OPERATIONAL TRANSPARENCY: AN ADVANCED SAFEGUARDS STRATEGY FOR FUTURE ON-LOAD REFUELLED REACTORS

J.J. Whitlock and D. Trask
Atomic Energy of Canada Limited

Abstract

The IAEA's system for tracking fuel movement in an on-load refuelled heavy-water reactor is robust, but an opportunity remains to exploit the wealth of data streaming from the reactor vault during operation and provide real-time, third-party monitoring of reactor status and history. This concept of Operational Transparency would require that large amounts of operational data be reduced in near-real time to a small subset of high-level information. Operational Transparency would enhance the IAEA's ability to monitor the state of the core to an unprecedented level. This paper provides an overview of the novel concept of Operational Transparency in heavy water reactors, using potential application to CANDU reactors as an example, and explores some of the technical challenges that will need to be solved for efficient implementation.

1. Introduction

Traditional "comprehensive" IAEA safeguards (i.e. those implemented under a State-level Comprehensive Safeguards Agreement, or CSA [1]) are based upon accountancy and control of nuclear material, administered through a "State System for Accounting for and Control of Nuclear Material" (SSAC – in Canada represented by the CNSC) on behalf of the IAEA, and verified by the IAEA through inspection. The IAEA maintains Continuity of Knowledge (CoK) between inspections through a combination of Containment and Surveillance (C&S), including seals, cameras, and other monitoring instrumentation. In addition, the IAEA has access to operational data from the safeguarded facilities, which it can use in the investigation of perceived anomalies.

Many countries, including Canada, have also implemented an Additional Protocol to these comprehensive safeguards[1], giving the IAEA enhanced inspection and sampling powers that enable it to draw broader conclusions about a State's likelihood to be engaged in clandestine proliferation activities, particularly at locations beyond the boundaries of facility-based traditional safeguards. The Additional Protocol was developed in response to inherent weaknesses in the traditional approach exposed by Iraq's clandestine program following the first Gulf War (1990-'91).

A smaller number of countries, including Canada [2], operate under an Integrated Safeguards (IS) regime, based upon the above State-level conclusion about absence of proliferation activity. Under an IS regime safeguards verification can be less frequent, and randomly scheduled, allowing greater efficiency for the IAEA. The IS regime relies on a more "information driven"

[1] See www.iaea.org/OurWork/SV/Safeguards/sg_protocol.html.

approach to verification; in effect the IAEA endeavours to work “smarter” rather than “harder” to achieve the same overall safeguards goals.

Globally, the class of on-load refuelled (OLR) reactors is represented most prominently by the CANDU design. CANDU reactors in Canada and off-shore, whether or not operating under an IS regime, are subject to safeguards that include special instrumentation to count fuel bundles exiting the core and entering the spent fuel reception bay (see Figure 1). In this respect, CANDU reactors tend to have more advanced and comprehensive safeguards than other commercial designs [3]. For example, the safeguards approach to a PWR relies on the fact that unauthorized access to the core between refuelling outages would be obvious to outside observers due to the required shutting down of the core.

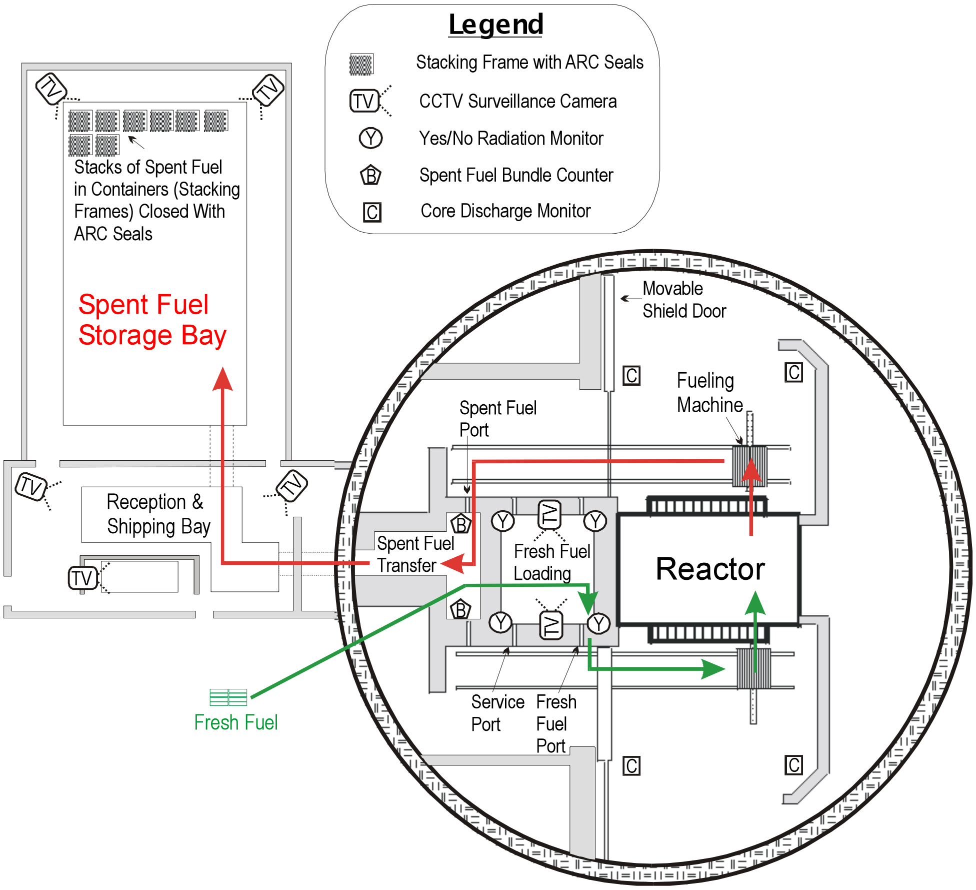


Figure 1 Typical IAEA Safeguards Equipment for CANDU [4]

2. The Challenge

The IAEA considers CANDU reactors to be sufficiently safeguarded, but at a greater expense to the IAEA than other designs due to the need to verify daily fuel movement and more frequent transfers of used fuel to dry storage. Significant efficiencies have been achieved in both of these areas, particularly in jurisdictions operating under an Integrated Safeguards regime, through remote monitoring and reduced inspection frequency [2]. Additional achievements in efficiency in the safeguarding of CANDU reactors will of course always be welcomed.

More generally however, some concern is associated with the safeguardability of advanced (non-CANDU) OLRs now under development – including both process flow reactors (aqueous or slurry systems such as the Molten-Salt Reactor), and "quasi-process" flow reactors such as the pebble-bed designs. These technologies require a stochastic approach to fuel management that is fundamentally unsuited to traditional IAEA nuclear material accountancy and control methods. This has prompted the IAEA Novel Technologies Unit, for example, to explore more advanced and less discrete methods of monitoring, such as the potential use of anti-neutrino detectors to monitor bulk consumption of fissile material.

At a somewhat higher level of observation is the following notion: regardless of the technical soundness of traditional safeguards processes, there will likely be an need within the "nuclear renaissance" to provide increasing levels of assurance and comfort to the public that safeguards are robust, in order to retain social acceptance for continued and expanded operation. In a similar sense that guides emerging nuclear safety and security concepts, one envisages a need for increased transparency of the soundness of nuclear safeguards. The more linked these goals are to inherent and operations-based features of the technology, the more confidence the public will tend to have in their effectiveness.

It is in this context of increased efficiency and effectiveness with regards to emerging OLR safeguards implementation, as well as social acceptance of nuclear safeguards in an evolving nuclear renaissance, that the concept of "Operational Transparency" is proposed as an attractive, and perhaps necessary, safeguards concept for further development, with specific application to current heavy water reactors for development and demonstration purposes, as outlined below.

3. The Opportunity

CANDU reactors represent conceptually a "stepping stone" in the technology path from current bulk-refuelled systems with discrete accountancy, to process-flow OLRs with stochastic accountancy. A CANDU system is a well-characterized, well-understood system with a long track record of robust safeguards, while at the same time involving a daily flow of a relatively small-item fuel inventory during operation.

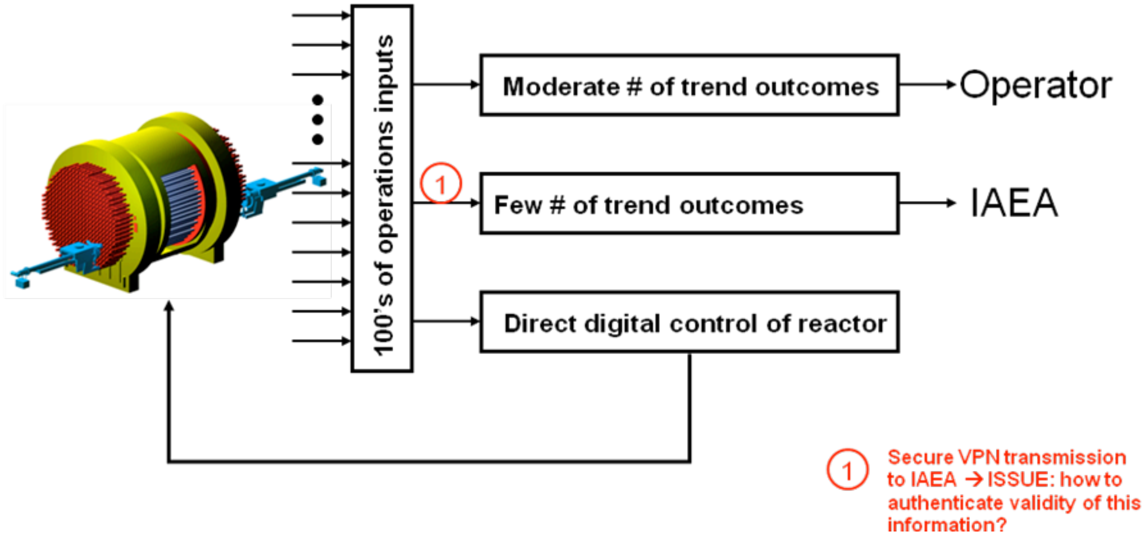
It is conceivable that CANDU reactors could be utilized in the development of advanced safeguards techniques that fall under the general category of "Operational Transparency" – the use of real-time operational data in the implementation of safeguards monitoring. Currently, spent fuel reprocessing plants represent the biggest challenge to the IAEA in terms of process-flow accountancy, although most of these facilities have historically avoided full IAEA safeguards since they tend to be located within Nuclear Weapons States. As the IAEA makes increased use of remote monitoring of discrete and process-flow systems, it becomes a smaller and smaller additional step to remotely monitor the actual operational data of these systems, in real time.

The advantage of implementing this approach on a demonstration basis at a CANDU plant is that the data characterizing fuel movement already exists, since fuelling machine movement within the vault is an automated and fully indexed process. In combination with the wealth of in-core data available from operational instrumentation, this presents a sizable real-time digital record characterizing the use and movement of fissile material, which the IAEA can mine for trend verification. The challenges, therefore, lie in the authentication of the raw data itself, and the efficient processing and reporting of information.

These two challenges are briefly addressed below.

4. CANDU Operational Transparency

As mentioned above, the IAEA currently has access to operational data from CANDU stations; however, in practice this wealth of information is only mined in the case of anomalies. The goal of Operational Transparency is to access much the same information, but in real time or near-real time through the same process and status signals used by the plant Operations. In the case of a CANDU reactor this would include in-core flux measurements, pressures, temperatures, reactivity mechanism positions, and fuelling machine positioning. This large amount of data would be processed by IAEA software that determines operational trends and flags deviations from routine operation.


100's of operations inputs
Moderate # of trend outcomes
Operator
1
Few # of trend outcomes
IAEA
Direct digital control of reactor
1

Secure VPN transmission to IAEA → ISSUE: how to authenticate validity of this information?

Figure 2 Concept of Operational Transparency applied to CANDU

The emphasis, therefore, is on trending and stochastic analysis of data, rather than discrete accountancy. This approach is in alignment with the mode of operation of process-flow facilities, and also in alignment with the emerging concept of "Information-Driven Safeguards" that the IAEA is moving towards as an efficiency measure.

This information flow is shown in Figure 2, starting with hundreds of operational inputs from the reactor core. These signals are used in the direct digital control of the reactor. The same raw signal flow is processed to provide trending and other status updates to the Operator, representing a moderate number of outputs that can be selected, displayed and further analysed in the control room or by Operations support staff elsewhere at the site.

The innovation of Operational Transparency is to independently process this same raw signal flow, either on IAEA servers at the plant site or remotely at IAEA headquarters in Vienna, and produce a relatively small number of trended outcomes that inform IAEA safeguards verification staff. For example, one can think of a number of output flags numbering less than ten, of which any single negative output indicates a significant deviation from normal operation based on processing and trending of hundreds of raw inputs.

The software to provide this trending and analysis is essentially similar to that which is used by Operations at the plant itself. The challenge, therefore, is not necessarily the processing of the data to provide useful intelligence at the IAEA, but the robustness of the data flow itself as indicated in Figure 2: authentication of the original data (which originates from the reactor Operations instrumentation), and reliability of the data transmission (which originates in the State of potential concern). Robust cyber security is therefore a critical component of Operational Transparency.

5. Achieving a Necessary Level of Cyber Security

The sheer quantity of data logged from any operating nuclear system will require an innovative approach to cyber security in order to establish confidence in the information. Fortunately the voluminous and systemic nature of the data itself will provide some measure of this confidence, in that the interaction of the hundreds of data flows is a complex relationship leading to system-wide signatures that will be difficult to mimic. Trending software can be tuned to look for particular anomalies, and trends of anomalies that will highlight the presence of data tampering.

The strategy is to use the properties of the process itself to verify streams of data to one another. For example, the detailed flux map of an operating CANDU core, along with zone level indicators, can be used to generate an expected fueling scenario (in a similar process that the Operator would be expected to use to generate fueling scenarios). This expected scenario can then be digitally compared against the actual fueling operation as interpreted from fuelling machine movement and core discharge monitors. Significant discrepancies would be flagged for further investigation, and it is only at this point that human engagement in the verification process takes place.

Another advanced technique of data authentication is to multiplex the raw signal data with a unique signature that corresponds specifically to the raw data source and can be manipulated in real time. The manipulation of the signature and corresponding timestamp ensure that the data originated from that specific source at that specific time and thus ensures that the data was not pre-recorded or spoofed by another source.

In addition to the issue of data authentication at source, a subsequent concern is reliability of the data transmission itself. In this respect the IAEA has a significant amount of experience with Remote Monitoring, and has developed sufficient confidence in the effectiveness and efficiency gains presented by the technology to move towards a broader implementation of the concept of Remote Safeguards Inspections [5] [6] [7]. The ability to remotely collect and analyse both monitoring and operational data is recognized as a mature option that enables the IAEA to reduce costs while implementing many of the effectiveness measures introduced by Integrated Safeguards. Reliability of data transmission therefore does not appear to present a significant challenge to the concept of Operational Transparency, although the sheer increase in volume of data may present an added technical challenge. In this respect it is possible that remote (satellite) data processing at the site, and transmission of a reduced data set to IAEA headquarters, would present one possible solution.

6. Summary

In summary, Operational Transparency offers the following enhancements to the current reactor safeguards regime:

1. Access to the core of an OLR while operating, in a virtual sense. The current paradigm of monitoring material flow in and out of the core is adequate for CANDU technology but will be insufficient for advanced process flow and quasi-process flow reactor technologies.

2. Dependence upon trending and stochastic processes, with a resulting greater ability to detect unforeseen off-normal events. The need to second-guess all modes of technology misuse or material acquisition, required with deterministic safeguards approaches, is replaced with a system-level sensing capability.

3. Significant example of "information-based" safeguards, which can potentially offer more comprehensive coverage, using less IAEA inspector time and resources. Efficient processing of operational information robustly supplied and verified, can therefore enhance a traditional CSA regime or support an Integrated Safeguards implementation.

4. A perception of greater transparency of application, in that independent oversight of nuclear material movement and storage is tied to operational data that is difficult to mask or modify. This leads to increased public confidence in the effectiveness of safeguards based on this concept.

Strategically, prototype application of Operational Transparency to a CANDU plant would provide a test-bed for development of stochastic remote monitoring techniques for use with advanced process-flow and quasi-process flow reactor systems under development.

7. References

[1] IAEA Safeguards Glossary, 2001 Edition, June 2002, available at: www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_prn.pdf.

[2] E.F. Saburido, N. Whiting, J. Doo, "Information driven safeguards: new concepts for implementing the State Level Integrated Safeguards Approach in Canada", IAEA Symposium on International Safeguards, Vienna, Austria, Oct. 31-Nov.5, 2010.

[3] J.J. Whitlock, A.G. Lee, "CANDU: Setting the Standard for Proliferation Resistance of Generation III and III+ Reactors", International Conference on Opportunities and Challenges for Water Cooled Reactors in the 21st Century, Vienna, Austria, Oct. 27-30, 2009.

[4] IAEA Technical Report Series No. 392, "Design Measures to Facilitate Implementation of Safeguards at Future Water Cooled Nuclear Power Plants", 1998.

[5] K. Schoop, P.Schwalbach, J.F. Levert, G.Basso, M. Boella, D. Korosec, J. Regula, "Developments in Implementation of Remote Data Transmission", IAEA Symposium on International Safeguards, Vienna, Austria, Oct. 31-Nov.5, 2010.

[6] J. Araujo, C. Charlier, D. Hatt, A. Lebrun, N. Muroya, P. Rance, I. Tsvetkov, R. Zarucki, M. Zendel, "Enhancing and Optimizing Safeguards Implementation by Remote Safeguards Inspections", IAEA Symposium on International Safeguards, Vienna, Austria, Oct. 31-Nov.5, 2010.

[7] I. Tsvetkova, D. Hatta, O. Heinonenb, B. Morana, N. Muroyaa, R. Zaruckia, M. Zendela, "Remote Safeguards Inspections: Concept and Practicalities", IAEA Symposium on International Safeguards, Vienna, Austria, Oct. 31-Nov.5, 2010.