enormous benefits that improve the speed and quality of decision-making at an operational level, and provide much better assurances to support Enterprise-wide risk oversight by Board Directors and others with an independent role, such as Nuclear Regulators.

IV. IDENTIFYING THE OBJECTIVES

Start by identifying the most important questions that you need to answer and then identify how you would do that reliably and consistently. Involve other business and functional directors in this process so that the analysis takes into account their concerns and priorities. This is best done through the establishment of an Executive Committee on Security, or a Security Council comprising Executive Directors. Identify the positive assurances and metrics that need to be provided to the oversight Board (and Regulator) and start to think how these can be mapped out across the enterprise and how data from other business and functional areas can support the analysis.

Key areas to look at might be the HR function, Safety, Operations, Engineering and Maintenance, Supply Chain, Quality Management, Finance, Medical, etc. Think about the data needed to provide Strategic, Tactical and Operational information so that there is a hierarchy of key performance areas and lower level indicators across the organisation.

Think about how you would need to visualise the data so that they provide meaningful information that communicates important messages. Everyone will be familiar with IT-security reports that can be data rich and information poor; “last week we had 21,000 attacks on the firewall” – is that good or bad? What does it mean?

As well as identifying assurance metrics also consider how the investment in the security systems can support the organisation’s key strategic objectives. Instead of security just being seen as an unproductive overhead, management will begin to realise that the security systems already in place – video, access control and intrusion detection – are an ideal source of business information (and business intelligence) and that the investment in security systems can now be leveraged to create more powerful tools that help improve operations. Think about how integrating safety objectives into the security access control arrangements could provide increased assurance over whether staff and contractors all have the necessary safety competencies and work permits to be allowed access. Not only does this alter the value and cost proposition of establishing an integrated solution to support the existing systems – it also dramatically changes the Return (ROI) on the historical and current security Investment.

Think about any organisational implications from the analysis; since all parts of the organisation have security needs and responsibilities what does this mean for the organisational structure? Should the security department report to the Executive responsible for Corporate Risk? Does the security programme need to be managed corporately across the organisation rather than being delegated to subsidiary parts of the business? How do you integrate the management of cyber and physical protection systems and reduce what many specialists see as major weakness in those organisations that overlook the importance of these interfaces?

If having completed the analysis (and done it thoroughly as recommended here) you conclude that you don’t need sophisticated software to manage the information and improve situational awareness, then that is your decision. Our experts agreed and thought that a lot of small data challenges may not justify the expenditure in implementing integrated data analytic software solutions, but be aware that the complexity of threats and the volume of data are only ever going to increase with time.

V. IMPLEMENTING AN INTEGRATED DATA ANALYTICS PROGRAMME

If your analysis has identified significant benefits from implementing an integrated data analytics programme, what are the recommended "next steps"?

These include:

- Talk to as many other organisations as possible with experience in integrated data analytics. See what they have done, how it has added value, what problems they have experienced. Form user-networks and communities of good practice to share ideas and concerns. Try and see comparable systems in action so you can appreciate what is achievable – and what is not. Talk to the government organisations that are responsible for the critical national infrastructure in their country; integrated data analytics is already in widespread use in other sectors and there will be things to learn from them.

- Establish an Implementation Team from across the business – generally this should not be led by either the IT or security community but by a business manager with the necessary vision and authority to address the more common blockages and obstacles to implementation (see later for examples of these).

- Break the implementation programme into a series of smaller steps and look to identify benefits at each stage. Implement a pilot programme that can provide "quick wins" – examples might include a reduction in maintenance costs for security equipment, a reduction in false alarms, reduced queuing and time wasting at access control points, improved speed of personnel clearances and other security-related administration. It might also include improved NMC&A processes, including better calibration systems and measurement uncertainty control, improved process monitoring and reducing the resources needed for inventory management.

- Work with your external consultant to derive maximum benefit from the software solutions; the bigger vendors have extensive experience in a wide range of industry and government sectors and can help guide you to the most effective solutions based on effective practices and experience with other clients. The nuclear industry does not have to build these systems itself but does need to be an intelligent customer; some organisations and their executives have concerns over major IT projects (over budget and late) and these concerns need to be properly explored and the investment costs properly identified. Modern software developers have to produce products for the "Facebook Generation" – simple, reliable interfaces and drag and drop capabilities. The visualisation of the data is absolutely key to supporting effective decision-making and this should be a priority area.

VI. DATA ANALYSIS AND THE ESSENTIAL ROLE OF HUMAN ANALYSTS

Integrated data analytics presumes that data are being brought together from different functional and business areas so that new insights can be established by monitoring trends across traditional functional boundaries. As noted, it is essential to identify the questions that you want answering, for example:

- Have all personnel with access to restricted areas the necessary security clearances and safety proficiency?
- What is the efficiency of the personnel access control procedures and what is it costing in lost production?
- Would simultaneous attacks on the IT and physical protection systems be detected in real time so that action could be taken?
- Do the process monitoring systems indicate any anomalies that are correlated to particular personnel being on duty?
- Is the incidence of theft correlated with particular combinations on workers and security guards that might indicate collusion?

Having identified your key questions, the data requirements can be defined, as can the speed with which data have to be analysed. Is it necessary, for example, to analyse data in near-real time as might be the case for security-related detection and monitoring systems? Is it necessary to combine data in many different formats and structures (such as video streaming, access control data, employee and guard shift rotas)? These considerations will help determine the data processing requirements based on what are known as the "4 Vs" – Volume, Velocity, Variety and Veracity:

- **Volume:** the scale of data,
- **Velocity:** the analysis of streaming data,
- **Variety:** the different forms of data, and
- **Veracity:** the uncertainty of data.

This is where the application of "Big Data" Analytics may have a role in very large or complex organisations (see text box below), especially those that are analysing data from open sources and social media. But our expert group thought that the application of Big Data technology to nuclear security was probably premature and not warranted financially; the costs of significant Big Data solutions can run to $millions/annum and the perceived corporate benefits may not justify such investment at present.

What is "Big Data" Analytics?

The expert view was that Big Data Analytics is generally the term reserved for data analysis requiring enormous processing power because of the volume, velocity, variety and veracity (the 4-Vs) of the data streams. It often involves the analysis of large amounts of open source information, such as social media, and where speed of analysis is important. Some believe that "Big Data" is just the modern terminology for integrated data analysis, but on a much larger scale.

Defining the key questions and basic data requirements are a prerequisite for the development of the algorithms that process the data and highlight actionable information. And like any other modelling or simulation technologies, it is essential that the repeatability and reliability of the system are tested, to gain confidence in the data, software and subsequent analysis and avoid cognitive and other biases. Metrics are important to help monitor system performance, including the false alarm rate or where erroneous conclusions are drawn.

Two factors will assist in this process:

- Using realistic test data and introducing deliberate anomalies into the data stream to ensure that they are detected reliably, irrespective of the which analysts are interpreting the data, and
- Making sure that human analysts are always the ones that take the final decisions.

This second point was emphasised by the expert group and can be particularly challenging, because the analysts need to be subject matter experts (SMEs) as well as being highly competent in data analysis and interpretation. The broader business community is struggling to find the right calibre of analyst and finding them in sufficient numbers to support the growth of data analytics, including Big Data analytics. Issues that were raised included:

- Should you rely on external analysts working for a contractor? – The general feeling was that this was not an ideal solution and that in-house expertise was desirable but would take time to develop,
- How do you define the competences required of the analysts and where do they go for training and continued professional development? A growing number of vendors offer "Big Data Bootcamps" to provide training for analysts, but determining which training programmes add real value for an organisation remains a challenge.
- In which part of the organisation should they work? – Within each of the functional and business areas or in a central data analytics unit reporting to the Corporate Risk Executive? The view was that seconding SMEs to a central data analytics unit was the right approach, and it is important to establish who has authority to direct their work and receive the outputs for action.
- The whole issue of data and information access needs to be addressed; how should the analytics software and outputs be structured to provide hierarchical access controls to limit access to sensitive information that only specific analysts require?

VII. COMMON OBSTACLES TO IMPLEMENTATION AND OVERCOMING THEM

All new technologies and business approaches have their supporters and detractors; the latter identifying the cultural, political, cognitive and resource obstacles to doing anything new – and the proposed implementation of integrated data analytics will be no exception.

The predictable objections are likely to revolve around the following concerns:

- The cost and previous track record (failure) of big IT projects,
- The organisational implications of integrating data, particularly if different contractors are responsible for different information silos,
- The confidentiality of the information and "need to know"; with security departments being naturally averse to sharing any information,
- The overall culture of the organisation and levels of trust between departments,
- Fear of being found to be running inefficient or incompetent departments, and using secrecy and information silos as a means to shield unwanted attention, embarrassment and external review,
- Objections from the Regulator responsible for nuclear security, because of a conservative attitude to technology and data analysis.

There are many more potential obstacles. The objective, therefore, is to develop the arguments and business proposals to overcome these predictable objections. This requires there to be a champion, at a senior level, who is able to constructively challenge the current performance and investment decisions that are being made to support the existing security programme, and to ask the tough, cross-functional questions that have been touched on earlier:

- How are investment decisions taken regarding the security programme and on what basis are enhancements prioritised?
- How is the overall performance of the security programme measured and where are their opportunities for efficiencies and improvements in effectiveness?
- How does the security programme support the wider strategic objectives of the organisation; provide six significant examples of where this happens,
- On the basis of realistic and effective independent vulnerability assessments, to what extent did the security systems anticipate or react to the threats and where were there gaps?
- What is the current level of operational and capital expenditure for the overall security programme (including human reliability, cyber and physical protection, information security, etc.) and what percentage of the budget is spent on testing the systems and data analysis to ensure it is fit for purpose?

Most organisations probably can’t answer these questions easily without significant research, or may never have considered the questions at all. Until they do and come up with meaningful answers, it is unlikely that the culture will be right for integrating data analysis because it requires an awareness of current limitations and a desire to promote change and learning. Integrated Data Analytics can also provide an organisation with tremendous insights into its processes and support its objective of being a “Learning Organisation” if the will is there to take action.

> *Learning organizations are where people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective aspiration is set free, and where people are continually learning to see the whole together.*
> **Peter Senge, 1990**

VIII. WHAT NEXT FOR THE NUCLEAR SECTOR?

In many respects the nuclear sector is well placed to take advantage of integrated data analytics because it is a highly technical, engineering-based sector that uses plant and reactor simulators, robotics, advanced process control systems and has demanding maintenance programmes. It is also the case that in the last 10-15 years the cost of security has spiraled upwards and now uses a significant percentage of the operating budget – anything up to 8% of the total operating budget for nuclear power plants (NPPs). On many NPPs there are more security personnel on shift duty than any other type of employee/ contractor. The threat from cyber attacks is understood and real and the reputational impact of a significant security event, just like safety, would have major consequences. There is a growing realisation following the Fukushima Daiichi incident that the initiating event for a major crisis could be either a safety or security event, and that there needs to be a closer relationship between safety, security and emergency planners/responders; encouraging signs for developing enterprise-wide approaches and the integrated data management systems required to support them.

We are also aware that the field of integrated data analytics is considered to be relatively new in some quarters and that a period of familiarisation is required, and hope that this White Paper helps to support that process.

There are opportunities through conferences (such as the IAEA Nuclear Cyber Security Conference in Vienna in June 2015 and the INMM Conference in July 2015 in the US) to promote the key messages in this paper, and to approach influential nuclear industry groups to establish their interest. Just as the Information Security Forum (ISF) has an industry working group on Big Data, with over 100 corporate members, we should seek to establish a nuclear sector “group of the willing” to become engaged, with the objective of finding ways to support a pilot scheme. Perhaps this will be part of a bigger National Critical Infrastructure project, since experience already exists in this sector and some governments are investing heavily in this “new” technology.

WINS will also maintain an active interest in the field and use its influence and activities (including workshops on Meaningful Security Performance Metrics, and the Interface between Cyber and Physical Protection, both scheduled for Spring 2015) to help catalyse further interest in the deployment of integrated data analytics.

You can support WINS and this research by helping identify where integrated data analytics are being utilised in the nuclear sector (especially for security-related risk management) and the benefits and issues that are being experienced by practitioners, including bets practices.

IX. FURTHER READING

— Where have you been all my life? How the financial services industry can unlock the value of Big Data, October 2013, PWC Financial Services Institute, *http://www.pwc.com/us/en/financial-services/publications/viewpoints/unlocking-big-data-value.jhtml*

— The case for an enterprise-wide approach to risk management, July 2010, Turner and Townsend, *www.turnerandtownsend.com/*

— Why Integrate Physical and Logical Security? June 11, 2011, CISCO Systems, *https://www.cisco.com/*

— Securing Cyber-Physical Systems, Alvaro Cárdenas Fujitsu Laboratories and Ricardo Moreno Universidad de los Andes, www.csrc.nist.gov/

— Understanding Big Data, Analytics for Enterprise Class Hadoop and Streaming Data, 2012, Paul C. Zikopoulos, Chris Eaton, Dirk deRoos, Thomas Deutsch and George Lapis, Published by McGraw Hill

— Various Reports from WIPRO, *http://www.wipro.com/insights/industry-research/*

— Various Reports from Splunk, Splunk App for Enterprise Security, Advancing analytics-driven security, *https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/splunk-app-for-enterprise-security.html*

— Various Reports from Oracle, Big Data Analytics, *http://www.oracle.com/technetwork/database/options/advanced-analytics/bigdataanalyticswpoaa-1930891.pdf*

— Various Reports from Palamir, *http://www.palamir.com/enterprise/*

— Various Reports from NICE, *http://www.nice.com/security*

OUR VISION

To help improve security of nuclear and high hazard radioactive materials so that they are secure from unauthorised access, theft, sabotage and diversion and cannot be utilised for terrorist or other nefarious purposes.

OUR MISSION

To provide an international forum for those accountable for nuclear security to share and promote the implementation of best security practices.

2015 © World Institute for Nuclear Security (WINS) All rights reserved. Graben 19, A-1010 Vienna (Austria)
Tel.: +43 1 23060 6081 | Fax: +43 1 23060 6089 | Email: info@wins.org | Internet: www.wins.org
International NGO under the Austrian Law BGBI. Nr. 174/1992 | GZ: BMeiA-N9.8.19.12/0017-I.1/2010

ISBN 978-3-903031-66-1