Preface

Nowadays one of the most important objectives of the nations is the protection of their critical infrastructure against cyber threats. Several countries already issued directives or laws requesting operators of critical infrastructures to fulfill a minimum set of security requirements. I wrote this text for the previous edition. It remains very actual. The legislation progresses slowly, but the increase of cyber threats has its own speed. Responsible organizations are more than ever requested to improve the protection of their operating facilities. The standard IEC 63443 has the objective to cover the various dimensions of industrial cybersecurity and is therefore widely used for the development of holistic protection concepts for operators as well as for product suppliers.

When I started to work in the area of cybersecurity applied to industrial environments, it became rapidly clear to me that the topic is manifold. Protection against cyber threats requires a number of different, often independent measures. For example you have to pay attention among others to user management, malware protection as well as patch management. Three measures, which are totally independent, but of equal importance. 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.

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.

This is the third edition of this guideline, reflecting the last developments in the IEC 62443 since 2020. It describes in detail the holistic approaches for the development and practice of a security protection scheme for industrial facilities, as well as secure development lifecycles of products. The concepts described in the previous editions have been confirmed and refined. In particular the grouping of requirements in common security objectives is today more concrete. The elements of a security program of asset owners will be the base for common objectives, as this structure will be settled as an international standard in 2023 or beginning of 2024.

Sandhausen, autumn 2023 *Pierre Kobes*