

GETTING STARTED IN INDUSTRIAL (ICS/OT) CYBER SECURITY

**For IT Cybersecurity
Professionals**

Mike Holcomb, GRID, ISA 62443

v2023.1

Acknowledgements

To Michael Assante

None of us would be here without you nor would the world be as safe. Rest in peace.

To Rob Lee

Thank you for all you do to encourage others to not only get into the ICS/OT cyber security field, but to enlist them in your vision of safeguarding civilization.

To those in the ICS/OT community

For all the owners, operators, engineers, automation professionals, technicians, cyber security team members and others that keep our facilities safe and operational, thank you for all of your dedication!

To all those wanting to get into ICS/OT cyber security

Don't be discouraged. You can play a big part in protecting the world around us!

About the Author

Mike Holcomb is the Fellow of Cybersecurity and the ICS/OT Cybersecurity Global Lead for Fluor, one of the world's largest engineering, procurement, and construction companies. His current role provides him with the opportunity to work in securing some of the world's largest ICS/OT environments, from power plants and commuter rail to manufacturing facilities and refineries.

As part of his community efforts, Mike founded and leads the UpstateSC ISSA Chapter and BSides Greenville conference. He also wrote and taught all six cyber security courses for Greenville Technical College's cyber security program which focuses on helping educate the cyber security practitioners of tomorrow.

Mike also provides consulting services to outside parties through his company, UtilSec LLC.

Introduction

“How do I get started in industrial cyber security?”

This is the most common question I receive.

To help answer this question, I wanted to write a quick start guide to share (while I work on a much longer book).

How you get started though depends on your background. Are you an OT engineer or other professional? Are you in IT cyber security? Do you have no experience in either?

This guide is written for those of you in IT cyber security today that want to learn more about the fascinating world of industrial (ICS/OT) cyber security.

Tips for Before You Get Started

Here are a few things to keep in mind:

1. Take your time to learn

Learning this field requires you not only to learn about ICS/OT control systems, but also engineering concepts from a range of sectors. It will take time!

2. Be prepared to use Google (A LOT)

Coming from an IT background, you will undoubtedly come across many acronyms and engineering concepts that are new. Don't be afraid to research!

3. The ICS/OT cyber security community is an incredible resource and ally

There are a lot of incredible people that make up this community that want to help you succeed in helping protect the environments that move the world around us!

Welcome...

To protecting the world around us!

The world of ICS/OT is vast and often unseen. Most people take their “always present” electricity, clean water, transportation, pharmaceuticals and other manufactured goods, for granted.

I know I did.

And now I keep working to fight the good fight and help others do the same!

The Threats Increase Daily

Just like the IT world, OT is vulnerable.

Whether OT realizes it or not, the attackers do. The number of attackers is not only growing, but diversifying. Up to a few years ago, most OT environments only had to be concerned with nation-state adversaries.

Now every OT environment needs to be concerned with all the other types of attackers (e.g., ransomware groups, hackers, lone wolf operators).

As we say in the IT world...

**It's not a question of
IF, but a question of
WHEN!**

An Abbreviated History of ICS/OT Major Events

The ICS/OT world has had its fair share of security incidents, some with potentially devastating consequences. Most incidents are not publicly disclosed and we will never know about them.

Here are just a few important public incidents to know about:

2003: Davis-Besse Hit by SQL Slammer

This power plant had to shut down part of its systems down due to a SQL Slammer infection that came from the Internet (via a unauthorized vendor connection). The environment was believed to be airgapped with no external connections.

The real kicker? Davis-Besse is a nuclear power plant.

An Abbreviated History of ICS/OT Major Events (cont.)

2010: Stuxnet

The United States and Israel created the first known piece of malware to target ICS/OT systems. The malware known as Stuxnet was responsible for physically destroying many of the centrifuges used in Iran's nuclear arms program.

The incident launched a cyber arms race.

2015 & 2016: Ukrainian Blackouts

Russian adversaries targeted different power facilities to create blackouts in the Ukraine two years in a row.

At night. In the middle of winter.

Other similar ICS/OT-related attacks can be observed in the current Russian invasion of the Ukraine.

An Abbreviated History of ICS/OT Major Events (cont.)

2017: Trisis / Triton

A Russian adversary compromised the SIS (Safety Instrumented System) at a petrochemical refinery in the Middle East. The SIS is designed to act as a failsafe to safely shut down a plant in the event a fault condition is detected.

The only reason an attacker would take control over the SIS is to cause an explosion and to do harm and/or kill.

2021: Colonial Pipeline

The IT systems at Colonial Pipeline were infected by ransomware resulting in the OT network which controlled the pipeline being taken offline. The result was that the largest gasoline pipeline in the United States was down for 10 days.

Ten Steps to Getting Started

This guide focuses on the ten steps for IT cyber security professionals to get started with industrial (ICS/OT) cyber.

Here are the prioritized ten steps:

- 1. Learn to think like an engineer**
- 2. Understand industrial control basics**
- 3. Explore training options for learning**
- 4. Learn the standards and regulations**
- 5. Gain hands-on experience**
- 6. Network with the community**
- 7. Stay current**
- 8. Find an experienced mentor**
- 9. Build relevant soft skills**
- 10. Get certified**



#1. Learn to Think Like an Engineer

Coming from an IT cyber security background, this was the most critical step for me. I had never thought about control systems and engineering, even if I had enjoyed related courses like physics.

I just never thought LIKE an engineer.

I did not look at how different industrial sites ACTUALLY worked.

Once I could start to look at how each unique environment runs, it helped me understand:

1. The importance of keeping people safe
2. What is important to running a facility
3. We need a common bridge between IT and OT

Just Remember...

Every ICS/OT environment is different!

Each power plant is different. Each refinery is different. Each manufacturing plant is different.

Make sure to spend significant time researching how the environment you work in is designed, operated and maintained.

Without doing so, you can never begin to understand what is at risk and how to protect it from cyber attacks.

Resources for Exploring Critical Infrastructure Sectors

Here are some links on different types of ICS/OT environments to get you started:

Critical Infrastructure Sectors

youtube.com/watch?v=YmedABQthec

Chemical Engineering

youtube.com/user/pratheepthavara

Hydropower 101

youtube.com/watch?v=q8HmRLCgDAI

Facts About Critical Manufacturing

youtube.com/watch?v=y7fYND7AojU

How a Nuclear Power Plant Works

youtube.com/watch?v=AMXxXoHtM-o

Commuter Rail

youtube.com/watch?v=cjDvE24lhxM

Resources for Learning to Think Like an Engineer

One of the challenges ahead is connecting with engineers. To do so, it helps to look at the world from their perspective.

Think Like an Engineer

engineercalcs.com/do-engineers-think-differently/

Free MIT Courses

<https://ocw.mit.edu/>

- Introduction to Engineering Concepts
- Principles of Engineering Practice
- Introduction to Engineering Systems

**Think of other ways you
can find common ground
with OT folks!**

#2. Understand Industrial Control Basics

This step can be a whole new world for those coming from an IT cyber security background. When we first hear about industrial cyber security, it is hard to visualize the systems we are actually talking about.

The number of new acronyms can seem overwhelming at first.

PLC **ICS**
IACS **MES** **IED**
RTU **SIS**
BMS **DCS**
SCADA
CPS **OT**
HMI

But Don't Worry...

Remember...

**Everything in IT and
cyber security seemed
new and overwhelming
at first too!**

There was a time where you didn't know what TCP or UDP are, what the OSI model was, let alone how an exploit was different from a payload.

Every field takes a little bit of time to get familiarized with. ICS/OT is no different nor is it more complicated!

If I can do this, you can definitely too!

Resources for Learning About Industrial Controls

Get started with these resources on learning about different OT systems:

- 1. ICS/OT Cyber Security Books**
- 2. ICS/OT Podcasts**



These are for getting started quickly!

More resources are listed as you read on!

Top ICS/OT Cyber Security Books

"Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" by Andy Greenberg

"Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions" by Clint Bodungen, Stephen Hilt, Aaron Shbeeb, Bryan Singer and Kyle Wilhoit

"Countdown to Zero Day" by Kim Zetter

"Industrial Network Security" by Eric Knapp and Joel Langill

"Industrial Automation and Control Systems Security Principles" by Dr. Ronald Krutz

"Industrial Cybersecurity" by Pascal Ackerman

My Favorite ICS/OT Cyber Security Podcasts (So Far...)

Control Loop

theycyberwire.com/podcasts/control-loop

Unsolicited Response

unsolicitedresponse.libsyn.com

The (CS)2AI Podcast Show

cs2ai.org/podcast

The Industrial Security Podcast

industrialdefender.com/podcast

The PrOTect OT Cybersecurity Podcast

waterfall-security.com/ot-insights-center/?type=podcast



#3. Explore Training Options for Learning

Getting started or further developing your knowledge can be frustrating.

And expensive... but doesn't have to be!

Formal courses and other content exist to help you learn, just not to get certified.

While getting certified can help demonstrate your passion and growing knowledge of the ICS/OT cyber security world to get your first job in the field, growing that knowledge in the first place is what is most important!

That's why getting certified is the very last step suggested in this book!

Next you'll find some free, and not so free, resources to get started with.

Free ICS/OT Cyber Security Training Resources

Here are some free resources to get you started on your learning path:

1. ICS Training Available Through CISA

The Cybersecurity & Infrastructure Security Agency in the US makes some incredible courses available for free.

You do not need to be a US citizen to learn.

cisa.gov/ics-training-available-through-cisa

2. UtilSec YouTube Channel

All of my content that I put out on LinkedIn makes its way to my YouTube channel. Including a walkthrough of this book!

youtube.com/@utilsec

Not Quite Free ICS/OT Cyber Security Training Resources

In addition to the free training, other options exist for low to substantial costs:

Dragos Academy

dragos.com/dragos-academy/

ISA / IEC 62443

rb.gy/ap3wa

SANS ICS Training

rb.gy/66a6y

Udemy Courses

udemy.com

**Check out more
resources in the
Certification section!**

#4. Learn the Standards and Regulations

There are two main standards that are used to establish cyber security management programs in ICS/OT environments. Learn them! Live them!

1. ISA/IEC 62443

The gold standard, 62443 is internationally recognized by most entities.

rb.gy/mo3r1

2. NIST 800-82

The United States' NIST provides an accepted framework for managing ICS/OT cyber security in this document release.

IT professionals should feel more comfortable with NIST to start.

csrc.nist.gov/pubs/sp/800/82/r3/final

#5. Gain Hands-on Experience

The first time you are on-site at an industrial facility will be an eye-opening experience, helping to truly show the impact and importance of such sites.

But not everyone has the chance to visit a plant right away let alone have other opportunities for gaining real world experience.

Here are some ways to get experience:

- Build a home lab for testing
- Learn to program PLCs

Be sure to think of other ways to gain experience coming up in Step #6!

Build a Home Lab for Testing

Here are some suggestions on building your home lab for learning ICS/OT:

1. Keep Your Lab Network Isolated

To ensure the rest of the world stays safe from your experiments, and vice versa, keep your lab air gapped - just as any good ICS/OT network should be!

2. Start Small and Build From There

A home lab can take on a life of its own, and a costly one at that. Grow only as your resources allow you to.

3. Use Physical Assets When You Can

While it is always best to use the real thing, ICS assets don't come cheap - even off of eBay!

Build a Home Lab for Testing (cont.)

4. Virtualize for Reduced Costs

Save yourself some money and use virtualization where you can.

5. Use the Right Tool for the Right Job

Don't forget to consider IT-related tools for learning ICS/OT. Wireshark is an excellent example of a traditional IT tool used in the world's largest ICS/OT networks.

6. Leverage Simulations

When resources are tight, use solutions that emulate assets you can work with and learn from.



Learn to Program PLCs

One of the best ways to learn about ICS/OT environments is from the ground up. You can start with programming a PLC which is the most commonly used type of control system.

You can look at using either software that simulates a PLC or purchase a real PLC.

I'm a big fan of the CLICK PLCs from Automation Direct. Fully functional, used in production environments and low cost!



PLC Programming Resources

Here are some free resources to get you started:

PLC Academy

plcademy.com

AutomationDirect PLC Training

automationdirect.com/programmable-logic-controllers/plc-training

PLC Basics Playlist

youtube.com/watch?v=ReTtgzN-Dmc&list=PLIn3BHg93SQ85ymy4VvtmRGxo2Stps2lv

Learn PLC Programming in 7 Hours

youtube.com/watch?v=c4cEeA6mdq0

Use an Arduino and OpenPLC Software to Emulate a Real PLC for Programming

rb.gy/63hca

#6. Network With the Community

The ICS/OT cyber security community is growing every day along with the many “veterans” you can learn from and share with.

- **Professional associations**
- **Conferences**
- **ISACs**
- **Social media**
- **CTF Challenges**



Professional Associations

Here's a list of groups associated with ICS/OT cyber security:

ISA (International Society of Automation)

www.isa.org

C2SAI (Control System Cyber Security Association International)

www.cs2ai.org



Conferences

Here's a list of great conferences which focus on ICS/OT cyber security:

Control Systems Cyber Senate

cybersenate.com

Dragos Industrial Security Conference

dragos.com/event/disc-2023/

ICS Village at Defcon (and other events)

icsvillage.com

S4

s4xevents.com

SANS ICS Summit

sans.org/cyber-security-training-events/ics-security-summit-2024/

ISACs

Information Security and Analysis Centers are built around individual sectors. Membership is limited to those that work in the associated area.

Participate with the appropriate ISAC. Not all are free and/or inexpensive.

A few popular ones for ICS/OT:

E-ISAC (Electricity)

eisac.com

ONG-ISAC (Oil & Gas)

ongisac.org

ST-ISAC (Surface Transportation)

surfacetransportationisac.org

Find a comprehensive list at

nationalisacs.org

Social Media

So many thought leaders and professionals that want to share can be found on social media.

Here are some great active people to follow on LinkedIn:

1. Anna Rebeiro
2. Dale Peterson
3. Danielle Jablanski
4. Dawn Capelli
5. Derek Harp
6. John Kingsley
7. Jonathon Gordon
8. Marcel Rick-Cen
9. Michael Holcomb
10. Pascal Ackerman
11. Rob M. Lee
12. Roya Gordon
13. Shiv Kataria
14. Tony Turner

CTF Challenges

CTFs can be great ways to get hands-on experience in ICS/OT cyber security.

Keep an eye out for any that come up.

Organizations like SANS and Dragos open their ICS/OT CTFs to everyone virtually.

Dragos' next 2-day CTF is coming up on Nov. 2nd.

Be sure to check it out!

dragos.com/event/capture-the-flag-2023/



#7. Stay Current

This can be a struggle for some people, especially once they have the role they want.

Yet, it is extremely important that you keep up-to-date with the latest cyber security news.

The attack landscape is always changing.

Always keep an eye out for the latest attack, and review older ones.

Do you understand how each one works?

How do you protect against such an attack?

Is your organization protected?

Resources for Staying Current

Here are a few of my favorite resources for staying current on ICS/OT cyber:

Dragos Blog

dragos.com/blog

Mandiant Blog

mandiant.com/resources/

Industrial Cyber

industrialcyber.co

Bleeping Computer

bleepingcomputer.com

Security Week

securityweek.com/category/ics-ot/

SANS Internet Storm Center

isc.sans.org

#8. Find an Experienced Mentor

Working with someone who has done much of what you want can help fast track your progress.

Keep the following in mind with a mentor:

- Don't be afraid to ask someone to be your mentor. If they say 'no,' don't take it personally. Keep asking others!
- Set goals with your mentor on what you want to accomplish.
- Define expectations for both parties including how often you'll meet and the required commitment level.
- Be sure to work with someone that seems to genuinely want to help.
- Make sure your mentor has the time. Even if they want to help, they might be too busy to be an effective mentor.
- Work with your mentor on exploring the other steps in this guide.

#9. Build Relevant Soft Skills

Besides the technical knowledge, there are many soft skills that will benefit you:

Be an empathetic facilitator

One of the most difficult aspects of ICS/OT cyber security is getting IT cyber security professionals and ICS/OT team members to work together.

Look at cyber security from the other team's perspective and "build bridges" to where we are all on the SAME team!

Explore other skills

Active listening, problem solving, flexibility/adaptability, patience, cultural awareness, negotiation and integrity and others will only help you in the long run.

#10. Get Certified

Industry certifications cannot replace the need for hands on experience, but can help demonstrate the knowledge you have been building throughout your ICS/OT cyber security journey.

There are two main certification paths that are recognized the most by the ICS/OT community:

- ISA/IEC 62443 Expert Series
- SANS ICS Certifications

Other certification paths which are growing in recognition are available from other providers such as Exida and TÜV Rheinland.

NOTE: I have completed all of the ISA/IEC and SANS courses and exams, but do not have personal experience with any others.

ISA/IEC 62443 Expert Series

- The 62443 Standard from ISA/IEC is considered THE standard for securing ICS/OT environments.
- ISA / IEC provides a certification path of four courses.
- Once you complete all four courses, you become a certified ISA/IEC 62443 Expert.
- Courses are more designed to teach OT professionals cyber security.
- You must take each course before you can take the associated exam.
- Each course/exam costs ~\$2,000 USD.

NOTE: The courses do not make you an “expert” in 62443 or ICS cyber security, but can be a great starting point!



SANS ICS Certifications

- The SANS Institute is the world leader in cyber security education.
- SANS offers three ICS cyber security courses today created and taught by global thought leaders such as Rob Lee, Tim Conway and Justin Searle.
- Each course is independent and has its own focus.
- Courses are more designed for both IT cyber security and OT professionals.
- You do not have to take each course before you can take the exam.
- Each course/exam costs ~\$10,000 USD.

NOTE: I took the GRID course in-person with Rob Lee and found it was the most valuable course of my 30 year career.



Certification Resources

ISA 62443 Expert Series

rb.gy/ap3wa

SANS ICS Training

rb.gy/66a6y

Exida

rb.gy/ce758

TÜV Rheinland

rb.gy/1nmc1



The End (For Now...)

The journey into ICS/OT cyber security is not a simple path, but it is a very rewarding one.

As the world continues to become increasingly automated and interconnected, the number of cyber threats and attacks against ICS/OT networks only continues to grow.

There will be an ICS/OT cyber attack which results in catastrophic consequences.

And the world needs you to help prevent it!

Thank You for Reading!

Thank you for taking the time to read through this guide (or at least to skim it)! I hope you found it helpful in getting started on your journey into ICS/OT cyber security!

No matter where you live in the world, the global community needs you in helping to protect critical infrastructure and other specialized OT environments!

If you have any questions, comments or suggestions, please do not hesitate to reach out. I would love to hear from you!

Mike Holcomb

[linkedin.com/in/mikeholcomb](https://www.linkedin.com/in/mikeholcomb)

michael@utilsec.com

**COMING
SOON...**

GETTING STARTED IN INDUSTRIAL (ICS/OT) CYBER SECURITY

**For OT & Automation
Professionals**

Michael Holcomb

LIKE THIS?

- **SAVE**
- **REPOST**
- **FOLLOW**
- **CONNECT**



MIKE HOLCOMB
HELPING YOU SECURE ICS/OT