
Nuclear Plant Journal

*An International Publication
Published in the United States*

Outage Management & Health Physics

Safe and Secure Operation

By Richard Rosano and Mark Satorius, EXCEL Services Corporation.

*A reprint from the May-June 2017 issue of Nuclear Plant
Journal.*

May-June, 2017 Volume 35 No. 3

Bruce, Canada

ISSN: 0892-2055

Safe and Secure Operation

By Richard Rosano and Mark Satorius, EXCEL Services Corporation.

Richard Rosano

Dick Rosano is EXCEL Services' Senior Vice President of Critical Infrastructure Protection and has more than 40 years of experience in the field. His career includes service in senior management positions at the NRC over the span of 32 years, including Chief, Nuclear Reactor Security and senior security advisor to three NRC Chairmen. Specific ongoing projects include consulting services in NRC licensing, risk assessment, security plan development, cyber security risk assessment, force-on-force preparation, facility security assessments (e.g., blast analysis) critical infrastructure protection, and testing of security programs.



Following Federal service, Mr. Rosano has spent more than 10 years as a consultant and manager of regulatory programs for the nuclear industry.

He has a Bachelor's in Criminology from the University of Maryland.

An interview by Newal Agnihotri, Editor of Nuclear Plant Journal, on March 16, 2017 at the U.S. NRC Regulatory Information Conference in North Bethesda, Maryland.

1. *Do nuclear facilities rely on wireless systems? And, if they do, are some or all of these systems vulnerable to cyber threat?*

Richard Rosano: First of all, few systems in the nuclear facility are truly wireless and before wireless transmission is chosen, the system's attributes and role in safe operation are fully considered. To answer your second question, to interfere with the wired transmission, you have to get somewhere near that system to attack it directly and introduce a defeat signal.

With a wireless system, on the other hand, you can introduce defeat signals through a variety of capture methodologies. There's electronic capture, and jamming systems. To jam a wireless signal, proximity to the system is not always necessary; you could set up a jammer from the highway outside the plant and interfere with wireless signals. Many digital systems are going wireless to keep pace with technological developments; so with the added vulnerability these new systems must incorporate encoders and decoders at each of the nodes so that any interruption in the system will be detected and defeated.

2. *Is cyber security safety related?*

Rosano: It depends on what system it serves. Systems that relate to administration, human resources, even budget and finance pose a risk for the employer, but are not safety-related, so cyber attacks on these systems would be a net loss for the company but not directly impact safe operation. The way to find out if the cyber component is safety related is to assess whether the system it supports is safety-related, and if a defeat of the cyber component can contribute to loss of safety.

There are three ways that an adversary would want to use cyber to attack a plant. The first way is to take down the communication system for monitoring and managing operational systems. That's a safety problem. Interfering with the flow of information in the operational system could prevent the plant from maintaining safe conditions

The second way is instead of taking down communications, the adversary can introduce false or misleading information so that the operators themselves take the wrong action. That, too, is a safety vulnerability.

The third way is to attack the security system, to bring it down so that an overt attack on the plant is made easier because the security system can't work.

The first two are direct attacks on the safe operation of the plant. The third attack can facilitate a land-based adversary attack by bringing down the security system. Security is safety related because security supports safe operation, but a lot of the embedded regulatory standards for what are called safety-related systems, those standards of performance, those standards of even redundancy don't always apply to all of the security systems, because it's handled in a different part of the regulations.

Mark Satorius: Not all reactor systems that are monitored or controlled by wireless digital controls are needed for safety, that is, to safely shut down the reactor, and keep it cool. From that perspective, if you have a wireless digital control system that is either taking measurements on a system necessary for safe operation of the plant, or that is causing that system to respond, such as by opening or closing valves or by causing the system to start safety-related equipment, that would be safety related. There are other components, for example, the turbine generator that generates the electricity. A lot of times, it has digital controls that can be wireless, but those are not really safety related. You don't need the turbine to be able to safely shut down the reactor and keep it cool.

3. *Are the cyber security consultants licensed or certified?*

Rosano: There is a regulation 10 CFR 73.54. That has to do with cyber security and cyber protections for the plant. So, cyber security and cyber vulnerabilities are actually quite heavily regulated now, for the plants.

But no, the people who are offering their cyber services to this industry are no more licensed or certified than anyone else who hangs out a shingle and suggests that they're a cyber expert.

In the entire Title 10 of the code, there's only one category of employees who are licensed, and that's the plant operators. All of the others, the engineers, the maintenance people, the supervisors, security guards, none of them are licensed.

The people who have actual experience in cyber security, those who have either worked in the cyber program of the NRC, designed the cyber program at the plants, they're obviously more marketable and more likely to get the next job. It could be through the free marketplace and survival of the fittest that these are the ones who get the most work.

4. *What formal education is needed to be a cyber security consultant?*

Rosano: Throughout the United States and certain other countries that I'm familiar with, there are university degrees in computer science. When we say cyber security, we're really talking about marrying one discipline, computer science, with critical thinking about how an adversary might deploy cyber systems to carry out an attack on a facility, through a direct attack on those systems. So, cyber security is really just a field of study within the area of computer science. There are a lot of programs that award varying levels of degrees, bachelors and up, in computer science. These are probably the people who will lead this cyber security effort going forward.

5. *How can robots help the plants reduce radiation dose?*

Satorius: There have been robots of one sort or another for many years. They've been used especially in high

dose areas. Say for example, a leak develops in the reactor coolant system while the plant is operating. Operators know that there is a leak somewhere in the containment building because they see the humidity levels go up because reactor coolant would flash to steam, resulting in an increase of humidity. Because there are NRC requirements to immediately shut down the reactor if any leaks from the reactor coolant system are detected, the operators need to know where the leak is from in order to determine if a plant shutdown is necessary. Often

these leaks are in difficult areas to access, or in high heat, or high radiation environments. As a result, operators will often use robots to gain access to areas to determine the source of the leakage and not put a worker in dangerous environments. In many cases, these robots can keep radiation doses As Low As Reasonably Achievable, or ALARA, to find these leaks, so there's less overall dose that's received by workers. Even a dose that would be below regulatory requirements is still a dose and should be avoided, if there are other methods to look for and find leakage in operating systems.

That's the primary use for robots, that is to be able to monitor or inspect inaccessible places, whether due to heat or water or radiation or whatever. You can send these robots in there. Police use them a lot, too, for standoffs with individuals, so that they can send these robots in to do various things. You would be surprised, some of the things that they can do, and you aren't putting a person's life at stake by having a criminal that's in a house, barricaded. You can use robots when there are suspicious-looking bags or parcels that have been left in airports or in other busy places. The police will use

Mark Satorius

Mr. Satorius is EXCEL Services' Senior Vice President of Executive Performance



Solutions. Prior to joining EXCEL, he spent 26 years at the U.S. Nuclear Regulatory Commission (NRC), where he served in several senior leadership positions, including the Executive Director for Operations (EDO). As the EDO, Mr. Satorius was the chief operating officer of the Commission, and was authorized and directed to discharge all the operational

and administrative functions necessary for the day-to-day operations of the agency.

Mr. Satorius has testified before Congressional Committees and at NRC Commission Meetings on topics such as safety and security issues at licensed nuclear facilities. Since retiring from the NRC, he has been appointed to the United Arab Emirates International Advisory Group where he provides safety and security insights to the Emirate Regulator as they prepare to transition their first nuclear power plant from construction to operations.

He has a Bachelor's in Mechanical Engineering from the US Naval Academy.

them to get close so that they can make a determination whether it's a danger to people or not.

High-level waste management is another area that would have high dose rates as a result of spent fuel that's non-shielded. You get tremendous amounts of radiation from used fuel assemblies if they're not underwater and if they're not properly shielded. If you have an

accident with one, if you dropped one of the carriers or dropped a fuel bundle in the spent fuel building, you can use robots to approach that and assist in recovering without having to give people a high level of radiation dose.

There is also work you have to perform when you get inside the bowls of steam generators, to perform eddy current inspections in the steam generators tubes to assure integrity of the tubes. There are certain indexing machines that they have to put into play. They index over and will send a device up the tubes and perform their testing. Maybe not a robot in the conventional way of thinking, but they are robotic. In other words, they're machines that can be made to do what a human usually does. It may not look like a robot, and it may not even have mobility, but they are robotic-type applications.

6. *Concluding comments.*

Satorius: As former NRC employees, we can still have the same values and the same integrity that we had as regulators as we perform consulting activities for our former licensees.

And by helping licensees do things right, we're really still doing our life's work of making sure, radioactive materials are used in a safe manner. We're just applying it a little bit differently. I think that's one of the things you'll see with just about every former NRC person that has decided to do work with helping licensees. One of the things that EXCEL, with Donald's leadership has decided to do, and I think he probably reiterated this several times, but he has had consultants working for him, very, very capable consultants, for almost 32 years. They do great work with what I call implementation-type activities. That's doing license amendment preparations, advice on how to put license amendments together, installing improved tech specs, which allow the plant to operate a little

bit more smoothly because they get more time to work on certain tasks and take certain components out of service for periods of time to repair them or to maintain them, so they'll be more reliable. His company has been doing what's called a 24-month fuel cycle extension. What that means is that they put in reactor fuel that you can operate the plant for 24 months before you have to refuel it. A lot of BWRs are already on a 24-month cycle, but many plants, especially PWRs, are on an 18-month cycle.

Initially, back when it first started up, they were on a 12-month fuel cycle. There's more research done with fuel, so you can have fuel that will last longer in the core. He's had well over 100 individuals working for him for years just doing those type of nuclear activities, that enable licensees to be more efficient, and in all cases, to maintain the safety of the plant or improve the safety of the plant. Just recently, I came on board and Donald has asked me to put together a team of higher level, experienced, former NRC executives. We've put together a team of about 16 or 17.

Rosano: Again, thank you for the opportunity to talk about this because it's important for us to be able to converse on the subject or summarize what we've spent our lives working on. What I believe EXCEL is doing is bringing to an already successful business a new line of people who worked as regulators over decades. I've spoken to a number of industry people and a number of NRC colleagues that I still communicate with; we've worked on different sides of regulated affairs for years, but when it comes to safety we've always been on the same team. In the past, while we were still with the NRC, we, as regulators, had a job to do. Those who run the plant, they had a job to do. But the roles of the

regulator and the industry are married in the goal of providing safe production of nuclear energy.

In closing, I'd say that the nuclear industry worldwide has a unique opportunity during this period of time in which, with all of the older plants that we have, the traditional, large footprint, above-ground plants, we're also about to embark on many new technologies, including small modular reactors and a variety of designs not based on the traditional styles. In security, we have for too long been stuck with technologies of the 1970s. The first answer is too often "get a guy with a gun" and protect the plant. Now that we are building new nuclear facilities, it's an opportunity for us to find a moment to break from the old traditions that we, frankly, should have outgrown by now, and we should start to look at future and more advanced ways of dealing with security. Weaponized robotics could be a big part of protecting a plant. Drones can be used for surveillance. We can use drones instead of static cameras. We can use a variety of different mobile assets that are more than just a guard walking the beat. We can use super-smart cameras that have the ability to track and predict the movements of people. There are so many advanced technologies and systems. This is our chance to do it. We at EXCEL are leading the effort to apply the new systems to the new plants.

Contact: Richard Rosano and Mark Satorius, EXCEL Services Corporation, 11921 Rockville Pike, Suite 100, Rockville, MD 20852, telephone: (301) 984-4400, email: Richard.Rosano@excelservices.com, Mark.Satorius@excelservices.com. ■