QuickStart Guide

For Manufacturers

MADE IN Missouri
FOUNDED IN 1966

PROUD TO BE A MISSOURI ASSOCIATION OF MANUFACTURERS partner!

CNC Machining Security

This guide is used in the design of security controls implemented around CNC machines and their networks. This guide is not a full step-by-step process for setting up security around CNC machines, but is to be used as a starting point to begin analyzing a client's network and facility to determine the types of controls needed for securing CNC machines.

ABOUT SSE

Systems Service Enterprises, Inc. (SSE) is a leader in Information Technology and Training solutions for small-medium sized businesses. A WOSB with 300 employees, SSE was founded in 1966 by Susan S. Elliott. SSE is headquartered in St. Louis, Missouri with a sister office in Jacksonville, Florida and is able to serve clients throughout all 50 states.

As an ISO 9001:2015 certified organization, SSE has not only the technical expertise, but the disciplined processes and business maturity to deliver customized best-in-class IT and cybersecurity solutions across several highly regulated industries. SSE has maintained our, and our customers' networks to various industry regulatory standards and protects data for ourselves and our clients. Established processes, standards and quality solutions allow SSE to meet the most complex challenges.

SSE is Certified as a Registered Provider Organization (RPO) by The CMMC Accreditation Body (CMMC-AB).

nqa. ISO 9001 QUALITY MANAGEMENT

CYBERSECURITY MATURITY MODEL CERTIFICATION CMMC-AB RPO REGISTERED

BACKGROUND INFORMATION

CNC, short for Computer Numerical Control, is the process for manufacturing through preprogrammed software that dictates the movement of factory machinery and tools.

These machines can be loaded with a variety of software to machine the part in production. These machines can be supported from a wide set of Operating Systems such as Windows XP, Windows 7, as well as proprietary Operating Systems from the manufacturer of the machine.

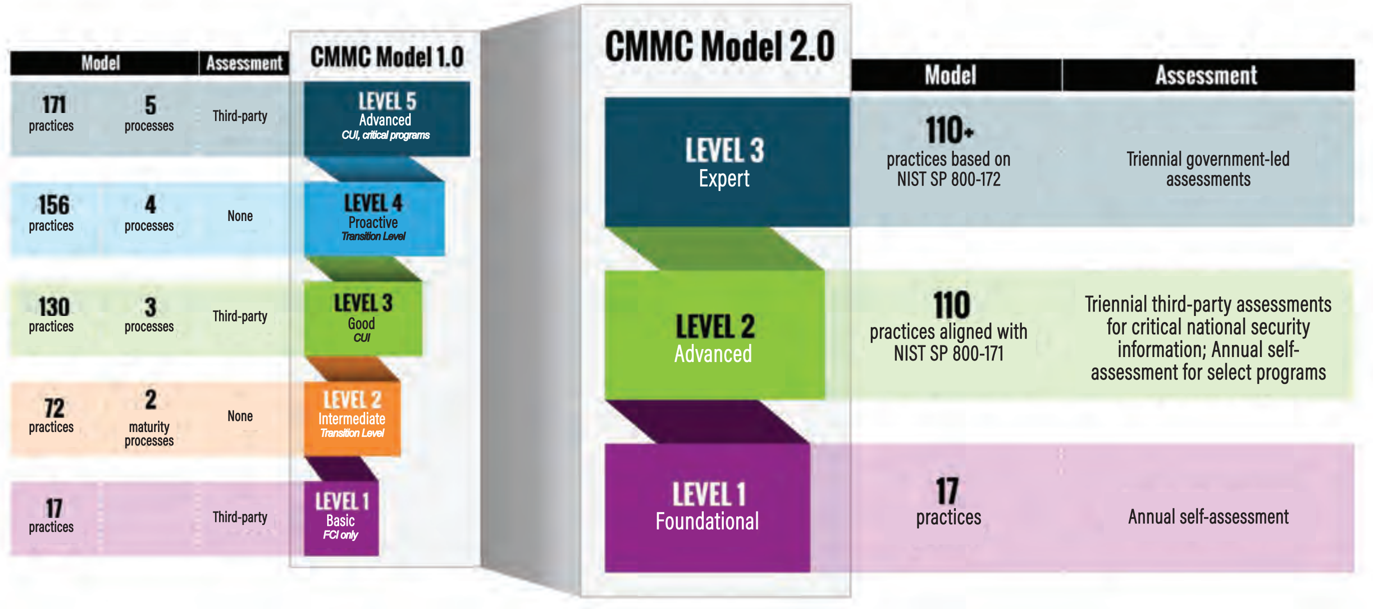
The CNC machine uses G-Code (Geometric Code) and M-Code (Machine Code) depending on the machine in use. These codes can be transferred to the CNC machine in a variety of ways including, but not limited to: USB, Floppy Disk, and/or LAN connections.

C
N
C

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Beginning now, more than 300,000 companies and subcontractors that conduct business with the U.S. Department of Defense (DoD) will have to certify—and potentially overhaul—their cybersecurity controls and policies to comply with CMMC or face a tremendous impact to their bottom line. In a recent **Security Management** article, DoD contractor and cybersecurity expert **SSE** outlined these challenges and how companies should plan to meet them.

Whether your organization works directly with the federal government or is a subcontractor, the requirements of the DFARS Interim Final Rule and the newly announced CMMC 2.0 guidelines apply. Failure to comply with these requirements could prevent future contracts, task orders or delivery orders awards. But, worse than that, failure to comply could bring litigation under the False Claims Act. Certainly, it's a position in which no company wants to find itself.



CMMC Model 1.0

Model		Assessment	
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

BEGINNING THE DESIGN PROCESS

To begin designing the security around the CNC machines in the shop, it is best to first understand how the machine works. This includes how the machine gets their G-Code and where the G-Code comes from.

It is crucial in the design process to understand the flow of data to best control and secure it. Knowing how this data moves will also help determine where limitations are in the data path.

For example, some machines may not support newer encryption types and may rely on older encryption or in some cases, no encryption may be supported.

Starting from the beginning, understanding where the G-Code comes from, and working to the end, how the G-Code is being imported to the CNC machine, is a good approach to designing security as certain sources for G-Code will dictate controls implemented down the line.

This process will help determine whether logical, physical or both logical and physical controls are needing to be implemented. Answer the following question; What is used to move the G-Code, is it some form of removable media or does it travel along a medium?

If the answer is removable media, work to narrow down the controls to be implemented. Is the removable media going to another system connected to the CNC machine or directly to the CNC machine?

This will provide a path to begin designing controls around the transfer of data which CMMC has outlined specific practices for, such as MP.L2-3.8.5 “Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas” and MP.L2-3.8.6 “Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.”

> *“Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.”*
>
> *SC.L2-3.13.8*

If the answer is a type of medium, begin looking at how the connection is made and secured. Using mechanisms such as Access Control Lists (ACL’s), port restrictions and certain firewall configurations will help in securing these machines from outsider threats while still providing functionality to perform day-to-day tasks.

Practices regarding transmission control can be referenced to aid in design. These practices include SC.L2-3.13.6 "Deny network communications traffic by default and allow network communications traffic by exception" and SC.L2-3.13.8 "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards."

While going down the path of logical controls, ensure that physical controls are also met for the CNC machines. Examining where the machine is located in the facility can assist with determining appropriate safeguards as well.

Begin thinking about personnel who may have access to the machine and whether or not this can be controlled. If the machine sits in an open room where all personnel could potentially access the machine, it may require more controls to be implemented to help mitigate the risk by using monitoring equipment such as surveillance cameras.

Practices within the Physical Protection (PE) domain can be leveraged for mitigating these risks as well. PE.L1-3.10.3 "Escort visitors and monitor visitor activity" and PE.L2-3.10.2 "Protect and monitor the physical facility and support infrastructure for organization systems" are practices which can be referenced during this section of design.

CONCLUSION

Building towards CMMC compliance needs to start with a foundational layer of best practices and an understanding of all aspects of your environment. The specific domains and steps discussed in this guide will assist manufacturers in getting started in the compliance processes. The following questions are important to ask and answer:

- ✓ Do you have newer machines with shared access by multiple employees with legacy or proprietary Operating Systems (i.e. Microsoft Windows XP,7)?
- ✓ Have you performed a case-by-case investigation on your business practices to determine the best course of action such as data transfer using encrypted removable media?
- ✓ Do you have network connected transfers with Access Control Lists in place to limit the machine's exposure to security threats?
- ✓ Have you disabled any non-approved network adapters?
- ✓ Do you have controlled access and monitoring of access to the machinery?

It is all about getting to a secure state to do our part in protecting sensitive information across the nation's Defense Industrial Base (DIB). The DIB as a whole is working through the same framework and resources are becoming more widely available each day.

Companies like SSE are available to help others to reach the end goal of protecting our businesses, customers and nation from enemies, both foreign and domestic.

SERVING OUR CLIENTS

We are proud of our outstanding client retention, with the average tenure of SSE clients being 8$^+$ years.

SSE has also been recognized for its proven performance by MSPmentor (501 Global List - five years running) and by St. Louis Small Business Monthly as a 6-time winner of "Best IT Firm" and a 3-time winner for ''Best In Customer Service."

All of which is made possible thanks to an expertly trained and knowledgeable staff dedicated to serving our customers and with certifications in our IT tools and security standards:

- 15 Certifications in our core technologies (Unitrends, Meraki, Kaseya, etc.)
- 14 Certifications in general IT competencies (A+, Net+, Dell, ITIL, etc.)
- 10 Certifications in IT/cybersecurity
  - o 3 Information Security Systems Managers (ISSM)
  - o 2 National Institute of Standard Technology (NIST)
  - o 1 Certified Ethical Hacker (CEH)
  - o 4 Facility Security Officers (FSO)
- 1 Project Management Professional (PMP)
- **2 Registered Practitioners (RP) by the CMMC Accreditation Body**
- **SSE has been recognized as a Registered Provider Organization (RPO) by the CMMC Accreditation Body.**

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

HOW CAN SSE HELP?

Schedule an initial CMMC Consultation

www.sseinc.com/nist

SSE®

☎ (314) 439-4769