DMR for Electric Utilities Roundtable

Theme Four: How will DMR Serve Utility Security Objectives?

Recorded in Tucson, Arizona - May 2012

How Will DMR Serve Utility Security Objectives?

The DMR for Electric Utilities Roundtable was a moderated open discussion. Several themes reoccurred through the day. This transcript pulls together the phases of the discussion that centered on the theme, “How Will DMR Serve Utility Security Objectives?”

Member: What happened was this big release of money into the infrastructure created a demand for products, such as smart meters, different RTUs, different IP-enabled devices that all of a sudden that really didn't have a chance to go through a proper cyber security checks. So the worst nightmare that Department of Energy had was: okay, now we are funding installations that could actually be the demise of the grid, because we are operating too fast to deploy technology that we don't quite understand how to secure yet. So that is kind of where we are today is that we are forging new ground in the U.S., trying to build this Smart Grid that we don't know what it is going to be yet. We want to make sure that each little piece interoperates with each other in a way that is secure and not -- that is not going to cause further reliability issues. Because the old model, it was quite -- you know, you knew where your perimeters were.

Moderator: They were centralized, which is easier.

Member: Yeah. You had: power generation is ‘this’, there are firewalls, I know how to secure this plant. Transmission at a high voltage level. Here's the firewall. This is contained. And distribution was a totally separate system. So now when you are talking about a Smart Grid and a home meter AMI infrastructure that can communicate with energy control centers which communicates with weather systems, which also communicates with marketing building, which Internet portals, which also communicates to low generation systems. Now you are breaking that hardened perimeters and creating this ubiquitous system that if you are not careful could create additional vulnerabilities in the process.

Member: A lot of smart meters, like the ones we deployed, have the remote disconnect. And so you really want to make sure you have a secure connection so that somebody doesn't maliciously start shutting off, you know, all these people, all your customers power.

Moderator: We will be getting into the security aspects. But, you know, the interesting point here is that this seems to be another juncture at which you want to say, well, what is our strategy for managing this whole thing? I mean, all of the IP connectivity allows for the possibility of things managing themselves more towards the edge of the network and being more dynamic and talk. You just plug stuff in. It says, “hi, I'm such and such a device with this IP address, and I'm part of this group here, and we will manage ourselves”. But on the other hand, as a utility manager, you've lost a bit of control. But if you insist on centralizing the control, you run out of bandwidth. And if you add security, that puts more load on the bandwidth. So where does the utility go? What is the feeling? Are we still going to want centralized management? If so, what or are we going to go only distributed.

Member: You need to be a little careful, because it is not an either/or.

Member: No.

Member: And it is not an "everything has to talk to everything", and you have to break perimeters. It is a careful set of deliberate steps about what you are going to do and what you are not going to do. So, for instance, there is a big project on home area networks where, yes, it is a very decentralized sort of a thing. But nothing is allowed to join if the IP address and the MAC address aren't on a verified list from the manufacturer. And so you are just not allowed in if a central location doesn't already have from the manufacturer the appropriate MAC address information, and so on and so forth, and that has to be verified. Once that is verified, you are allowed to be a part of the network, but the firewall and meter says, nothing from inside of that home area network goes further up the utility communications network. So I will broadcast into the home, and I will take actions to say, "yes, you heard it", but in terms of other information coming back, "no, sir, none of that information comes back". And by carefully thinking through the layers and the way things work, you can have a combination of both centralized and decentralized, which is a lot safer to operate and gives you enough control to feel comfortable, but doesn't force you to have, you know, gigawatts of bandwidth, (pardon, wrong term, but you get the idea).

Moderator: I've got a question for Jonathan, though. The money that was released. You talk about projects being done prior to being, you know, completely cyber security enabled. Do you think that all of that money that was dumped on this market has potentially created a condition where some of the technology was deployed prematurely - before it was quite ready to be deployed…?

Member: Absolutely, absolutely.

Member: …in a rush to get it there, to get it in place?

Member: Yes.

Member: When we think about operating, we really operate in three modes today and a fourth in the future. We have a "business as usual, the sky is blue, everything is great, and everything should work". Then we have, "oh-my-God". Here comes the hurricane, the earthquake, whatever, and we are trying to deal with outage and figure out where it is and so on and so forth. And then we have a mode where we are actually trying to put it back together again, and that is different than an outage mode. This is a restoration mode. And communication is absolutely critical during that restoration mode, because we are trying to get as many people back up as absolutely fast as we can. And we got this new mode that is coming real soon, which is called, "I have to download intelligence to my devices in the field, and I'm actually pushing firmware or software or parameters or other information out into the field", which is a completely different way of operating than we operated in the past. And we got to know that whatever we put in doesn't matter. We can operate in all four of those modes. And if our primary design fails, we need to be able to cascade over to a secondary design and maybe a tertiary and, in some cases, maybe even a fourth or a fifth. And if you go down to Florida Power & Light and go into their various warehouses, you will find that they have these really cool trailers with complete radio base stations, antennas, and everything else. And they can tow them out in the field, anchor the trailer, roll the generator off of the trailer, put the antenna in the up position, and crank it 300 feet into the air and begin to transmit from a site that didn't exist before and put up an operations tent literally and work out of that tent. And we've got to remember that it ain't all going to work when it all comes apart, and we've got to have a way to put it back together again and make it operate. And we can do only so much in the way of initial design, and then we better have ourselves a first aid kit and a bunch of Band-Aids.

Moderator: And one of the interesting issues in this is that if you have a radio in an IP environment, it is actually easier to put things back together again quickly, but…

Member: Up to a point.

Moderator: …Up to a point.

Member: Yeah.

Moderator: There was a "but" there.

Member: But I think the initial question is: what core, IP core is different from, or it is more prone to a bad…your Motorola core, and that there is no difference. It doesn't matter. You have today implemented SmartNet, Motorola SmartNet, SmartZone, whatever. If the core goes down, your system is down, as well.

Member: No. When we had the instability on the network, my sites had a short outage, came back up, and they were fine.

Member: No, no, no.

Member: Everything else was down. EMS was down. My radio system was up.

Member: No, but if your core, if your smart core goes down and just one master site, if it goes down, you have to fall down to local trunking in your SmartZone equipment.

Member: Ours stayed up when we had the instability in our network. It stayed up.

Member: It stayed up. I know, it stayed, but if it goes down, it is the same as IP. No different.

Member: I think there is one important difference. When it comes to the old analog radios, everybody in the organization knows not to touch them other than the RF people. When you go to an IP system, there are a whole bunch of IT people who think they understand what they are dealing with, and they haven't, you know, had the cattle prods on them yet to learn not to touch it.

Member: And then you are also teaching RF technicians networking equipment. And in my case, we are in a union environment, and so there are territory boundaries around who touches what. And it is not necessarily the person who knows the equipment that is touching the equipment.

Member: I was listening to Jonathan talk earlier about the cyber security issues out there, and I was thinking “utility security has changed a lot”. No more is security just the fact that all of your barbed wire is intact, all your switches are padlocked, all of your gates are locked. It is so much more complex now. You used to be able to go out and say, okay, the wire is in the air. No one can touch them. All the switches are padlocked. Nobody can get to them.

Member: I think, ideally, for DMR to be successful, that you would perceive it as just another building block in your infrastructure. Where it fits, you plug it in, right? And ideally that makes sense. However, because of all the NERC CIP requirements for security, this plug-in part of the infrastructure needs to have all of the same cyber capabilities as a wire, as a piece of fiber, as anything else. So the actual technology that makes that happen needs to support all of the same security capabilities that we take for granted on other wired systems.

So that is for another discussion. But I plant the seed that if you were a network engineer and you could pick from various different sources to build out your design, and someone could tell you this DMR solution gives you the same level of security as a T1 or an MPLS network connection or as your own private LAN, then it would give you a lot of freedom on how you design a network at a high level.

Member: It may be that you want a higher level of security than you do on other building blocks both in the cyber area and in the physical area and then, obviously, in the operational security area, which most people don't even begin to talk about now. And it is going to become more and more critical as we operate more and more as a grid: that operational security aspect which military understands, and I don't think we as an industry yet quite understand.

Moderator: Bob?

Member: Converging a whole host of comments here. I agree with Doug in that to you have to understand the application. Certain applications are better served off DMR, and it reminds me that back a number of years ago, there was a Pennsylvania company (whose name escapes me at the moment) that made a mobile router that dealt with this exact issue.

Going over to Jonathan, if you added security to that aspect of a mobile router, now you've got a tool where   in this product, you can tag your data to say what type of data it was and how critical it was. It would look at what paths were available to it and make intelligent decisions. If it was a large payload kind of thing, it would try and wait for a WiFi hot spot at, for example, the refuelling depot or the maintenance garage or whatever it might be. If it was tagged as critical, as well, and there was no Wi-Fi, it would put it over a narrowband network and take advantage [of the radio network].

Moderator: (Unintelligible) [Securing the reliability of] this real-time environment is one of the issues that Jonathan has brought up. Apart from your data, you still have all the security requirements, which are going to add their own payload to your transactions, and this is going to partly determine your whole network architecture. You want, obviously, to reduce latency, to try to reduce the bandwidth required by whatever it is. But in order to improve the reliability of it and the management of it, you are going to add security to it. So you are going to be involved in an interesting tradeoff here.

Member: That's correct. Another issue around security is not just securing the actual information going over the system but providing the security features in the technology. Because I think that, on the IT side, we have already assumed that a network switch or a gateway or some wired device is going to give me SNMP data. It is going to give me the syslog. It is going to tell me the last time someone made a configuration change. It is going to give me a lot of forensic data as to who was using the system and how.

On a lot of the telemetry side of things that are moving to IP, what we are finding out is that those common security features that we come to assume are in place on the wired side aren't always there on the telemetry side. Just because the radio has moved to the IP side and gives you an IP trunk, that device doesn't always give you all of those same cyber security features that a similar IP-enabled device would if it was on the wired side. So that is something that we are very much an advocate of: pushing cyber security standards into these products that are moving into the IP world. And it is not just radios. You know, PLCs, RTUs, which are programmable logic controllers, remote terminal units, EIDs, [electronic intelligent devices]. Just summarize that whole classification and call them “embedded devices”. They don't share a common set of utility tools for the customer. So that is something I think, that Tait, as a vendor of these technologies, should be aware of moving forward as you release technology into the space: ensure that, if you are going to allow radio communications over the air in an IP environment, that each piece of the chain - not just the end devices, but the trunked equipment - all of the pieces along the chain support all of the cyber security requirements that a wire device would give you. And that is something that I think is not quite there in most cases. I haven't seen your equipment, so I'm not sure what is enabled there.

But as a general statement, we find that most telemetry companies that have grown up over the analog world side and are awaking into the IP world are having to learn how to embed those things into their technology.

Moderator: We tend to be the pipe. I think all radio manufacturers tend to be the pipe over which other stuff comes through. But if utilities are going to be recognized as critical infrastructure and if the federal government requires some sort of protection of that infrastructure and certain clarity about the vulnerabilities (not just from hackers but also ensuring the integrity of the information) are these industries, like the telemetry industry, going to be forced into doing things in order to provide the sort of security that the federal government requires?

Member: Over time, the answer is yes. You know, we've seen the adoption by FERC recently of NERC CIP before, is you begin to look at some of the things that are controversial in [NERC CIP] v5. While they are not prescriptive, per se, there isn't a lot of room between the lines to do things that aren't sort of prescriptive. They say –“you've got to be able to do X, we are not going to tell you how to do X, but you've got to be able to do X”. And in many cases, there are only one or two ways today to be able to do that. And as people begin to start to look at [NERC CIP] v6, which I've seen some initial drafting of from some of the guys working on the NERC stuff. We are going to get to the point where we are not going to have a lot of options, and there isn't going to be a lot of room between the lines to paint what we are doing.

Now, it took six years to get to [NERC CIP] v4. V5 has been running around in pieces now for five or six years. V6 may be another six or eight years beyond that. None of us may have to worry about it. We may all be retired by the time it happens. But the reality of it is, the system we are putting in place today, given the asset cycle in the industry, are going to be there in 2050.

Moderator: Well, whoever are the regulatory agencies on the federal side, whoever is enforcing security requirements or managing the security requirements, whether it be NERC or NIST or FERC or whatever, are they going to actually, have teeth and get tough and say to everybody "look, unless you meet these requirements, you cannot sell, you cannot sell to the utilities industry". This is now a regulatory requirement analogous to what the FCC does with public safety and manufacturers.

Member: Well, FERC can already fine utilities up to a million dollars day.

Moderator: What about the suppliers to the utilities, the telemetry guys?

Member: Well, that hasn't happened yet, but we may eventually get there. And if you look at what is going on with the testing and certification committee inside of the SGIP right now and some of the things they are doing around end-to-end testing, it would not surprise me in the long run if some of that end-to-end testing requirement isn't adopted by one or more federal agencies as a requirement and that you can't be certified to sell unless you can pass the end-to-end testing. I'm not going to say that is going to happen in the near-term or the mid-term, but it wouldn't surprise me, because DOD already has for everything they do a set of color books that you have to be able to certify against to be able to sell particular programs. It would not surprise me since DHS right now looks like the likely critical infrastructure security agency moving forward and, given their mentality about TSA, it wouldn't surprise me if we don't go to some sort of color book security requirement if DHS ends up running cyber security for infrastructure.

Moderator: So they will have somebody under them. Currently you've got NERC, NIST possibly, and FERC managing the requirements. Do you think that DHS will replace them or subsume them or what?

Member: Well, FERC already said they are not going to adopt any of the standards that are coming out of NIST. So the teeth out of the NIST side of things are pretty much gone. There is going to be a catalog of standards. These are standards that NIST thinks are useful and appropriate for the industry to use, but no mandate. FERC is going to adopt and approve NSB (phonetic) standards and NERC standards, but probably no others. And so we are probably looking at DHS, then, to adopt all of the security-related stuff. And the food fight will be between FERC and DHS as to how deeply into the bulk power system DHS is going to be allowed to get. And the other food fight will be between the NRC and DHS for how far into the nuclear plants DHS is going to be allowed to get.

Member: If you keep in mind that FERC and NERC only has auspice or oversight over the electric sector, which is one of the 18 critical sectors, DHS has responsibility for all of the rest other than nuclear.

Member: Yes.

Member: And they already have standards, the CFAT (phonetic) standards for chemical facility anti-terrorism standards, are already enforceable for chemical industries. So I think there is going to be an alphabet soup of regulatory oversight for cyber security for critical infrastructure. And how that goes back to DHS or FERC or NERC or where the oversight is for these standards is going to be a little bit of a mess for people, for asset owners, to grasp and stay compliant with.

Member: And you need to be careful about saying over the electric sector, because they only have purview over the bulk power system.

Member: That is right.

Member: And the pipeline transportation system for gas and oil.

Moderator: Okay. I'm going to take two comments now: one from Kelly and one from Bob Ward, and then I think we might break for lunch.

Member: What I would add is that, from a DMR perspective, we, as utilities, have to look at our business needs for transmitting data through that system. The system needs to have some basic standard level of security that it can offer to the traffic that it carries, voice or data. But the criticality of whether it is bulk electric control communications or it is not, and does it fall under NERC or DHS, or whatever, is more of an evaluation. And if it turns out it needs to be more secure than DMR can provide, then we will have to find another way to carry.

In other words, that is the way we normally, as the utility industry, respond to these regulatory requirements. What are the requirements and what does it cover, and then, how do I meet those requirements for what I need to do to run my business? (Too fast) DMR can still carry. It may not be that control does certain things that falls under regulatory guidelines. But we, as customers, will want the DMR technologies to be at least minimally secure from somebody on the corner trying to break in and listen to the voice communication so they can go take pictures of the incident or beat the responders to the site where they are being dispatched to or interfere with that communication.

Moderator: And the sort of security that radio - trunk radio systems - typically provide is well known.

Member: Yes.

Moderator: You know you've got radio authentication and registration. And radio technologies have got good encryption that provides air interface security. Bob Ward?

Member: Well, I want to constrain the electronic security perimeter at our network so that only those things that <u>need</u> to be inside of it <u>are</u> inside of it and not potentially risk commingling my video network with having it commingled with all of that other stuff.

Moderator: Sure….

Member: So I was trying to understand the relationship between NERC CIP and LAN mobile radio and how and why we would want to two to converge.

Member: And I don't know it that ever will or should, but I'm also not sure whether [NERC CIP] v5 and v4 - v5 and v6 - are going to go with regards to repair communication and so on and so forth.

Member: My point was just that if we want the technology to be as useful as we want it to be, then we should make sure that that technology offers a similar set of cyber security capabilities that other IT components do on the wired side, so that you are not constrained to say, "well, I would like to use DMR, but I really can't because it doesn't give me enough cyber features due to its technology or limitations". And I think if you look at the IT side of things, it is almost like looking at a crystal ball, because usually the control system SCADA telemetry industries usually lag IT by about five years. So you can kind of look at the technologies that are already allowed in IT routers and switches and firewalls, like IPSec, SSL, VPN. You know, you can go down the whole list of what typical IT components offer from cyber security, and you can kind of look at that as saying, well, those are probably things that an IP-based radio system should probably also be able to offer. So that was just my point there.

Moderator: Look, this is an interesting issue. Maybe we will break for lunch now and take this up again when we return, because it is a hot topic, and there is lots to explore here.

Moderator: So before lunch, we were discussing some of the security issues surrounding DMR, and Bob had a question that we might pick up right now.

Member: Right. Before the break, we were talking about NERC CIP and how it might interrelate with land mobile radio (LMR) and our desire to keep them separate, if possible, because of the onerous nature of CIP. The answers I heard were that potentially operational traffic with regards to the bulk electric system may require the same sort of protections that we have on other CIP traffic - meaning that things like encryption might be required. And I think we all recognize that encryption over an analog system is a non-starter, so DMR would be --

Moderator: Yes. The impact on the audio quality coverage is too great. That is one of the basic reasons why digital is attractive. Encryption has no impact on coverage or audio quality. You are aware of the encryption that DMR offers?

Member: Yes.

Moderator: AES encryption is going to be the standard for public safety, and that is consistent with requirements for interoperability between public safety agencies. You know, if there is a shared channel with a utility talking to local law enforcement needs to use, they can trade encryption keys and use common encryption algorithm to talk securely.

There are also security issues for maintenance workers. Brazil has such issues, because maintenance workers go into dangerous places. …

Moderator: The security issues actually extend right down. Part of security is privacy, as well. It extends right down to when you are talking about a system that goes from the generation plant down to the smart meters, maybe inside the house, too. So there is an issue of customer privacy, too.

Member: Yes, I think one of the early threats that we identified with the Smart Grid rollout was actually something that a lot of people didn't think about originally: the privacy of the load profiles. Because when you are using your appliances in your home when you are home, you have a certain load profile. And when you go on vacation, that usually flat lines or changes. So one if you are an attacker, why attack one system at a time if you could get access to all the usage data, overlay that on top of Google Maps, know who is on holiday and who is not, and maybe target those citizens.

I think there has been a lot of discussion around who owns the data. Is it the person that uses the electricity? Is that their data, or does the utility own the data? At what point does the private citizen release the data to the utility? What does that impact on privacy? So that is the question.

Member: There are also other third parties who want control of that data for marketing purposes and other reasons.

Member: Exactly. And there is a big incentive to know the load profiles from a utility perspective. You guys mentioned that before to accommodate for big load issues or to try to motivate users to use electricity during off-peak hours, so that the utility can delay transmission grid upgrades and try to get more load out of the system. I think that helps enable time-of-use billing, which we've seen in the commercial space, but I don't think that many residents or home users have been educated as to what time-of-use billing is going to do for them in the future. And I will just kind of throw that out there. I don't know if this is a security topic, but I think the way we use electricity is a private matter, and that privacy issues of confidentiality, integrity, availability - all three pillars of cyber security - apply, and how do you address those issues with Smart Grid if you are using DMR as a last mile?