



The ABCs of Network Security - BBB (Borrow)

Industrial Network Security by David Teumim

Reviewed by Nick Sands

One of the hottest topics in the control industry is security for process control systems and networks. Finally ISA has a book on the subject, *Industrial Network Security* by David Teumim. Teumim is a certified information system security professional (CISSP) and a workgroup leader for SP99, the committee working on manufacturing and control system security. The book is very basic, an introduction to an introduction to the subject. But with such a new area, this elementary book is a good beginning to the body of knowledge.

The first chapters are an introduction and background, answering many questions. What is an industrial network? Why should it be secure? Can it be secure and open? Who should work on security? How is the cost justified? Teumim contrasts IT security issues, managed corporately by a CIO and a cybersecurity manager, with security for manufacturing control systems, managed by a plant personnel like the automation and control manager. The shift of control systems from proprietary to commercial-off-the-shelf hardware and software and network connectivity have created new vulnerabilities in industrial networks. But cybersecurity alone is not enough. A complete security program also includes personnel security, and physical security.

Cybersecurity consists of protecting the availability, integrity, and confidentiality of the systems and data. This requires understanding the threats to the systems and the vulnerabilities of the systems. Threats like the Slammer worm and buffer overflows are explained. Some of the highlights of this book are the examples of real attacks on control systems and the consequences. Countermeasures can be designed to protect against the threats. Usually a system for identification, authentication, and authorization is one of the most important layers of defense.

The remainder of the book covers the steps, at a very general level, to execute an industrial network security program. The first step is planning and design for security, such as separation of networks. An understanding of the technology, like encryption and firewalls is important. To make an effective security system requires writing clear policies for the application of technology, trained and aware people, and periodic audits and other methods to provide assurance of the effectiveness of the security program. Some example approaches to industrial network security programs from Dupont and Proctor & Gamble form the last chapter.

Every company in the control community will have people that can benefit from reading this book, people that need a basic understanding of information security for manufacturing and control systems. Teumim just introduces the subject though, with little detailed information. Future books or revisions of this book will have more lasting value as references. So even though this book is a must read, it is not a must buy at \$54 (ISA member price). It is a great book to borrow (BBB).