# Preface

I would like to thank you for purchasing the second edition of "Industrial Network Security," especially if you are one of the many supporters of the first edition.

When the second edition was announced, many people asked me, "why a second edition?" and even more followed that up with, "and why a coauthor?" These questions are harder to answer than you would think.

When I wrote the first edition, I set a very high standard for myself and did everything that I could do at the time to create the best book possible. While the first edition was well received, I've gained more experience and knowledge since then, and the industry has advanced. The threat is now better understood, thanks to an increasing trend in industrial cyber security research. Unfortunately, there has also been an increase in the development of new exploits, and there have been an increasing number of large-scale incidents. In short, there is a lot more to talk about.

However, I did not want to just update the first edition.

One of the biggest problems with industrial cyber security is that it spans two domains of specialized knowledge: Information Technology (IT) and Operational Technology (OT). Some things that come naturally to an IT veteran are hard for an OT person to grasp. Some things that an OT guru takes for granted seem odd to an IT pro. There are two separate perspectives, two separate lifetimes of experience, and two separate lexicons of "tech speak." A new breed of industrial cyber security professional is slowly emerging, but even among this minority there are clear factions—we know who we are—who have strong opinions about disclosures, or regulations, or particular methods or technologies, and take hard stances against those with opposing beliefs.

What I have seen, however, is that when our differences materialize as conflict, it becomes a barrier to good cyber security. When people come together and work cooperatively, the incongruences and misperceptions quickly fade. E*verything* becomes easier, and good cyber security is almost inevitable. In the second edition, I wanted to address this fundamental challenge.

Not easy.

My background is in IT, and although I've worked in industrial cyber security for a long time, it is impossible to alter my core perspectives. The only way I could get an additional perspective into the book was to put my manuscript where my mouth is, and write the second edition in cooperation with another author.

Enter Joel Thomas Langill. Joel, aka the SCADA Hacker, brought a lot of extremely valuable perspective to the second edition. Where my background is mostly in IT, his is mostly in OT; where my research tends to focus on emerging technology and countermeasures, Joel is more grounded in the real world, and has refined cyber security planning, assessment, and mitigation techniques over years in the field. We had a common goal, and a lot of common beliefs, but very different perspectives.

Joel and I kept each other honest, and shared new ways of looking at very common issues. It resulted in the refinement of the original text, and the addition of over

40,000 words of new material, including several new chapters (for those who are not familiar with publishing, that is almost enough to make a whole new book).

It was not always easy. Just as IT and OT clash within industry, our perspectives sometimes turned discussions into arguments. However, we almost always came to the conclusion that we were actually saying the same things. We simply used terminology differently, and we saw certain problems through different lenses. Neither of us was wrong, but our idea of what was "right" did not always match up 100%. But we worked through it.

Through compromise and cooperation, what is left on the pages of this book should be more beneficial to more people—IT or OT, Technologist or Policy Maker, Security Researcher or CISO. Our hope is that the second edition of Industrial Network Security will provide a common frame of reference that will help bring the industry a little bit closer together. And if you read something that you do not agree with, we welcome you to give us *your* unique perspective. Joel Thomas Langill, Eric D. Knapp, and Raj Samani can be reached on twitter at @scadahacker, @ericdknapp, and @Raj_Samani, respectively, and we look forward to continuing the discussion online.

Best Regards,

**Eric D. Knapp**