Preface

This is the fourth edition of this guideline, reflecting the actual development in the IEC 62443 series. Like in the previous editions, the purpose is to describe a holistic approach for the development and practice of a security protection scheme for industrial facilities, as well as secure development lifecycles of products. Protection against cyber threats requires a number of different, often independent measures. A holistic approach for a sustainable protection of operating facilities requires in general the contribution of product suppliers but also of integrators and operators and includes technical as well as organizational measures.

What has to be noticed since the last edition, published in 2023?

I think one important development is the acceleration in the regulation in Europe. The Cyber Resilience Act (CRA) for products with digital elements puts more responsibilities on suppliers for supporting their products along the entire lifecycle. For products used in an industrial environment, activities are going on in CENELEC to develop harmonised standards based on IEC 62443 to support compliance with the CRA. Asset owners are increasingly requested to implement security programs fulfilling the requirements of the Network and Information Security Directive (NIS 2). NIS 2 requires member states to implement it into national law by October 17, 2024, establishing technical and methodological requirements for cybersecurity risk management. The German government adopted its first draft of the NIS 2 Implementation Act on July 24, 2024, which will impose extensive obligations on approximately 30,000 companies operating in Germany. Asset owners, service providers and product suppliers benefit significantly in their effort to comply with CRA or NIS 2 by basing the implementation of their security programs on IEC 62443.

The standard series IEC 62443 achieved a major step in 2024 with the publication of the second edition of the part 62443-2-1 which is addressing the requirements to the security program of asset owners. This is one of the key documents of the concepts described in this book and already depicted in the previous editions. The elements of a security program of asset owners described in the second edition of 62443-2-1 will be the base for restructuring all other documents of the series to better show their relationship. Another development is the publication in 2024 of the publicly available specification IEC 62443-2-2 which is based on the content of this book.

I participated actively in the emergence of the standard IEC 62443 and developed several of the concepts described in this book. These have shown their value when implemented in the company where I made my longstanding career and I am happy to continue to promote the standard IEC 62443 as a consultant. The standard is bulky, reflecting the complexity of the topic. This book is a tentative to facilitate the access to the standard by giving an overview and describing the main concepts which are underlying the standard. These are also the basic principles when designing and deploying protection concepts for operating facilities as well as integrating security in the product development lifecycle. It is intended to be useful for decision makers, managers, technical leaders, engineers and technicians as well as for students.

In this edition of the guideline, I tried to precise the concepts of Security Programs (SP), Security Protection Schemes (SPS) and Security Protection Ratings (SPR) and I added a new clause describing how IEC 62443 and ISO 27001 / ISO 27002 should be integrated for the implementation of the protection of industrial facilities against cyberthreats.

Sandhausen, autumn 2025 *Pierre Kobes*