UKNI
UNITED KINGDOM – NORWAY
INITIATIVE

Trust in Verification Technology

A case study using the UK-Norway Information Barrier

Introduction

This paper summarises the key insights into the development of trusted technologies for verification that have been gained through the UK-Norway Initiative (UKNI). By investigating the issues arising during development of an 'information barrier' – nominally for use in the context of nuclear warhead dismantlement verification – participants in the UKNI have explored approaches for building equipment that can be trusted by parties that do not necessarily trust each other.

This is not a straightforward problem. Given what might be at stake in a future nuclear weapon verification scenario, it is not enough to assume that equipment intended to fulfil one particular purpose is in fact performing as intended: given that trust between verification parties may well be low, it seems incongruous to trust that verification equipment is fine. In the software industry vast sums of money are spent on anti-virus or malware protection because of the risk that malicious actors might attempt to exploit vulnerabilities in existing computer programs. Similarly in verification, we are motivated to consider ways in which it might be possible to satisfy ourselves that verification equipment is performing as intended and has not been exploited in some way.

Three main issues are considered in this paper. In an arms control environment it is clearly very important to ensure that inspection data are accurate, genuine, and that any measurements recorded are indeed the products of the item being measured. At the same time it is also important to ensure that sensitive information – which might be sensitive for national security or non-proliferation reasons – is protected. The host must be confident that equipment deployed into sensitive facilities is suitable for the environment into which it is deployed (in terms of safety, for example), and that the equipment cannot be used for espionage. Finally, it is also important to understand what verification measurements actually mean in an operational context.

It is clear that neither the host nor inspector is likely to want to simply trust equipment, although they will probably have different reasons for their concerns. Each party will instead need to build confidence that verification equipment is working as they expect, by actively making sure that any identified risks are mitigated and opportunities to exploit unidentified risks are controlled and minimized. However, given the different concerns of host and inspector in relation to the use of verification equipment, the requirements of the host for building confidence are unlikely to align with the requirements of the inspector for building confidence.

For either party individually, requirements for confidence could be met by designing and building (or sourcing and supplying) equipment to their own specification, and then operating that equipment in the manner most suited to their own needs. However, the host might be concerned, for example, that inspector-supplied equipment might have additional functionality designed to facilitate espionage. Conversely, the inspector might be concerned that host-supplied equipment would generate bogus results in order to fool the verification process. This means that, in order to satisfy both partners' requirements for confidence, any solution for collecting and analysing the data must be mutually agreed.

Collecting Data about Nuclear Weapons: Attributes and Non-Proliferation

Information about the design of nuclear weapons can be highly proliferative as well as sensitive from a national security perspective. Because of this, direct measurements of certain physical characteristics of nuclear weapons would be extremely challenging, if not impossible, to implement in a potential future verification regime. At the same time, amongst the sensitive data, potentially useful information exists if it can be extracted. A solution to this problem has been proposed in the form of 'information barriers'.

Information Barriers

Conceptually, an information barrier analyses data that contains sensitive information and produces results that are then communicated as an unclassified output: See figure 1.

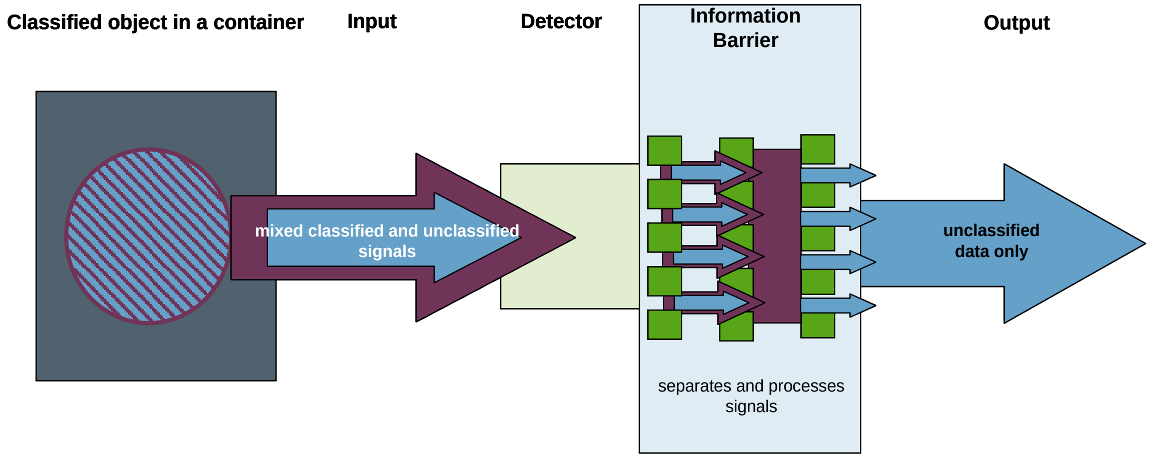
Classified object in a container
Input
Detector
Information Barrier
Output
mixed classified and unclassified signals
unclassified data only
separates and processes signals

Figure 1: A conceptual information barrier

Two different basic approaches to protecting sensitive information about physical properties of warheads with information barriers are commonly discussed:

- *Template matching* entails devising a measurement system which can confirm, over repeated measurements, that some pre-determined physical properties of an object remain unaltered, without revealing the specific values of the properties being measured. This means that inspectors can verify that properties of the object remain unaltered over time, or that a class of objects all exhibit similar properties.
- An *attribute measurement system* with an information barrier ensures that measurements taken on sensitive objects result only in the release of information that confirms the

presence (or absence) of some mutually agreed attribute (or attributes), or indicates if evidence has not been found. Using attributes, inspectors can verify that certain properties of the object meet pre-determined criteria at the time the measurement is taken.

Verification using attribute measurements

If the parties agree to pursue attribute measurement as the basis of their approach to verification, as the UKNI participants did at the beginning of the information barrier project in 2007, then the decision of which attributes are acceptable to both parties is only a first step. Both parties must also be satisfied that the method used to determine whether a particular object passes the tests set for the attributes is suitable. This process of determining a suitable method could well be challenging. It might not be possible to discuss some of the measurement issues (intervening materials between the fissile material and detector, for example) that would otherwise influence the development process, and which would normally be constrained or known under laboratory measurement conditions, because the relevant details are themselves sensitive.

Confirming presence or absence of the attribute in question must be useful for verification while also avoiding any compromise to the host's national security, or release of proliferative information. The latter point is particularly relevant (including for a research project such as this) when a non-nuclear weapon state is involved.

The UKNI Approach

Given all these considerations, the UKNI set out to investigate how treaty partners can each build and maintain confidence in an information barrier that could be used as part of a system designed to detect certain attributes of a nuclear warhead or other Treaty Accountable Item (TAI) [1] without revealing any sensitive information. The UKNI information barrier project has operated in the context of an imaginary nuclear weapon dismantlement scenario, where the plutonium core of the weapon is considered the TAI.

UKNI participants agreed that two attributes for verification would be:

- The presence of Pu -239; and
- A ratio of the plutonium isotopes Pu-239 to Pu-240 above some suitable threshold.

There is no common definition of weapons-grade plutonium, but is it commonly accepted that plutonium suitable for nuclear weapons should have relatively little Pu-240 isotope in relation to the Pu-239 isotope. There would certainly be significantly less Pu-240 in weapons-grade plutonium than there would be in plutonium produced in the civil nuclear

[1] A TAI is any object that is accountable under the treaty in question. In this case it refers to an object that inspectors would track through a dismantlement process to verify that a declared nuclear warhead has indeed been dismantled

fuel cycle. For the purposes of the project we used the ratio of nine parts Pu -239 to every one of Pu-240 as the threshold. This is not quite the same as saying that the threshold is 90% Pu-239, because other minor isotopes of Plutonium that are also present are discounted, but for the purposes of this paper we will henceforth refer to the 'threshold' as 90% Pu-239. We will return to discuss lessons on threshold setting later.

Developing Confidence in Equipment

Agreeing a theoretically suitable data analysis method is the first step; that method must be implemented in an agreed manner if both parties are to be satisfied. This requires that equipment must be designed and built in a manner which is transparent enough such that both parties can assure themselves that the analysis method has implemented as agreed, with no additions or changes. Both parties must also then be able to maintain confidence in the correct functioning and operation of the equipment once built.

The hardware, software, deployment process and lifecycle of the IB all require consideration and agreement. Changes to any one element may impact upon the conceptual operation of the equipment, including how mutual confidence is built and maintained. If left unchecked, design changes may lead to the development of gaps in the confidence building process, and so confidence could be lost.

For some equipment, mutual agreeable solutions may be easy to define. For other equipment, a solution may be significantly more complex. In either case, the level of 'trust', either in the equipment or between the parties, should not be relevant for the confident operation of equipment.

Confidence Building by the Host: Certification

Before any equipment is deployed into a controlled facility, the facility authorities – which have ultimate responsibility to their own national authorities for the safe and secure operation of that facility – will assess the equipment for any potential negative consequences that may arise from deployment. Assuming that the equipment isn't prohibited outright, restrictions on use or other operating conditions may be stipulated. Only under the defined operating conditions may that equipment be used, and even then it may only be used for a specific, defined purpose. This process of assessment is termed certification.

Safety

Equipment must be certified for safe operations in all areas where it is to be used. Of special relevance to nuclear weapons dismantlement verification is certification for operations in explosive facilities.

Safety requirements and certification of this type are also common in civilian facilities which handle explosives. Electronic equipment must be evaluated to ensure it can not discharge large amounts of energy into explosive materials under normal or abnormal conditions, to minimize the risk of accidental detonation. Modifications to equipment require risks to be reassessed. Changes could entail an altogether new assessment and certification process.

National security and non-proliferation

In many sensitive facilities there are severe restrictions on the use of equipment, not just by visitors but also facility staff. For instance, personal electronic devices (e.g. phones, cameras) are regularly prohibited in such locations. This sort of prohibition is a good example of an information security measure that many people are familiar with, in the commercial world as well as in military facilities. In a nuclear facility, restrictions might be put in place to protect physical security measures associated with the facility, or information about the items contained or processes conducted within the facility.

The use of any equipment – particularly radiation detection equipment or other electronic devices – by inspectors in the presence of nuclear weapons, in a weapons facility, therefore presents a clear security concern. However, if radiation detection equipment is to be used as part of an attribute measurement or template matching approach to verification, prohibiting the use of the equipment outright is clearly not acceptable.

The concept of an information barrier is used to satisfy the host's concern with regards to protecting proliferative and sensitive information. Nonetheless, the implementation of the concept needs to be conducted in a way which continues to satisfy host concerns throughout the lifecycle of the equipment – not just during operation. In order to be certain that all individual Information Barriers are built as agreed (and are therefore without modifications that could put security at risk), the host may well insist on manufacturing and supplying equipment.

This may prove problematic for inspectors, but it may be the only solution that results in authorisation for the deployment of inspection equipment into sensitive facilities. Consider an alternative case: equipment provided by another party, even if built according to a jointly-agreed design, could be subjected to such thorough certification assessment by the host (including dismantlement and detailed examination) the confidence of the inspecting party in the equipment would be lost, negating any benefit of inspectors providing equipment in the first place.

The UK-Norway Initiative approach to certification

In order to handle the issues of security certification, the UKNI has therefore worked therefore under the constraint that inspection equipment will be built and supplied by the host party. This situation may be considered the worst case scenario (from the perspective of the inspector) but has allowed the project team to consider how to operate under these stringent conditions.

Several design decisions in the UK-Norway information barrier were instigated to aid the certification process and have their basis in minimizing the amount of sensitive data captured by the device, as well as making it very difficult for the device to reveal any of the sensitive data which it could be exposed to. Some of the design elements meant to protect sensitive data are:

- No persistent memory for storing recorded data

- No outside communication channels (including battery power supply unit)
- Only green/red light as output
- No inspector access to equipment after it has been used inside sensitive/high-security areas

Additionally, to ensure the safety requirements are met for representative environments in which the information barrier might be deployed, the IB has been designed and built to meet requirements for use in facilities which handle explosives, particularly with regard to electromagnetic interference and compatibility.[2] .

Confidence Building by the Inspector: Authentication

Undertaking inspections with host supplied equipment is of course a severe disadvantage to the inspecting party; it raises questions about the extent to which the inspectors can be confident in the results from their measurements and whether the host party has in any way interfered or tampered with the measurement equipment prior to the inspection activities. If the inspectors cannot have confidence in their equipment then there is very little value in performing measurements with this equipment at all.

The UKNI has explored the extent to which it is possible for inspectors to build confidence in host-supplied equipment, and joint development of the inspection equipment can help facilitate this. With a transparent, joint design, both parties develop the same expectation and understanding regarding how the equipment *should* be built and the expected performance characteristics. This is not enough in itself, though: the inspecting party will need to undergo a process of developing and maintaining confidence that the equipment presented conforms to the mutually agreed design and agreed operational parameters. This process of building confidence is termed 'authentication'. Authentication requirements must be integrated early into the overall design of the system to ensure they are met under all circumstances

The information barrier developed by the UK-Norway Initiative is a measurement system that can be divided into three different parts: the hardware, comprising of the electronics; the software, containing the instructions to the microcontroller in the information barrier; and the procedures for deployment and use. Authentication processes need to be folded into deployment and use procedures, since it is the controlled use of the equipment that allows both parties to gain and then maintain confidence in the operation of the information barrier

The development of all these parts of the information barrier (and consideration of how they interact) has been focused on making a design which is possible to authenticate for an inspecting party, whilst maintaining facility certification. Authentication requirements under

[2] The design of the IB has been guided by chapter 8, volume 1, edition 2, change 3 of the United Kingdom Joint Services Publication 482, Nov 2006., and European Standards IEC 61000-4-2:2008, EN 61000-6-2:2005, EN 61000-6-3:2007

controlled conditions need to be considered for any equipment entering sensitive facilities, not just the UKNI information barrier.

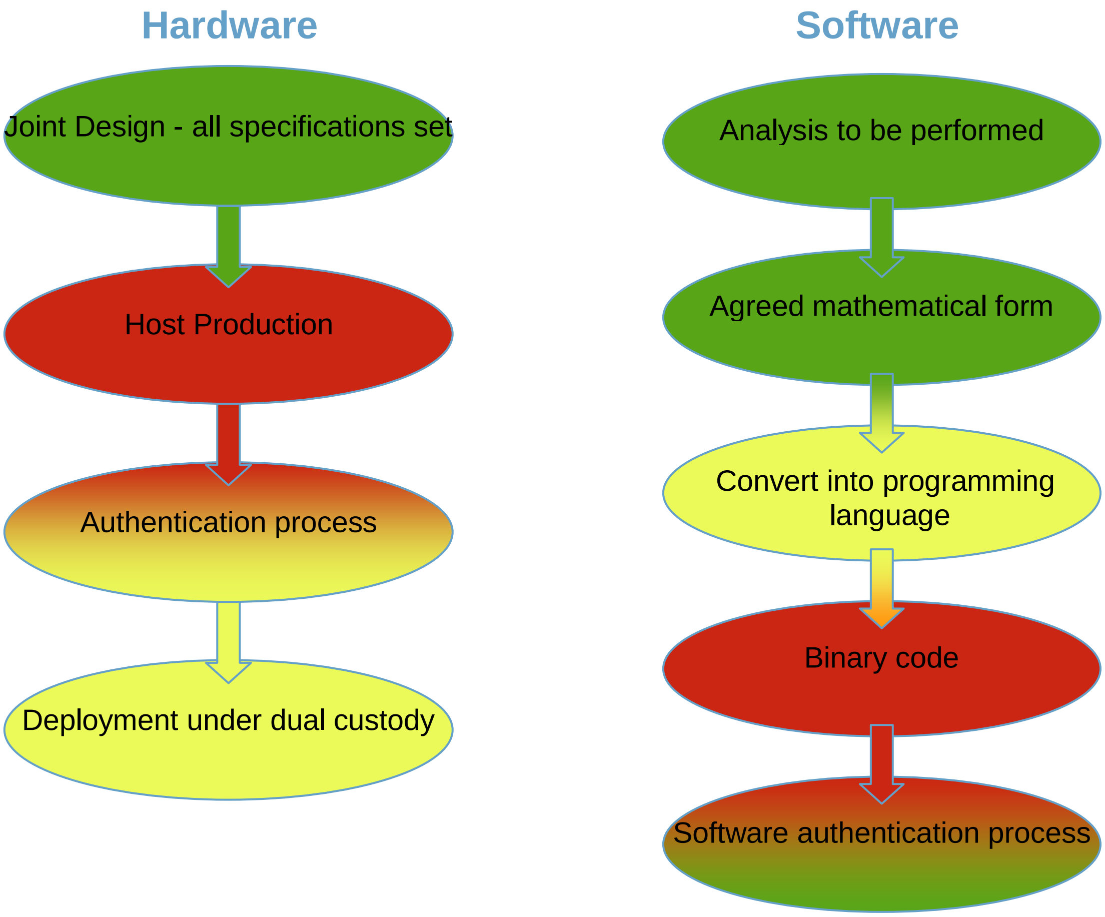
Hardware
Joint Design - all specifications set
Host Production
Authentication process
Deployment under dual custody
Software
Analysis to be performed
Agreed mathematical form
Convert into programming language
Binary code
Software authentication process

Figure 2: Conceptual processes for building mutual confidence. Note that software development and authentication is embedded within the overall process of designing and authenticating the hardware

Developing hardware for authentication

To authenticate hardware, it should be possible to investigate the item in question to ensure it has been built as agreed and that no modifications, additions or subtractions have been incorporated without consent from all parties. In an attempt to make the hardware of the information barrier possible to authenticate, and also to facilitate host certification of safety and security, a guiding principle for the development has been to keep the design as simple as possible. This principle has been followed on the assumption that fewer, simpler components will make it easier for the inspecting party to authenticate that all components are functioning as intended, and that no additional functionality has been added by the host party to influence ('spoof') the measurements. For example, a simple microcontroller, with a limited set of functions and memory, was preferred to more advanced microcontrollers, in an effort to simplify the authentication of that aspect of the hardware. The UKNI IB also uses a modular build, where separate functions are placed on separate electronic boards. Each board can easily be swapped out and replaced in order to facilitate authentication strategies that rely on destructive authentication of a number of randomly-selected boards to allow the confident use of the rest of the population ('authentication by association'). The information barrier has a number of electronic boards: including a high- and low voltage power supply, an analogue processing board and a digital processing board.

Developing software for authentication

Developing software in which both parties can be confident imposes several requirements on the development and the code itself. Since binary computer code is not readily interpretable without considerable background knowledge about the intended function of the code and the processor on which the code runs it is challenging for the inspectors to verify that the software running on host supplied equipment is the one mutually agreed between the parties. The UK-Norway Initiative decided at an early stage to pursue two different development tracks with slightly different priorities when it comes to building confidence in software, in order to better understand how authenticated software might be achieved.

The first track, pursued from the UK side, emphasised the need to demonstrate that the code on a microcontroller is correct in the sense that all procedures and algorithms agreed upon behave as intended in the software, and that any additional code would be highlighted for investigation. For this task the programming language SPARK was chosen. The way SPARK has been developed makes it is possible to obtain a very high degree of confidence in the correct implementation of agreed functionality, using that language. SPARK is a 'high-level' programming language so is closer to written English than machine code, which makes it the more readily interpretable to humans. However, because SPARK is a high-level programming language, the code also has to be passed through a compiler to make executable code for the microcontroller. The drawback of this approach is that the compiler makes it difficult to show the one-to-one correspondence between the SPARK code and the resulting machine code that the compiler generates.

To be able to gain confidence in the machine code itself the second track of software development, pursued from the Norwegian side, chose to use low-level assembly language for software development. Assembly language is closer to machine code, which makes it possible to follow exactly which operations the microcontroller executes. The code does not rely on external code libraries or compilers and is as such a self-contained, complete and transparent set of instructions for the microcontroller. The disadvantage of using assembly language lies in the fact that the low-level instruction set makes coding very labour intensive, and difficult to analyse.

As a final step towards validation of the complete set of machine code, the UKNI has developed a concept for showing equivalence between the SPARK and the assembly code. This means that one could make use of the advantages for both software development approaches to arrive at mutually agreed software for the microcontroller. Both parties can then be confident that the binary code performs the agreed functionality correctly and does not carry out any operations other than those agreed. It must be said that the validation procedure developed can only demonstrate close correspondence between the two versions of the IB code are currently implemented, rather than equivalence. This is because of code implementation differences chosen by the software engineers – the consequence of the differences could not be evaluated at the time they were chosen. This situation has resulted in the lesson of how strictly implementation requirements need to be defined to ensure software is coded in a defined, standard way.

Authentication procedures

It has proved challenging to develop authentication procedures that would not invalidate host certification. For the equipment to be authenticated, hardware and software need to be interrogated to determine conformance with the agreed design. The digital boards have been designed such that limited hardware tests on the equipment can be made with simple host-supplied equipment, in order to check aspects of its behaviour. However, this is not a robust authentication measure because tests must be carried out in a strictly defined fashion under host supervision, in order to maintain certification.

To authenticate the information barrier the project has had to rely on 'authentication by association'. As noted above, this is a procedure of random selection where inspectors are presented with a number of host-provided information barriers (or components). They can then choose a set of those items to enter the facility for operational use and another set are selected to take away so inspectors can conduct their own investigations in private, using all the technical means at their disposal, to verify that the information barriers are built as agreed. This gives the widest possible scope for those investigations, but also means that specific information barriers used to perform measurements will not have been directly authenticated.

Maintaining Joint Confidence

Once the information barrier is authenticated – either directly or by association – both inspectors and host will have to establish joint chain of custody over the equipment so that they can be confident that no tampering with, or replacement of, authenticated items can occur. The details of how this can be done in practice are highly dependent on the details task to be accomplished through use of the equipment. There is no single process that could be sufficiently designed to meet requirements for the broad array of facilities in which the equipment could be used or for the processes it might be used to monitor.

In the absence of a fully detailed verification protocol which would specific such details, the UKNI has developed a general deployment procedure (Figure 3) to allow further exploration of the issues in general terms. However, exact requirements on equipment and procedures for keeping chain of custody over authenticated IBs would have to be implemented based on the specific requirements of a concrete verification task. Therefore, we have been able to give an indication of what requirements might be in general, but it would be misleading to attempt to give more specific recommendations.

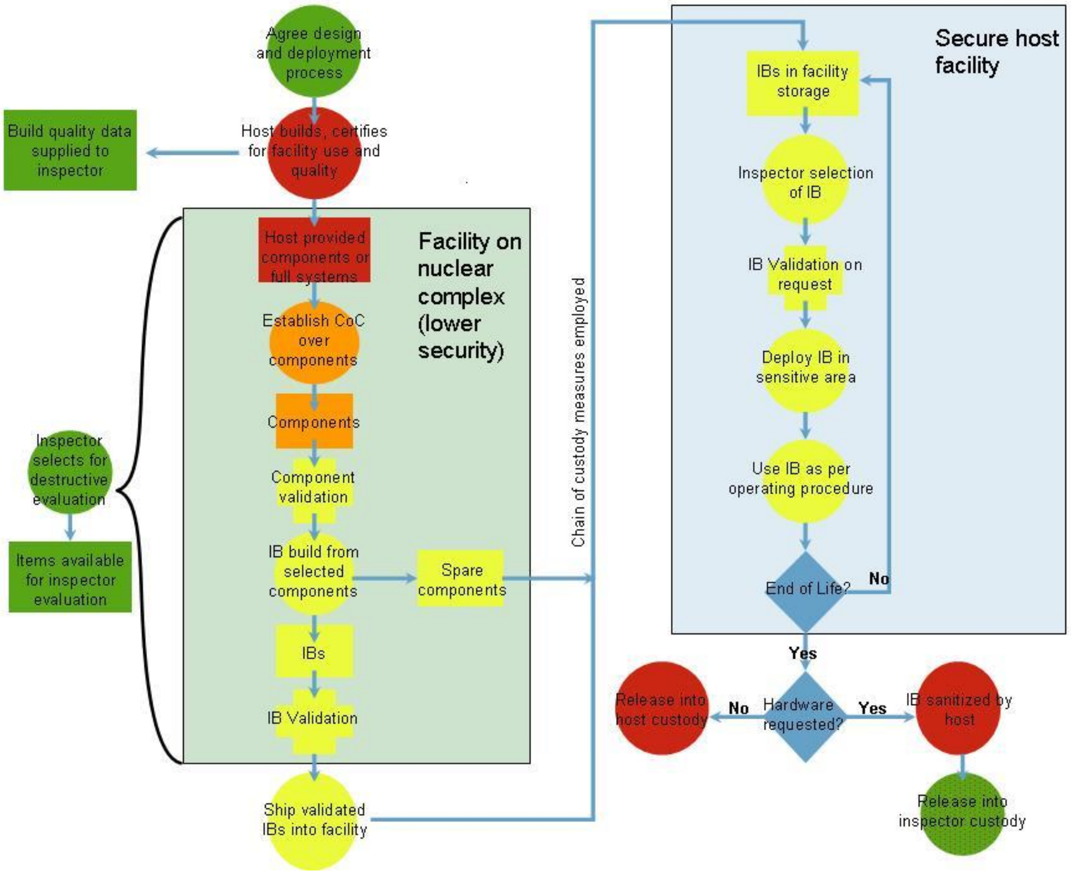
Agree design and deployment process
Host builds, certifies for facility use and quality
Build quality data supplied to inspector
Facility on nuclear complex (lower security)
Host provided components or full systems
Establish CoC over components
Components
Component validation
IB build from selected components
Spare components
IBs
IB Validation
Inspector selects for destructive evaluation
Items available for inspector evaluation
Ship validated IBs into facility
Chain of custody measures employed
Secure host facility
IBs in facility storage
Inspector selection of IB
IB Validation on request
Deploy IB in sensitive area
Use IB as per operating procedure
End of Life?
No
Yes
Hardware requested?
No
Yes
Release into host custody
IB sanitized by host
Release into inspector custody

Figure 3: Conceptual deployment process: Green fields indicate points in the equipment lifecycle at which inspectors have total freedom to probe data, equipment or records. Red fields represent points at which inspectors have no control of equipment (because it is host-provided) or operations (because they are host-controlled). Orange fields represent equipment and operations that take place under controlled conditions, before any confidence is established. Yellow fields represent operations and equipment that are all jointly-controlled conditions which should be conducted to build confidence. A low security environment will involve restrictions on activities, but may not be subject to such rigid security and safety requirements as more secure facilities. These facilities, in contrast, operate very strict controls, requiring authorisation from safety and security authorities for every process that takes place.

One such general lesson is to identify design requirements for ancillary or supporting equipment early; and to keep those requirements in review so long as the design of the primary equipment is also under review. In the case of the UKNI information barrier, some functions were included for equipment development purposes, to ensure that each IB behaved as expected. This information barrier therefore has the capability to relay all the data collected from an item to a computer connected to a data port in the information barrier, which, if accessed by the inspector, would result in release of that sensitive information. As the project evolved, it became clear that all engineering functions and code, and the data port itself, would need additional protection during deployment and so a strengthened requirement for tamper prevention or indication became apparent. As the UKNI information barrier is a research project, this is not a major problem – but it is a good example of how one aspect of equipment design could potentially have substantial knock-on consequences if authentication and certification considerations are not considered early in the design process.

A second, related example is the potential need for similar protection for the information barrier as a whole. The design of the IB does not include the addition of internal security features to protect data. This was done in order to keep the design simple for certification and authentication purposes. However, one consequence of this is that in a facility emergency situation – which might involve inspectors having to leave the facility without first securing the information barrier – the information barrier would be left vulnerable to tampering by a malicious host. Although designing, building, certifying and validating a tamper prevention or indication solution has not formed part of this project, we note the potential requirement for such a solution under the general deployment circumstances that we have outlined.

Confidence in Results from Verification Measurements

This section of the paper deals with the third issue we identified earlier, that of understanding what verification measurements mean in an operational context. The key facts to bear in mind throughout this discussion are that the operational environment is very different to the laboratory environment, and that verification processes – particularly those that involve measurements of nuclear weapons or weapon components – do not necessarily permit the degree of control or prior knowledge that good practice in experimental design would normally dictate.

Verification-specific challenges

An interesting challenge in developing information barriers is in understanding how the equipment should perform in an operational context. Under 'normal' developmental circumstances, equipment might be tested extensively on its intended target to ensure developers understand how the equipment should perform. It is not possible to do this in the verification scenario because detailed test results from a 'real' nuclear warhead, or TAI, contain the very data to be protected. Testing the accuracy of an information barrier such as the one developed by the UKNI is thus not possible in the traditional sense, at least not by the inspecting party. Operational performance expectations therefore need to be found without revealing classified information to the inspecting party during equipment testing.

The UKNI information barrier is, in common with other radiation measurement technologies, making its output based on statistical analysis of the data that is collected. Because of this, the output of the pass/fail criteria of the information barrier will never be an absolute judgment on the presence or absence of the relevant attribute within a declared Treaty Accountable Item. This is because of the random nature of nuclear emissions. This means there will always be a possibility that a measurement will result in a false positive or a false negative (a false positive is the case where an item passes a test that it should fail; a false negative is the case where an item fails a test that it should pass).

Of course, the inspecting party can test the information barrier against any number of surrogate objects with a range of isotopic ratios, in order to collect data concerning the rate of false positive and false negative results returned by the information barrier in controlled conditions, and this is exactly what the UKNI has done. In 2012, Information Barriers were used in a civil nuclear facility in Dounreay, Scotland, to collect data against surrogate objects. More data has been collected since then, using international standard Plutonium samples. However, the degree of correspondence between the surrogate test items and the real TAI can never be discussed, because this again could lead to some information leakage that the information barrier is trying to prevent. This complicates the inspector's attempts to understand what it really means when an object declared to be a TAI fails an attribute measurement: is it that the object is bogus; or is the measurement a false negative? This situation demonstrates how both parties need to understand when and how attribute measurement equipment can be usefully deployed. It also brings us back to the subject of thresholds that we mentioned earlier.

Threshold setting and equipment performance

As we noted earlier in this paper, verification using attribute measurements involves the agreement of an attribute, or set of attributes, that a TAI has, and the subsequent testing of objects against those attributes. In many cases these attributes will define quantities of interest (a mass greater than a certain amount, for example, or in the case we have here, a Pu-240/Pu-239 ratio below a certain level). The value of this quantity that defines the boundary between objects that are and are not true TAIs is termed the threshold. Naturally the inspecting side will wish to ensure that this threshold is set such that it has a genuine meaning in arms control terms. This might involve looking for a threshold such that relatively few, or perhaps no, items that are not TAIs are able to pass the test. In the case of the UKNI information barrier, this might involve the inspecting side looking to set the threshold as high as possible, on the basis that this reduces the likelihood that non-weapons-suitable could pass the attribute measurement.

Unfortunately, a high threshold could be problematic for the host. The statistics of measurement are such that the closer that the threshold gets to the genuine isotopic composition of the treaty accountable items, the greater the likelihood that a genuine item will fail the attribute measurement. Assuming that the host genuinely intends to carry out the arms control measures it has agreed to, and that it want to comply fully with the verification processes, this high threshold could result in some concern about the possibility of being – wrongly – judged non-compliant. Therefore the host has an interest in ensuring that the threshold is sufficiently far from the actual values of the TAI attributes to reduce the expected false negative rate to an acceptable level.

Equipment performance has a strong part to play in addressing this issue: for equipment that is very capable at discriminating between items with attributes above and below the threshold, the host may be able to tolerate a higher threshold; if the equipment is less capable at distinguishing between objects just above and just below the threshold then this means that the host would be motivated to push the threshold down to avoid excessive false positives. Either way, in order to do this the host will most likely need to carry out additional work to assure themselves that the TAIs produce statistics at least as good as those that the inspector might expect from the controlled tests.

In general, the threshold needs to be agreed between the parties, based upon data obtained in controlled tests. It should be set such that items meeting or exceeding the declared threshold are very likely to pass the test. Under this circumstance, TAIs with an isotopic ratio at or above the declared threshold should very rarely return a negative result against the equipment threshold. The benefit of this is that negative results can be treated as real failures by the inspectors, and further action can be demanded.

Population analysis

It is clear that deploying an attribute measurement information barrier such as the one developed by the UKNI may be of limited value if used only once against an individual object declared to be a TAI. It is not a piece of equipment that can be used to give a yes or no answer when deployed against an unknown object, without understanding more about the context of the measurement., even though it might be a strong indicator. For example, when presented with a population of TAIs, each of which is measured once, the pass rate obtained from the group will look the same in the following two different situations:

1. A homogenous population is presented, such that all items genuinely possess the attributes (perhaps only just above the threshold); and
2. An inhomogeneous group, consisting of a subset of items which possess the attributes at a value *significantly* higher than the threshold, (and so have reduced false negative rates) mixed with another much smaller subset of items that have attributes below the threshold

This would not be straightforward to implement, but this simple example shows how manipulation of population characteristics by a deceitful host could open up the possibility of fooling an inspector into thinking that more weapons had been dismantled than was in fact the case. There are two equally simple counters to this strategy though: highly discriminatory equipment coupled with a high threshold; and repeat testing of items. The first measure would act to limit the number of fake items that could be included in the population without detection, while the second would allow identification of anomalous items (at the cost of an increased verification burden).

This is a complex situation, which will be covered in greater detail in forthcoming publications of UKNI information barrier work. However, the discussion above demonstrates how parties have had to work together to understand the context in which equipment is to be used and the performance characteristics of the equipment.

Performance of the UKNI information barrier

The UKNI has tested the information barrier multiple times against a number of non-military plutonium samples which exhibit isotopic ratios both above and below the 90% Pu-239 threshold chosen for the project. Based on these measurements it appears that the

performance of the information barrier, in terms of its ability to distinguish clearly between objects just above and just below the threshold, is good enough to render the kind of deception strategy outlined in the previous section very challenging.
This means that it could in theory provide additional confidence in the conformance of a population of objects to a declaration, provided confidence in the equipment is built and maintained as outlined earlier in this paper.

Even so, the instrument developed should not be considered as operational, or ready for deployment, but instead as a research tool. It works as intended and has proved to be a project rich in opportunities to learn about design principles for verification equipment, in which mutual confidence needs to be established and maintained. Some of those lessons are outlined in the next section.

Some Lessons on Joint Technology Development

The UKNI information barrier project has been, to some degree, one of trail and error, used to test some concepts that might enable the certification and authentication of inspection equipment. All the requirements and restrictions discussed in the paper have led to a bespoke design (and operating procedure) with a very specific function. This has helped achieve our overall aim.

Perhaps the most important lesson is the necessity of having a good understanding of how inspection equipment is going to fit into a wider verification regime. Designers need to understand the details of how the equipment is to be used, to truly understand the requirements for the design of the equipment and the constraints on it. The first consideration, for inspectors in particular, is to identify the information the inspectors want to get out of their measurement, and where that sits in the wider verification strategy. With an attribute measurement system such as the UKNI information barrier, the simple answer is of course the ability to detect the presence of an agreed nuclear warhead attribute. But since there are limits to the certainty of the measurement, as we have outlined in this paper, this also raises the question of how accurate and unambiguous the results from the measurements have to be. This judgment will depend on the value of these measurement data in the overall verification strategy, which might consist of multiple overlapping verification techniques. Those who design these strategies need to consider what the presence of a certain attribute set would prove at any one point during a verification process. A clear understanding of the purpose of the measurement, in context, is therefore necessary to ensure the equipment is developed appropriately.

A second vitally important consideration is the need for compromise between the measurements one would ideally like to perform and what is actually possible in practice. As we have outlined in this paper, there could well be restrictions on safety or security grounds; there might also be physical constraints on being able to take the measurements at all due to lack of space in the relevant for facility, or limits on the time available to perform a measurement. One of the experiences gained in developing the UKNI information barrier has for instance been that – even if it is possible – authenticating and establishing joint host-inspector custody over inspection equipment can be a very time-consuming activity.

In order to manage the certification and authentication issues we identify in this paper, the UKNI information barrier has been developed as a bespoke piece of equipment. Even though our aim of has been to keep the information barrier as simple as possible in terms of physical hardware, this has not meant that development has been as easy as possible. Software development in particular has been complicated the limited memory size and simple architecture of the chosen micro controller, which meant that all functionality – including all mathematical operations used in data analysis – has been written from new. Similarly, all of this design simplicity does not translate to simplicity in deployment. The procedures needed to authenticate and keep a chain of custody over the authenticated equipment over time would be very laborious, and need to be very detailed to ensure that both parties can keep confidence in the results from the measurements performed.

The final lesson worth highlighting from the UKNI development work may in hindsight seem obvious, but, to develop a piece of equipment to perform a specific task it is preferable to have this task well defined at the start of development. The UKNI information barrier has went through several phases of development,: from detecting the presence of Cobalt-60; through to the detection of a threshold value for the ratio of Cobalt-60 to Sodium-22; and finally arriving at the current detection of plutonium presence and quality. This meant that certain design decisions were taken early on in the project and persisted through the development phases, ultimately compromising certain aspects of the information barrier. The Measurement of a ratio of two Plutonium isotopes is not the same as measuring the ratio of two different materials. Legacy solutions might not have been present if we had aimed our work at plutonium detection from the start. For instance, recent improvements to the isotopic analysis method might have been made much earlier, allowing much more time for research into threshold values. Alternatively, a more powerful microcontroller might have been chosen, or a fully specified tamper indicating enclosure could have been developed.

However, the fact is that the UKNI was not in a position to start development directly towards the current information barrier functionality when the collaboration began in 2007, simply because we were yet to learn the lessons that the project has taught us. Since the UKNI is the first collaboration of its kind, between a NWS and a NNWS, there were also of course uncertainties in the early phases on how to work together and what scope to set for our joint work. The various phases of development were each necessary at their time, even though they have left us with a legacy of some sub-optimal solutions in our current information barrier, and we want to highlight the value to researchers in Norway and the UK of sharing the experience of learning about equipment development for arms control throughout this project.

Overall, the UKNI has demonstrated that it is possible to jointly design verification equipment that can detect the presence of weapons-suitable plutonium, without compromising national security or non-proliferation obligations. We have also outlined the issues that would need to be addressed for the results to be understood and trusted by both parties in an inspection process, and have developed solutions to some of those problems.

Based on our work, we are clear that, in order to successfully design and implement verification technologies, the context and the purpose of the proposed measurement and the whole lifecycle of the equipment should be considered. Hardware, software, and ancillary equipment requirements, as well as authentication requirements, certification constraints and deployment processes all need to be kept under review. Individual design elements should not be finalized until the impacts and consequences for the broader system are understood. Everything is important; and nothing is ready until everything is ready.