NRECA CRN™
COOPERATIVE RESEARCH NETWORK

TechSurveillance Magazine

Data Diodes for Cyber Security

BY COURTNEY BARRY
MARCH 2012

Data diodes, devices which allow communications to go only one way along a data link, are increasingly being investigated as a more secure method for safe data transport in high security facilities, particularly with the NERC CIP (cyber security) standards, which state that entities must ensure that "every critical cyber asset resides *within* an electronic security perimeter." Used most commonly in the IT community for government agencies such as the Department of Defense and the Department of Energy, the diode is also becoming more commercially prevalent in the electric power industry, as well as in nuclear and hydro-electric power plants. But there is some skepticism about the actual protection offered by the diodes and many co-op representatives are taking a wait-and-see approach.

Introducing Data Diodes

Data diodes come in different designs. The most common design incorporates a laser and a charge-coupled device (CCD). The laser encodes the information being passed unilaterally; the CCD receives the information. The one-way flow of data is enforced on a hardware level: the CCD cannot transmit information, nor can the laser receive it (see **Figure 1**).

One manufacturer that uses this design is BAE. Robert Jones, the Global Product Manager at BAE, says that the strength of this design is that "It doesn't have an IP entrance. It doesn't respond to a ping. Even if enemies of the U.S. were to capture one of our data diodes, the best thing they could do is build one for themselves. They would not be able to reverse engineer and find a way to compromise the device."

Not all data diodes are built on the laser+CCD design. In some cases, the unidirectional flow of data is enforced via software.

Not all data diodes are built on the laser+CCD design. In some cases, the unidirectional flow of data is enforced via software. Jones makes the case

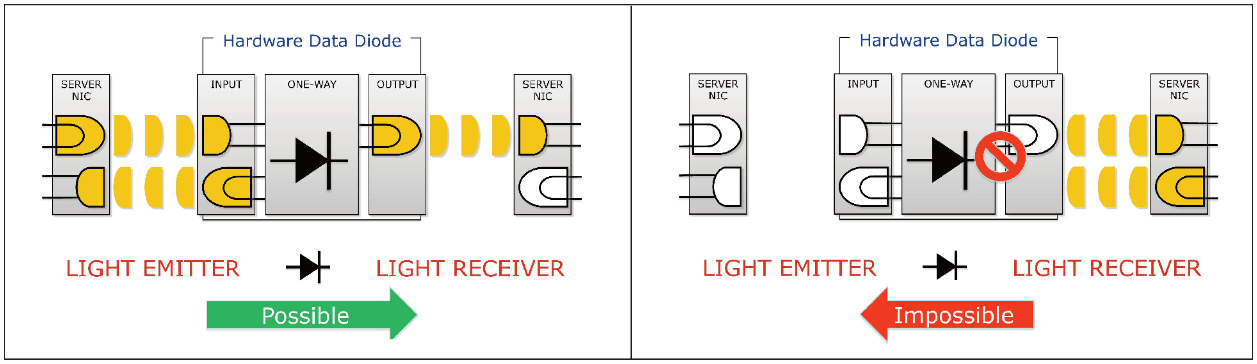

FIGURE 1: The Data Diode permits the one-way flow of information, while blocking the flow of data in the other direction.

Certain diode solutions not only physically enforce one-way flow of data, but can also, by using specific content filters, scan and screen *data.*

that these are not true data diodes, since the one-way flow is being *logically* enforced (rather than enforced through the physical properties of the hardware). "They are based on firmware or basically programmed logic," he says, and thus are vulnerable to infiltration and hacking.

Diodes are not a firewall. However, certain diode solutions not only physically enforce one-way flow of data, but can also, by using specific content filters, *scan and screen* data. Using what Jones calls 'true file typing,' he says, "We can look at what the file is and no matter how much you change the name or try to describe it, we can actually look at the file and determine, is this really a word document or is it really a virus, or is this really an executable *disguised* as a word document?"

General Uses for Data Diodes

Where would a data diode be useful? Joost Bijl CISSP, Marketing Manager for Fox IT in the Netherlands, says there are two ways diodes might be used to increase security in an electric cooperative.

The first scenario involves preventing data leakage. A higher classified network containing very sensitive information is usually disconnected from other networks. A typical example is an R&D network or the SCADA network at a power plant. This disconnection is inconvenient because you need updated digital information in that network. The current practice is using destroyable media such as CDs or USBs to make this 'connection.' However, these can be damaged or, in the case of USBs, vulnerable to viruses. The data diode improves this situation hugely because you can automate the process while maintaining that high level of security. "In this way, data only gets in and you can be sure it doesn't get out," says Bijl.

In the second scenario, the diode allows for connecting data the other way around: making sure that data from the SCADA network can leave that network, for example, to the business network of a power plant or to the Internet, but not permitting information to flow back in to the SCADA network. This might be useful, for example, if Smart Grid operators need to monitor the status of their power supply.

Larry Shivers, EMS Support Manager for Tri-State G&T Association in Westminster, CO, says that, while Tri-State is not yet using data diodes, he has looked at them for future implementation. "The way a co-op might use it would be if they have a SCADA system and want to pass data to a corporate network. That's how we would probably use it as well."

"The diode itself doesn't pass the control signals across to the other side. The only thing going through the diode is the actual data…"

– LARRY SHIVERS, TRI-STATE G&T ASSOCIATION

Shivers says, "The diode itself doesn't pass the control signals across to the other side. The only thing going through the diode is the actual data, whereas most other devices pass the Internet Protocol (IP) control signals as well. There's no way for someone to come in and find out what the IP addresses are on the other side."

Version 4 of the NERC CIP compliance documentation encourages using one-way devices as opposed to firewall or other devices.

NERC CIP Applications

The fact that IP control signals are not passed means that data diodes may become important for NERC CIP compliance. Version 4 of the NERC CIP compliance documentation encourages using one-way devices as opposed to firewall or other devices.

But NERC has not been 100% aligned with the use of data diodes. Shivers says he received some information from NERC about diode implementation and they were using cautionary language, that diodes might not deliver the actual protection that was being touted, and also advised checking on how they were rated in terms of cyber assets. For more on NERC and Data Diodes compliance, go to **http://www.nerc.com/files/CAN-0024%20Routable%20Protocols%20and%20Data%20Diode%20Devices.pdf**. (Also see CRN's *TechSurveillance* article, *Security by Design—A Cooperative Perspective* by Jerald Dawkins and Randall Nason, September 2010, that outlines new government and industry regulations exerting strong guiding pressure on utility companies and electric cooperatives.)

David Dockery at Associated Electric Cooperative Incorporated (AECI) says they have been interested in data diodes but haven't purchased any yet. They have researched them for possible deployment protecting cyber assets at their Critical Asset facilities, oriented outward for data export. The primary value would be improved defense of critical cyber assets against remote attacks. Yet due to high data-diode costs, they also are interested in any NERC CIP compliance-related value.

So far, says Dockery, it seems clear that NERC CIP Standards and auditors see no more value in deploying data diodes than any other network devices designed to control electronic access. (See NERC CAN-0024, as well as NERC's "Standards Under Development", Project 2008-06 Cyber Security – Order 706, Version 5 Standards in initial ballot.) NERC's position seems curious to Dockery, in light of value the Information System industry places upon data diodes, for helping guard electronic access to highly valued assets. So, Dockery explains, "AECI is still hoping our industry will influence the NERC CIP

Version 5 Standard, currently in its initial phase of comment and ballot, into recognizing the greater protective value to these devices."

Dockery added that he knows of one large IOU that has extensively deployed data diodes. However, this utility can leverage economies of scale for large data diode purchases, and has enough legal resources to defend their use of data diodes to regulators—should it come to that.

Cost of Data Diodes

Data diodes can be tailored to meet individual customer needs; certain things can be added, such as additional protocols. As a result, price can vary substantially. A large component involves certification.

Fox IT's Bijl says if you go with a SCADA or business addition, it's usually around $30,000 with turnkey delivery. Jones explains that industry scrutiny goes further, and that diode devices certified under the common criteria—a methodology for testing reliability established by the "Five Eyes" nations of The Technical Cooperation Program (New Zealand, Australia, Canada, the U.S. and the U.K.)—can range in price from just under $30,000 to more than $150,000. (Uncertified diodes and solutions are being marketed by foreign competitors, and they may be less expensive, but they are not U.S. government approved.) Price differences are largely driven by the device's bandwidth capability, Evaluation Assurance Level (EAL), Mean Time Between Failure (MTBF), and Diode Type (back office or ruggedized for field or aircraft use).

Since most diodes are custom ordered, little needs to be done to the product on-site. This makes installation a streamlined process (mostly connecting cables and settings configuration options). Typically, it takes about two business days for installation, says Jones, one for set up and connection and one for training. For more complex solutions, it can take up to seven days.

Clearly, the need for more and better cyber security is under investigation. Most co-ops are researching them with an eye toward future cost-effectiveness, but are also waiting on the final conclusions made by NERC CIP compliance. As Shivers concludes, "It looks like a good technology to me just looking at it from a high level." ■

Diode Vendors

Owl Computing Technologies (http://www.owlcti.com) designs and markets data diode-based cross-domain solutions for government and military cyber security, and electronic perimeter diode defense systems for critical infrastructure entities like Power Generation & Water Management.)

Fox-IT (https://www.fox-it.com) gives PCS networks secure, real-time transmission of information by enabling one-way data transmission from the process control network and physically preventing electronic access to the sending network.

BAE Systems (http://www.baesystems.com) information security products enable classified information sharing, while enforcing network segregation. Available off-the-shelf or as part of a total system solution.

Waterfall® Security Solutions Ltd. (http://www.waterfallsecurity.com) provides Unidirectional Security Gateways and data diodes for Process Control Systems, SCADA systems, Remote Monitoring and Segregated Networks, enabling secure and real-time data transfer, from critical (e.g.: SCADA, production, industrial, etc.) networks to external/business networks.

About the Author

Courtney Barry, a writer in Austin, Texas, has written for publications including *Public Utilities Fortnightly, Public Power Magazine, The New York Times* and Wirednews.com. She previously worked for the Public Utility Commission of Texas.

Questions or Comments

Maurice Martin, maurice.martin@nreca.coop

Legal Notice

This work contains findings that are general in nature. Readers are reminded to perform due diligence in applying these findings to their specific needs, as it is not possible for NRECA to have sufficient understanding of any specific situation to ensure applicability of the findings in all cases. Neither the authors nor NRECA assume liability for how readers may use, interpret, or apply the information, analysis, templates, and guidance herein or with respect to the use of, or damages resulting from the use of, any information, apparatus, method, or process contained herein. In addition, the authors and NRECA make no warranty or representation that the use of these contents does not infringe on privately held rights. This work product constitutes the intellectual property of NRECA and its suppliers, as the case may be, and contains Confidential Information. As such, this work product must be handled in accordance with the CRN Policy Statement on Confidential Information.