

PROTECTING INDUSTRIAL CONTROL SYSTEMS

FROM ELECTRONIC THREATS

Preface

This book is meant to help both the novice and expert in information technology (IT) security and industrial control systems (ICSs) gain a better understanding of protecting ICSs from electronic threats. It illustrates that electronic threats to ICSs are real and have already caused extensive plant and environmental damage, power outages, and even deaths. By popular demand, it provides recommendations for securing these systems that will enable facilities to maintain their reliability and safety. The book was also written to fill a hole that exists in academia—security is taught in computer science departments, whereas control systems are taught in various engineering departments. Traditional security approaches can, and have, impacted the performance of control and even safety systems. This book can be used as an introduction to cyber security of industrial control systems prior to teaching control system theory in engineering classes or security classes in computer science.

As for an explanation of the title, the term “protecting” was chosen as this is not a book on how to attack ICSs. From a cyber perspective, they are very brittle, and attacking them is not rocket science. On the other hand, protecting them while at the same time maintaining their mission can be rocket science. The term “ICS” was chosen as ICSs include supervisory control and data acquisition, distributed control systems, programmable logic controllers, remote terminal units, intelligent electronic devices, field controllers, sensors, drives, emission controls, building controls (including fire suppression, thermostats, and elevator controls), and meters (including business and residential automated metering). For the purpose of this book, ICSs also include safety systems. The term “electronic threats” was chosen rather than cyber security because there are electronic threats to ICSs beyond traditional cyber threats.

Additionally, the book is about protecting the mission of the ICS—a compromise of a computer that isn't critical to the mission of the control system may be a cyber security event, but it is not of importance. One may say that “it takes a village” to secure ICSs, as Operations alone cannot do this. It takes a team of ICS expertise, IT security expertise, telecom knowledge, networking, ICS and IT vendor support, and most of all, senior management support to make this work.

I hope you find the book of interest.