2nd International Technical Meeting on Small Reactors
Ottawa, Ontario, Canada, 2012 November 7-9

Challenges for Remote Monitoring and Control of Small Reactors

Dave Trask
traskd@aecl.ca
Atomic Energy of Canada Limited
Fredericton, New Brunswick, Canada

ABSTRACT – This paper considers a model for small, unmanned, remotely located reactors and discusses the ensuing cyber security and operational challenges for monitoring and control and how these challenges might be overcome through some of AECL's research initiatives and experience.

1. Introduction

A quick investigation into suitable applications for small reactors reveals a considerable demand from Mars to the Canadian North, powering colonies, communities, mining operations, remote research stations and military applications.

This paper considers an application where it would be reasonable to assume that small reactors used in remote applications, where it would be impractical, unnecessary, and too costly to have permanent personnel on-site, could be licensed for autonomous/unattended operation.

So how can the public and licensors be convinced that remote autonomous/unattended nuclear reactors can be safely and securely operated?

It can be done! The first step is getting a license for any unattended nuclear facility and this was achieved by the Compact 20-kWt SLOWPOKE-2 (Safe LOW POwer k-ritical Experiment) tank-in-pool research reactors built between 1971 and 1985. These units are licensed for unattended operation for up to 24 h. They have no safety-related programmable electronic automation systems and can only be manually controlled locally.

In contrast, commercial operations where remote startup/shutdown, remote control, or where reactors are physically inaccessible for long periods of time, will rely on programmable electronic systems providing automation and monitoring capabilities inside the facility while using additional, independent programmable systems to communicate beyond the facility's walls.

As such the operation of the reactor will be directly impacted by the design, reliability and security of the programmable electronic systems. The good news is that technical solutions for remote monitoring and control are already commonplace in industry: in the oil and gas sector, power and energy, manufacturing, aircraft, missiles, space exploration and satellite industries. The bad news is that these systems are under cyber attack every day and in the nuclear industry,

even the perception of the possibility of an accident onshore or offshore can receive worldwide attention and negatively impact the industry as a whole.

It's not all bad news though, since these mission critical remote operations are successfully and securely controlled every day. The nuclear industry can learn from these applications, and directly benefit from broader industry research and experience. In addition, this paper discusses AECL's research and experience with several aspects of secure remote control and monitoring that could also contribute to more robust solutions in the future. This includes a form of biometrics and anomaly detection for remote data authentication, realtime operating system extensions for tracking, monitoring and blocking process activities, a uni-directional gateway solution for protection against cyber attacks while allowing secure remote monitoring, and recent realtime, system based, monitoring for anomaly detection in AECL's plant display system software.

Biometrics – a process that uniquely identifies field instrumentation "signatures" based on the noise or "vital signs" that are unique, predicable, and measurable relative to the instruments physical connections and location in the plant. By multiplexing the "signature" with the process data, remote operators can be assured that the data is authentic, has not been tampered with and that it is coming from a specific instrument connected to a specific process in a specific location. "Active Biometrics" is the addition of a random stimulus in the field to elicit a known signal response, which can be incorporated into process data, to protect against playback spoofs. This process can be reversed to program instruments to only accept commands from authentic sources as well.

Biomarkers[1] – investigating the value proposition of using "Biomarkers" to enhance security and safety of critical software systems. "Biomarkers" are extensions to a mircokernel-based operating system, such as QNX, and are used to "tag" inter-process interactions and then use those "tags" to track, block, and measure process operations.

Anomaly Detection – authenticating remote realtime operational data through process analysis looking for variants in the known or expected characteristics of an operating plant as a whole. This process considers that all aspects of a plant are interconnected and predictable for any plant state from water treatment, to instrument air, to plant noise, to room temperatures all the way out to generator output and grid state. For example, if the turbine speed or power output were being spoofed or tampered with then other plant process data could flag the anomalies since almost everything from plant power consumption, to cooling water flow, to outlet temperature, etc. throughout the plant must correlate with the reading.

AECL has also recently employed another form of anomaly detection on their Advanced Control Center Information System (ACCIS) that monitors itself in realtime for variants in communication, file integrity, and process integrity. Unlike an office computer system, a plant display or control system is very predictable and operates in a relatively steady state making it an ideal platform for anomaly detection. In these systems the number, size and images of the files on the disk are known and should not change as are the number and sizes of the processes running at any given time. Communications are typically restricted by safety and security zones and the data being sent is predictable in size, format, and frequency from source to destination.

AECL is continuing to investigate other areas and applications for anomaly detection since it is more robust and reliable for determining if a computer system has been compromised than traditional antivirus software given that:

- There are now too many malware signatures and variations to perform realtime signature comparisons on every piece of software
- Signature detection is ineffective against targeted attacks
- Antivirus software can introduce its own vulnerabilities

Uni-Directional Gateway – supports safe, non-interfering, realtime, process monitoring between safety or security zones or from points external to an operating plant by employing unidirectional communication that, due to the physical nature of the communication medium, renders it impossible for any access from the outside. The combination of safety certified OS and in-house developed software will support safe, secure, realtime remote monitoring.

2. Conclusions

This paper accepted the premise that there is a market, a business case and good environmental justification for small reactors, if not only to provide sustainable economic and social development of Canada's North with stable, secure, low-cost and environmentally responsible energy. It also accepts the premise that for these reactors to be economically feasible and publicly acceptable that they would likely be located in remote areas and would be essentially unmanned.

Given these assumptions, this paper considered some of the technical challenges for secure, remote, autonomous/unattended small reactor operation.

Threats to a small autonomous/unattended reactor can originate from anywhere, by anyone at anytime, whether from poor design, backdoors, poor maintenance, networks, counterfeit hardware, 3rd party software, physical damage, sabotage or even simple equipment failures.

However, the nuclear industry has the immediate benefit of tools, techniques and experience both inside and outside the industry, conducting mission critical operations using various forms of automation and remote communication for command and control. This technology is commonplace in industry and complements the rigorous nuclear standards for quality, safety and security and is the evidence that a licensable autonomous/unattended reactor is achievable.

As in any industry, new technologies present new challenges and AECL, like others, are continually providing research, tools, and techniques to benefit from them.

3. References

[1] Oliveira, A., A. Saif Ur Rehman, and S. Fischmeister, "mTags:Augmenting Microkernel Messages with Lightweight Metadata", ACM Operating Systems Review, 2012.