Y/DV-1758

A BWXT/Bechtel Enterprise

Y-12 NATIONAL SECURITY COMPLEX

MANAGED BY
BWXT Y-12, L.L.C.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

UCN-13672 (10-00)

ReflectoActive™ Seals for Material Control and Accountability

G. D. Richardson, J. R. Younkin, Z. W. Bell
BWXT Y-12, L.L.C.

To be presented at the:

Institute of Nuclear Materials Management 43rd Annual Meeting
June 23-27, 2002
Renaissance Orlando Resort
Orlando, Florida

June 2002

Prepared by the
Y-12 National Security Complex
P. O. Box 2009, Oak Ridge, Tennessee 37831-8169
managed by
BWXT Y-12, L.L.C.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22800

ReflectoActive ™ Seals for Material Control and Accountability

David Richardson, Jim Younkin, Zane Bell
BWXT Y-12, L.L.C.
Y-12 National Security Complex
Engineering and Technology
Oak Ridge, Tennessee, 37831, USA 865/241-8138

ABSTRACT

The ReflectoActive ™ Seals system, a continuously monitored fiber optic, active seal technology, provides real-time tamper indication for large arrays of storage containers. The system includes a PC running the RFAS software, an Immediate Detection Unit (IDU), an Optical Time Domain Reflectometer (OTDR), links of fiber optic cable, and the methods and devices used to attach the fiber optic cable to the containers. When a breach on any of the attached fiber optic cable loops occurs, the IDU immediately signals the connected computer to control the operations of an OTDR to seek the breach location. The ReflectoActive ™ Seals System can be adapted for various types of container closure designs and implemented in almost any container configuration. This automatic protection of valued assets can significantly decrease the time and money required for surveillance.

The RFAS software is the multi-threaded, client-server application that monitors and controls the components of the system. The software administers the security measures such as a two-person rule as well as continuous event logging. Additionally the software's architecture provides a secure method by which local or remote clients monitor the system and perform administrative tasks. These features provide the user with a robust system to meet today's material control and accountability needs.

A brief overview of the hardware, and different hardware configurations will be given. The architecture of the system software, and its benefits will then be discussed. Finally, the features to be implemented in future versions of the system will be presented.

INTRODUCTION

The need to ensure that special nuclear materials are safe and secure is not a new one. For this purpose there have been many tamper indicating devices (TID) that have come into use. These TIDs are designed to show that containers have not been unknowingly accessed. This is determined by performing a random inventory on a selection of containers. This method has proved effective, but with the technologies available today there are better options.

An active seal is a TID that is constantly monitored. The seal is attached to a container in such a way that it would have to be opened to open the container. Few systems employing active seals have been deployed, in large part due to their cost. The most obvious advantage with an active seal system is that, should any of the seals be tampered with the system custodian will know immediately. This allows a person to say with certainty that the material is safe and secure. Materials monitored by active seals system may qualify for inventory extensions. That is, the period at which the material must be verified is increased. Inventory extensions bring with it significant cost savings, which provides one of the best arguments for active seals. Installation of a single system might be more expensive than one or even five individual inventories, but an active seals system will pay for itself many times over during its lifetime. Increased periods between inventories also provide a health benefit, in that workers are not exposed to hazardous materials as often.

REFLECTOACTIVE ^{TM} SEALS

The ReflectoActive ^{TM} Seals system is a fiber optics based active seal technology. It is an adaptable system that provides monitoring for large storage arrays. The system software provides a material custodian the ability to monitor and to account for material access. The system is capable of monitoring 1500 + seals due to its fiber optic technology. This is all done at a relatively low cost per seal, as the hardware merely requires loops of fiber optic cable and an inexpensive attachment mechanism. The system consists of several pieces of hardware. Some of which are custom made as well as some commercial off the shelf hardware. The system consists a PC, an alarm box, a UPS, and must contain an Immediate Detection Unit (IDU) and/or an Optical Time Domain Reflectometer (OTDR).

The PC requirements to run the client and server software are fairly minimal. The client and server can be run on the same machine or on separate machines according to the particular installation's needs. A recommended configuration would be a Pentium III system with 128 MB of memory, running Windows 2000 Professional for a system running the server software. Windows NT 4.0 Sp 6a is also a viable option. The server will run on a Windows 9x/ME platform, but due to the inherent insecurity of these operating systems, those platforms are not recommended. The client software is capable of running on a Pentium class machine with 32 MB of memory.

The Immediate Detection Unit, or IDU, is a custom designed piece of hardware. Inside there are ten Link cards. These cards when connected to a loop of fiber can immediately detect when the fiber has in some way been breached. When a PC is present, the IDU passes the event on to the PC via a data-acquisition board and continues to monitor for other events. The IDU can also operate in stand-alone mode, if no PC is present, it will set off an attached alarm when a breach occurs. In some configurations the IDU also includes a fiber optic switch. This fiber optic switch allows the system to leverage the ability of the OTDR to find where a breach occurs.

The Optical Time Domain Reflectometer, or OTDR, is a commercial off the shelf piece of hardware. The purpose of the OTDR is to detect precisely where a breach has occurred on a given length of fiber. The OTDR does this by sending pulses of laser light down a strand of fiber optic cable. When the pulse goes through a connector, or seal, a small amount of the original laser pulse is reflected back to the OTDR. By calculating how long it took for this return pulse to get back, the OTDR can calculate how far away the reflection occurred. This data can then be viewed as a plot on the OTDR. In this way it is possible to precisely locate every seal on a loop of fiber. By looking down both ends of the fiber it is therefore possible to determine which seals may have been compromised and which seals that are still secure.

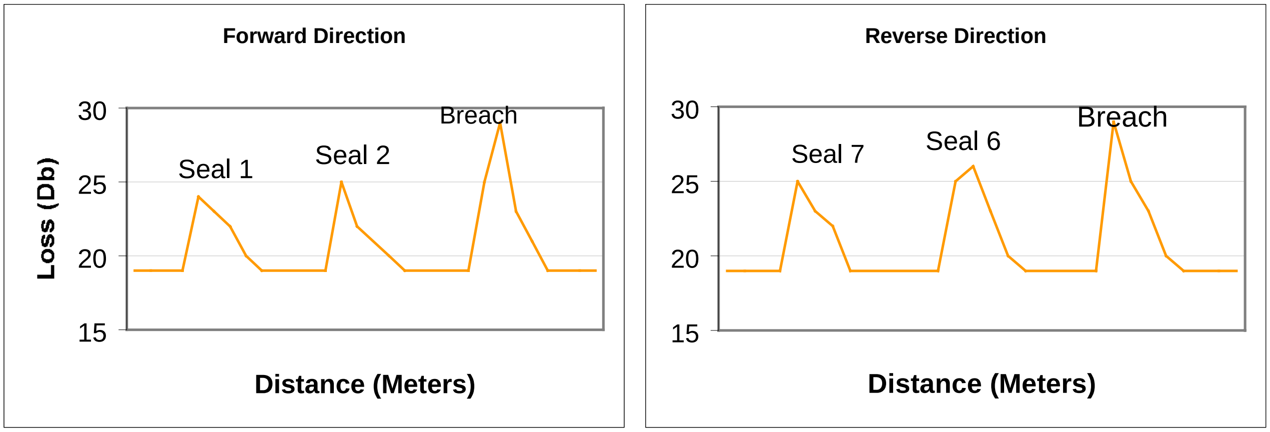

Figure 1 – Examples Of OTDR Plot (Seals 4 and 5 not secure)

Other hardware needed by the system includes a UPS and a custom designed alarm box. The UPS is designed to hold the system up in the event of a power outage. Should the power outage bring the system down, the UPS will have had time to log the power outage so that it does not go un-noticed. The alarm box controls both an audible and visible alarm. These alarms can be set in the event that a loop of fiber is breached. Both the PC and the IDU have the ability to set the alarms off, although as long as the PC is running it will take precedence. The alarms can only be acknowledged via the ReflectoActive ™ Seals Software.

SYSTEM CONFIGURATIONS

The ReflectoActive ™ Seals System can be configured differently depending upon the number of items that need to be monitored.

The OTDR only system is designed for a smaller number of containers. The OTDR system can only monitor one strand of fiber optic cable at a time. For this reason, it is not an ideal system for monitoring many containers, or for monitoring containers in different locations.

Conversely, it is possible to have a system that only contains an IDU. This allows for up to ten loops of fiber to be connected and monitored. Such an arrangement allows large numbers of containers to be monitored in different locations simultaneously. Fiber can be run from the IDU up to a few kilometers away to monitor if necessary. The downside to this configuration is that the IDU can only detect that there has been a breach on a loop of fiber. It cannot detect where the breach occurred. This solution is best geared towards static storage, where there will be very little need to access material.

The full implementation of this system contains both an IDU and an OTDR. This configuration adds a fiber optic switch into the housing of the IDU so that the OTDR can be integrated into the system. The fiber optic switch allows the OTDR to look down any one of the ten loops of fiber that are connected to the IDU in either direction. This is accomplished by wavelength division multiplexing. The frequency of the light transmitted by the OTDR and the IDU are different. The switch changes channels to the specified link. Hardware on the Link cards can then inject these two different wavelengths of light down the same strand of fiber. As soon as a breach occurs on any of the loops of fiber, the OTDR signal is injected into that loop of fiber. The OTDR can then verify which seals are secure and determine which seals may have been compromised by the breach. This configuration provides the most robust solution for large storage arrays.

Figure 2 – ReflectoActive ™ Seals Hardware

SOFTWARE DESIGN

The ReflectoActive ™ Seals System software design had several key roles to fulfill. One of these roles was the extensive application of business rules. Material access needs to be controlled administratively, and when material is accessed an event log needs to be generated. There was also a need for different classes of users. Certain users should merely be able to ascertain the system status, while others should be allowed to configure the system. Other rules, such as the two-person rule for accessing material, also needed to be implemented. Due to the reporting needs and the extensive business logic the need for a solid user-interface was apparent. The nature of the system also provided some argument for having at least limited access to the system across a private network. The end result was a DCOM client/server application written in Visual Basic, running on top of a Microsoft Access database.

SERVER SOFTWARE

The ReflectoActive ™ Seals Server software is the heart of the system. This piece of the software controls all the business logic, as well as directly talking to the system hardware. The client/server paradigm makes a lot of sense for this particular application. Especially since the software is designed so that authorized users are held accountable for their actions. The server software is set up to run as a system service. This ensures that the server will be monitoring the system as long as the PC is running. Should for some unforeseen reason the system go down, the IDU could still detect breaches until the PC is rebooted. An overview of the hardware interaction, and client to server interaction will be discussed.

The system service, once started, will begin to talk to the IDU via a National Instruments Digital I/O board. It determines if there has been a breach since the last time it polled the hardware. At this point, the server instructs the OTDR to begin acquiring a characteristic waveform for each of the ten links on the IDU. The server will compare these waveforms to a reference, stored in the database, and determine if there have been any changes from the values that were determined when the system was configured. When the server process detects some change in the system or hardware configuration it immediately logs it and fires off the appropriate event. The client only receives events when there is a change in the physical system. This is done to reduce network and inter-process traffic, as well as to reduce the system requirements for the client software.

The server software responds to requests from a client only when they have successfully logged on. Since this is a DCOM server, any number of clients can connect over a network connection. In practice, system administrators configure the number of permitted client connections based on operational needs. Once a client has logged on, only specific portions of the system software are made accessible to the user. This is critical to ensure that the user cannot circumvent the system. Another important feature is that the client connects through an intermediary object. The client instantiates a copy of this interface and all requests go through it. This intermediary interface has a unique identifier and is referenced by both the client and the server. If necessary the server can terminate the intermediary and cut the client off from the server process. This behavior provides a buffer between the user and server software.

The system state is also maintained in an encrypted Microsoft Access database. The server is the only process with direct control over the database. Limiting database access the server process ensures that all events are logged, and prevents clients from altering system events or configuration information. Every event generated by the system or by the user is logged here. This provides the system with an unalterable history and allows accurate reports to be generated. Reporting is handled via Crystal Reports and allows the user to discriminate somewhat, as to what types of events they wish to see.

CLIENT SOFTWARE

The ReflectoActive ™ Seals client is a lightweight client that provides a user the ability to interact with the seals system. The client can connect to the server software via DCOM on the same machine or via a private network. The client is instrumental in that it allows the events generated by the server software to be reviewed. Client features include the ability to add and remove items from a seal, as well as the ability to acknowledge when a breach has occurred. The client can also view the waveform for any of the ten links. The user can then compare the current waveform against the original reference waveform to look for any anomalies. The client provides the user the ability to interact with and monitor the server software.

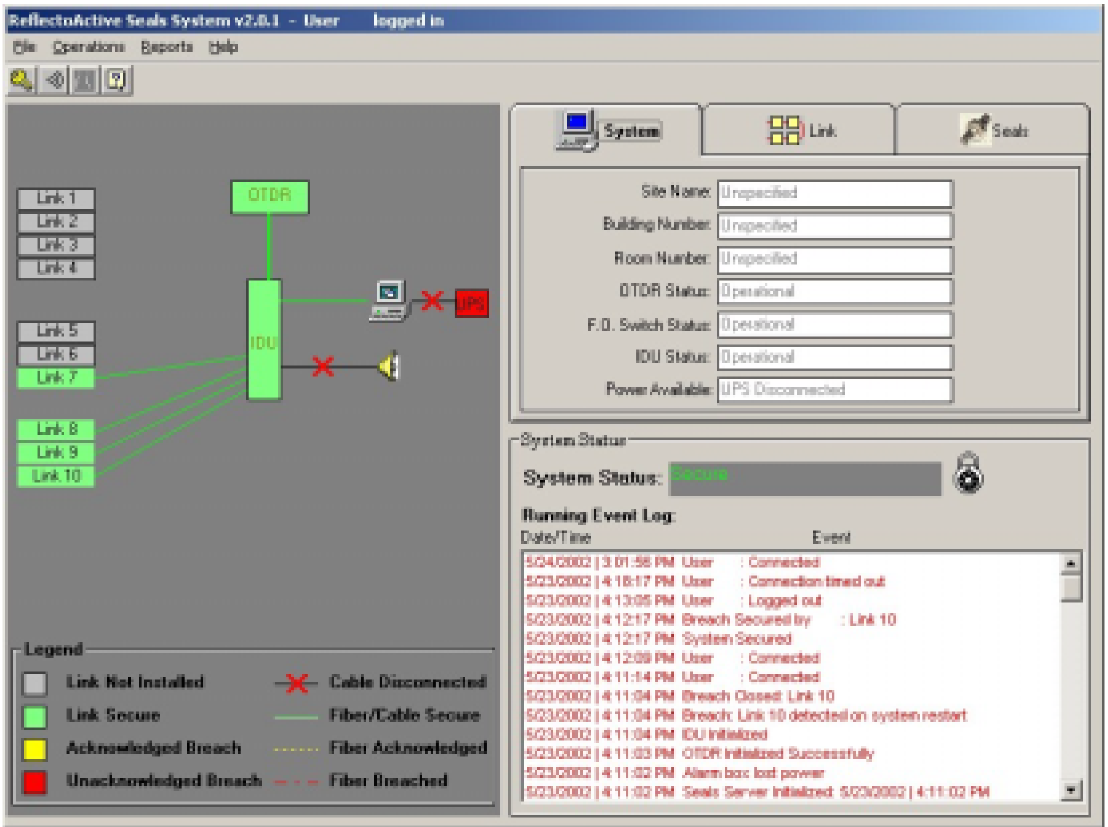

Figure 3 – ReflectoActive ™ Seals User Interface

CLIENT/SERVER ARCHITECTURE

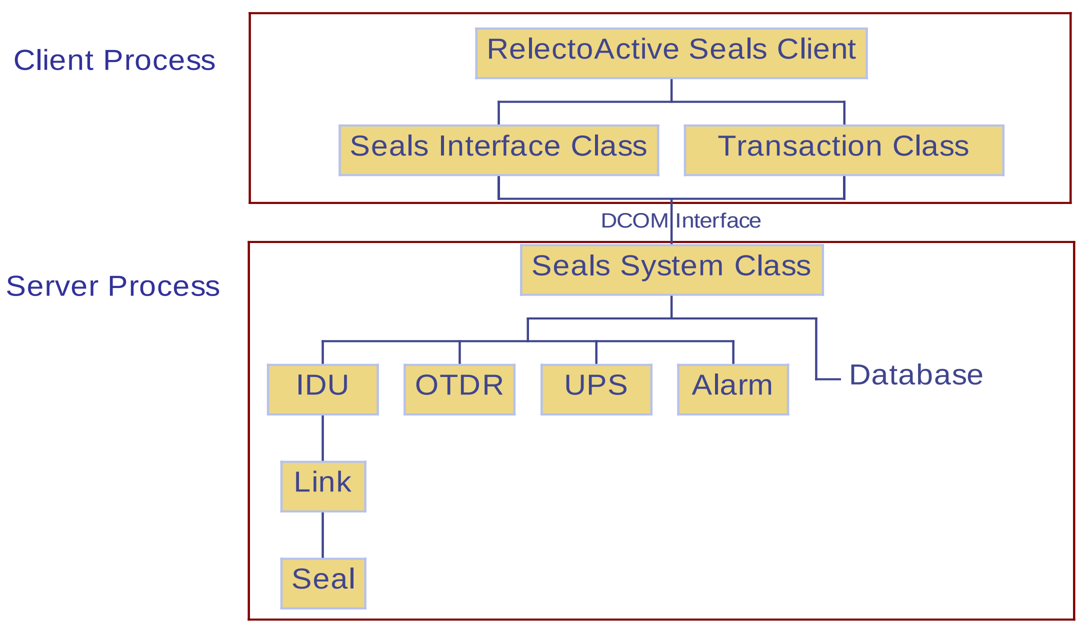

Figure 4 - Client Server Architechture

The architecture illustrated in figure 4 provides a picture of what the ReflectoActive ™ Seals software architecture looks like. Each box represents a class that can be instantiated at run-time. Once the system configuration is loaded from the database, a class is instantiated for each object in the system. This is an object-oriented architecture, which inherently has several advantages. The first is that the code is extremely modular. Should the hardware change, the code that controls that hardware is easily modified without breaking the rest of the system. Another important advantage of an object-oriented design is encapsulation. Not all of the methods are exposed to the user; only the properties and methods that have been determined necessary to operate the system are allowed. Finally, this structure is more easily understood. The layout of the software represents the physical layout of the hardware, making the code easier to understand, and more maintainable.

The system uses DCOM to facilitate communication between the client and the server. The Seals Interface class and Transaction class are defined on the server machine, to connect to the system, the client requests a copy of those objects. Therefore, theoretically any program that can use DCOM can also become a ReflectoActive ™ Seals client. This allows for multiple clients with different levels of functionality to connect to the system. For instance, a touch screen panel might be placed on the outside of a vault. A client could then be written that would allow a user of the touch screen to add and remove items out in the facility. A fully functional client could be located on the server machine. Another advantage of using DCOM client/server architecture is that the system can leverage the different security features DCOM has. By using DCOM security, the system owner can specify which users can access the software, as well as specify if they want the data to be sent encrypted.

FUTURE SYSTEM ENHANCEMENTS

The ReflectoActive ™ Seals system is very capable of doing its job well but as technology improves so can the system. One feature of particular interest is a biometric authentication technique. Several technologies have been investigated and hardware based on fingerprint recognition has been purchased for testing with the system. Biometric technologies afford an even better form of authentication and allow the system to verify that the user matches the credentials he provides. Another advancement of particular interest would be a more “plug and play “ type addition of links. Currently each link has to be manually configured. While the current method is done with relative ease, auto-detection of each individual link would be desirable. This may be possible by performing some waveform analysis on each link. Work has also begun on implementing XML reporting. This new reporting method will allow for more in-depth queries of the event database, as well as providing a reporting solution that doesn’t rely on third party software. Finally, a sensor network concept is being pursued. Each individual seals system at an installation is to report back to a central authority. A conceptual drawing of such a system can be seen in figure 5.

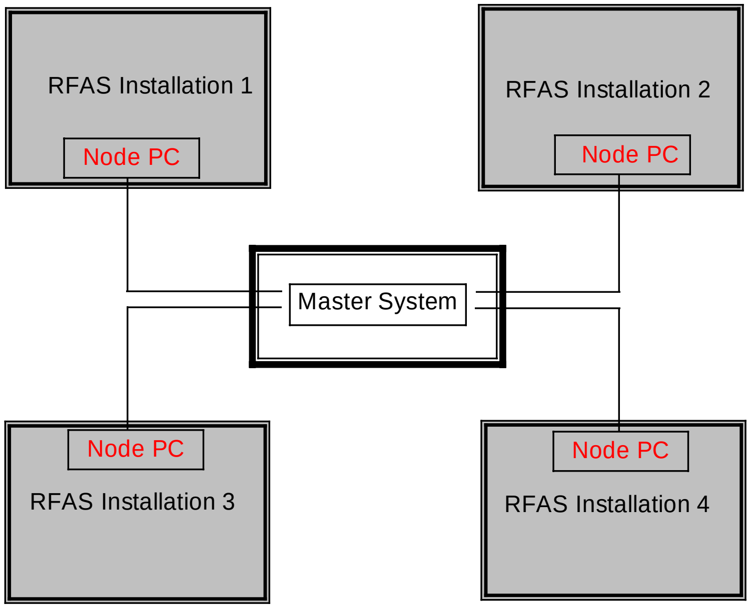

Figure 5. – Seals Sensor Network

SUMMARY

The ReflectoActive ™ Seals System is an active seal technology designed to monitor Special Nuclear Materials. It can bring active seals technology to a large number of varied containers. This provides health benefits for the workers and financial benefits for the custodian due to increased inventory periods. More importantly, the system ensures that these materials are safe, secure, and accounted for.

ACKNOWLEDGEMENTS

The authors would like to acknowledge SO-13, The Department Of Energy Office of Policy, Integration, and Technical Support, for providing funding for this effort.

"Automated Systems for Safeguarding and Accountancy of Stored Highly Enriched Uranium (HEU)," by C.A. Pickett, Z.W. Bell, T.W. Dews, et al., 1998, presented at the American Nuclear Society Third Topical Meeting, September 8-11, in Charleston, SC

"Automated Systems for Safeguarding and Accountancy of Stored Nuclear Materials," by C.A. Pickett, K.M. Baldwin, Z.W. Bell, et al., 1999, presented at the European Safeguards Research and Development Association (ESARDA) 21st Annual Meeting on Safeguards and Nuclear Material Management in Sevilla, Spain

Distribution:

Z. W. Bell
G. D. Richardson
J. R. Younkin
Y-12 Central Files