COLIBRIUM ADDITIVE
a GE Aerospace company

Cybersecurity & Additive Manufacturing

The Chain of Trust: Securing Additive Manufacturing's Digital Future

Paul Leendertse, Senior Product Security Leader,
and Lars Bruns, Executive Software Leader, Colibrium Additive

Most modern manufacturing equipment uses computer processors and networks for control and monitoring. Additive manufacturing, or 3D printing, goes one step further. It prints parts directly from digital models that can be sent and stored anywhere in the world. This makes it the world's first fully digital manufacturing technology—and this is both its strength and its potential weakness.

First, consider additive manufacturing's strengths. The 2021 Department of Defense Additive Manufacturing Strategy called 3D printing "a factory in a box" because it is so flexible. Metal additive printers can provide design freedom to produce a wide variety of parts wherever and whenever they are needed, from supply depots and naval vessels to forward airfields and military bases. The report argues that additive manufacturing could enable more agile logistics, shortening supply chains, slashing time-to-use, improving maintenance and repair efficiency, and producing out-of-stock parts for legacy systems.

Now, consider its weakness: like all digital systems, it is vulnerable to cybersecurity threats and cyber espionage.

The chain focuses on three distinct sections

Section 1 — **Securely sourced hardware with secure boot and hardened operating system.**

Section 2 — **Applications, communication, and data.**

Section 3 — **Deployment environment, user access, and monitoring.**

Colibrium Additive (formerly GE Additive), in partnership with our customers, has developed a cybersecurity vision to address this challenge. This vision weaves together an array of interlinked best-in-class standards and proven security technologies to create a nine-level Chain of Trust.

— **9.** Patching and Updating

— **8.** Monitoring and Auditing

— **7.** Access Control

— **6.** Secure Communications

— **5.** Code Integrity

— **4.** Trusted Execution Environment

— **3.** Trusted Operating System (OS)

— **2.** Secure Boot

— **1.** Hardware Root of Trust

Colibrium Additive uses the **Chain of Trust** as a framework that enables a secure-by-design methodology that starts with hardware we purchase from thoroughly vetted vendors and is built into our machine architecture. With a secure hardware foundation, we create layers of security controls that present significant challenges to potential adversaries, from checking the startup boot sequence for tampering through to the operating system and applications that run and monitor the machine. Together, these layers provide a defense in depth approach that reduces the attack surface that adversaries may try to exploit against the additive system.

We believe this **Chain of Trust** vision represents a holistic and cohesive approach to maintaining the confidentiality of data, ensuring machine availability, and protecting both the integrity of the design and the printed part from tampering.

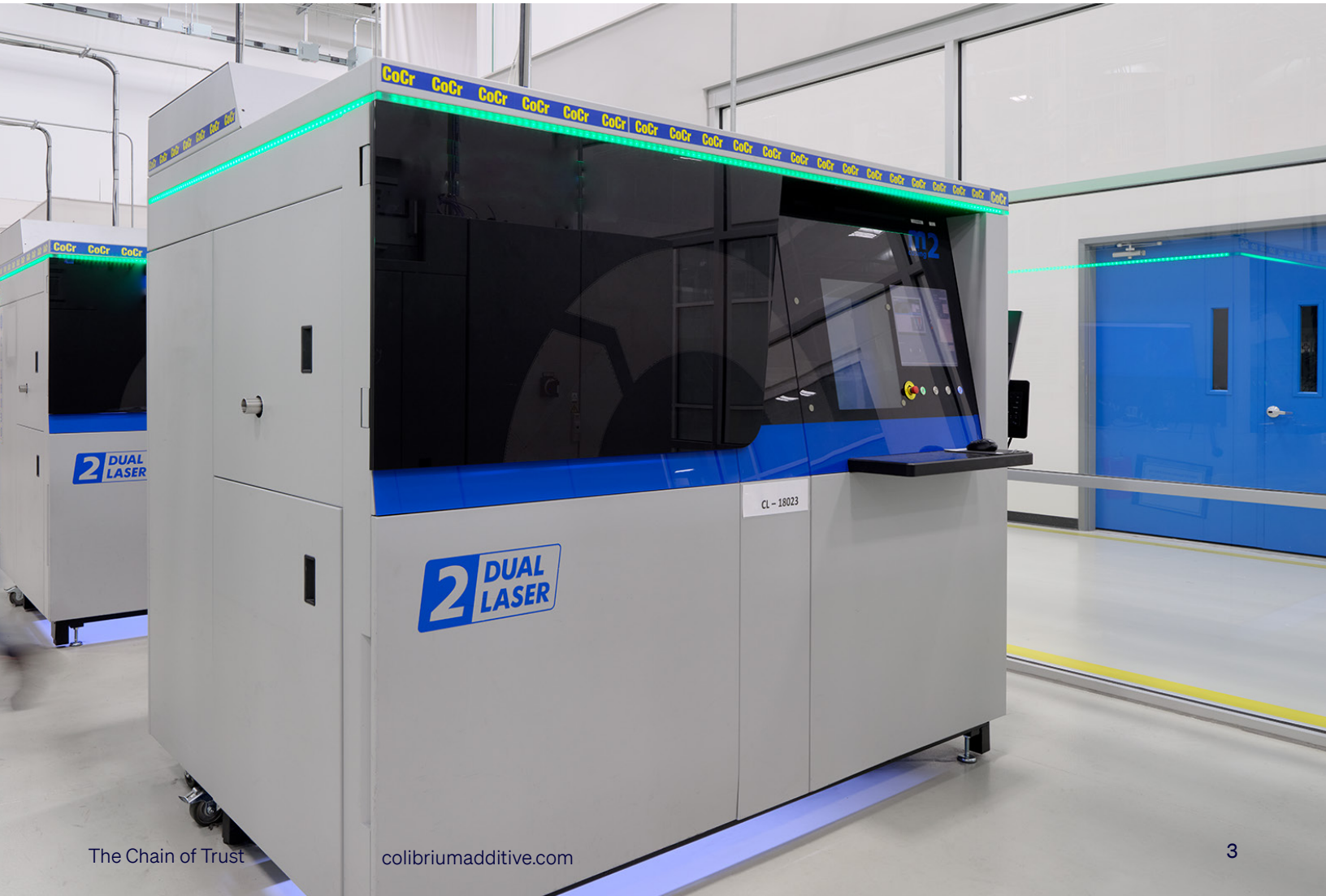
Yet, securing the additive manufacturing system will always remain a work in progress.

Cyberattacks come from a variety of threat actors who are continually evolving to find and exploit vulnerabilities in operating systems, applications, and hardware.

Colibrium Additive has made a substantial investment in seeking to protect our machine assets from these ever-morphing security challenges. We have developed a defined work process for building security into the additive manufacturing systems we develop (secure by design).

We also continue to work with the broader cybersecurity community to actively share information on threats and concepts to continually protect against, and adapt to, new threats. Our **Chain of Trust** vision is a collaborative approach to addressing areas of potential vulnerability and proactively designing protections against unknown and undefined future threats.

It starts with understanding our vulnerabilities.



The Challenge

Factory networks are not immune to attack. Historically, manufacturing sites have been a lower priority for cybersecurity investments, leaving them vulnerable and easier to attack. A simplistic approach to securing manufacturing sites included "air gapping" equipment inside the factory, isolating the machinery from business and corporate operations. This made it difficult to launch cyberattacks on production operations, although the use of USB media and the rise of insider threats have introduced additional attack vectors.

Over the past 20 years, however, industrial manufacturing corporations have embraced digital transformation and Industry 4.0 initiatives. This involves using digital technologies to capture data and manage business processes to improve performance, assure quality, and create new products and services.

This means leveraging machine sensors and analytics with linkages to corporate networks to boost awareness and support connected operations. These needs and opportunities conflict with a legacy "air gap" approach and can leave factories vulnerable to cyberattack if not properly secured and managed.

While corporate IT networks have undergone extensive investment in cybersecurity hardening and monitoring transformation over the past 20 years, many industrial operational technology (OT) manufacturing networks have not. In fact, corporations have often viewed factories as cost centers faced with operational expense challenges and pressures.

This made it difficult for factories to upgrade security and invest in important tooling and network segregation activities. It also explains why industrial facilities rank high among hackers' favorite targets.

As a result, industrial manufacturing cybersecurity systems face a threefold challenge:

1. To preserve the confidentiality of intellectual property
2. To protect the integrity of the design and finished parts
3. To ensure 24/7 system availability

These three challenges are often referred to as the cybersecurity CIA triad. Our additive industry is at the forefront of these challenges, with multiple opportunities to address and bolster them.

Confidentiality

Confidentiality involves protecting design geometry and other intellectual property (IP) from theft. This is especially true for additive manufacturing, since the process enables design teams to innovate on part design with unusual shapes and complex inner channels that allow for heat exchange and that cannot be produced by subtractive means.

Often, these complex parts play a significant and differentiating role in the performance of larger systems. This is certainly true for Colibrium Additive's parent company, GE Aerospace, a major producer of jet engines. Some of its designs leverage metal additive manufacturing to print components that disperse fuel and manage heat more precisely and with greater customization, improving engine fuel efficiency and maximizing thrust and performance, while also reducing maintenance costs

and emissions. Other designs consolidate and "light-weight" several or even hundreds of individual parts into a handful of components, slashing assembly times, and maintenance costs.

Consequently, these additively designed and manufactured parts give GE Aerospace significant advantages in the multibillion-dollar aerospace market. They constitute critical IP that must be protected from cybertheft.

Integrity
Integrity speaks to printing parts correctly, without alteration due to tampering, sabotage, or manipulation. This is especially critical in additive parts because printers build parts layer by layer. A complex aircraft engine heat exchanger, for example, may consist of thousands of layers. Maintaining digital integrity ensures parts are printed according to design intent.

Availability
Availability is an important metric in industrial production. Machinery is expensive and must remain in operation, sometimes 24/7, to meet monthly or quarterly production targets. This means securing the 3D printer against ransomware, viruses, and denial of service attacks that can lock down equipment and render it unusable.

Attackers

Additive manufacturing systems must fend off attacks from multiple types of cybercriminals. Examples include: individual hackers looking for quick news cycle prominence, well-funded criminal enterprises seeking financial ransomware gains, and nation-state-sponsored actors focused on stealing IP and eliminating capability. Each type of attacker presents distinct types of challenges.

Opportunistic attacks
Individuals with basic hacking skills tend to conduct opportunistic attacks. Often, this takes the form of emails with attachments that, once clicked, infect PCs and laptops with ransomware. Once infected, the hacker typically demands payment in untraceable cryptocurrency.

This type of attack can spread through networks, especially those that are not well protected, monitored, and segregated from one another. Someone in an office, for example, who clicks on a personal email attachment and infects their laptop, may log onto a factory network to check metrics or order status. This could allow a ransomware virus to spread to the industrial network and infect new machines. Proper cybersecurity hygiene, such as employee training (to recognize threats), spam filters, segregated networks, and labels indicating attachments from outside sources can help deter these low-level attacks. Additionally, advanced firewalls and allow-listing software can help to mitigate these threats.

Targeted attacks
Criminal ransom organizations go after defense contractors and other targets with deep pockets. They are not just interested in locking down your system for a big payday. They understand the value of your IP and want to steal and resell it. These perpetrators pose a significant data and IP exfiltration threat to larger organizations and include professional and organized crime groups in North Korea, Russia, Iran, and China as well as the United States and Europe.

Advanced Persistent Threats (APTs)
Nation-state hackers work for national security organizations or with them. Their goal is to access closely guarded data, intelligence, and critical IP from other countries. They may also engage in cyberespionage and practice access testing without detection. Among the better known of these organizations are Russia's Cozy Bear and Fancy Bear, China's Double Dragon (Cicada), North Korea's Lazarus Group, and Iran's Helix Kitten.

These advanced persistent threats (APTs) get their name for a reason. Unlike other hackers, APTs have the funding and resources to spend as much time as necessary to achieve success. They will identify specific objectives, then spend months or even years working their way through layers of cybersecurity countermeasures to access their target.

Forging a chain of trust

The concept behind the Chain of Trust is simple: focus on layers of security, from the hardware up through the tech stack, to make it as difficult as possible for hackers to breach the additive manufacturing system. While prevention of successful attacks is the main objective, Colibrium Additive systems can be integrated with customer Security Information and Event Management (SIEM) tools to help with early discovery of intrusions. Through these integrations, customer security teams can possibly stop or divert the threat and use audit trails for investigations and lessons learned.

Developing a Chain of Trust that interlinks hardware and software components sounds like a straightforward task. It is not. The security system has to guard against an incredibly varied range of cyber—and physical—attacks. Some attacks might originate from within the IT, or even the factory OT manufacturing networks.

Colibrium Additive's Chain of Trust provides the framework to guard against scores of similar scenarios, cyber and physical, and do it without impacting the usability of the machine. It took years to develop a conceptual approach that could reduce the risk that all these evolving possibilities pose to the additive manufacturing system.

Colibrium Additive's **Chain of Trust** can be divided into three distinct sections:

1 Hardware and OS

A **Chain of Trust** is only as good as its hardware and operating system. We build on electronics from trusted vendors that includes hardware-embedded cryptographic keys with anti-tamper features to support a secure system boot sequence.

2 Application layer

The next three links involve applications. This includes a trusted execution environment, data encryption at rest and in transit, as well as ways to ensure code integrity, and secure communications.

3 Deployment

The final three links support printer user security and integration into customer environments. They include use access control, monitoring and auditing, as well as patching and updating.

Hardening hardware and OS

Let us consider the hardware and OS links.

Hardware root of trust
Every Chain of Trust begins with a root of trust, a source that can always be trusted in a cryptographic system. We then extend this root of trust throughout the printer's hardware and the applications it hosts.

The embedded key also supports encrypted data storage and retrieval. If someone tried to remove the hard drive, he/she could not decrypt the data on it due to the use of a Trusted Platform Module (TPM) and keys from other printer specific hardware.

Secure boot
When a computer starts up, it goes through a sequence of steps that load the operating system and other critical software into memory from the hard drive.

Colibrium Additive printers with secure boot are designed to load only trusted and validated industrial operating system (OS) and software components into memory.

Our printers use firmware-enabled cryptography to verify the integrity of each step of the boot sequence.

The BIOS transfers control only to those components that have received positive confirmation of their authenticity. If there are any discrepancies, the system will not boot. This keeps someone with physical access to the machine from swapping out or altering the system's BIOS, and, say, giving orders to slowly move data from the machine to some unauthorized destination.

Trusted Operating System (OS)
Most cyberattacks target operating systems. Once in, a hacker can freeze a system with ransomware, steal data, or sabotage an operation. Hackers are constantly probing for vulnerabilities, and new ones turn up all the time. It takes multiple layers of defense to keep them out.

Colibrium Additive bases its industrial operating system on Microsoft Windows which is further hardened to optimize security features while decreasing the attack surface. Based on the Department of Defense Federal Security Technical Implementation Guide (STIG), Colibrium Additive has boosted that score to well above 90 (STIG level GREEN).

Application layer

Application layer links on the **Chain of Trust** cover execution environment, code integrity, and secure communications.

Trusted execution environment
Trusted execution builds on a secured operating environment and has two elements. The first is full disk encryption. All software and digital models are fully encrypted and unencrypted using a hardware-embedded key, only when loaded for processing.

The second element is allow-listing, which specifies exactly what software programs the OS is allowed to run. If someone tries to slip in malicious executables, it will not run because it is not on the allowed list. There are several third-party applications for managing allow-lists. Colibrium Additive has evaluated several leading programs to verify that may run on the printer without interfering with its operation.

Code integrity
Original equipment manufacturers (OEMs) use digital signatures that ensure the authenticity of their system BIOS, firmware, and application software. Colibrium Additive works with hardware vendors to allow only digitally signed and authenticated firmware to run on the system.

Advanced digital signing works with data encryption to protect against smash-and-grab data attacks. Colibrium Additive is also working on research programs that will comply with the National Security Agency's Commercial National Security Algorithm (CNSA 2.0) Suite, which is used to guard top-secret information. CNSA 2.0 is the first system designed to protect against today's advanced cyberattacks and quantum computers capable of decrypting conventional security algorithms.

Secure communications
One of additive manufacturing's greatest strengths is its ability to respond to unexpected needs by downloading a digital model and printing a part. This involves transferring digital files. To ensure security, Colibrium Additive encrypts and secures data transmission to components within its printers and over networks used to transfer files to and from the machine. This double layer of encryption reduces the risk of unauthorized disclosure or modification of data.

To do this, Colibrium Additive has embedded Materialise's Identify3D Suite into its WRX program. This software provides digital rights management and encrypts, distributes, and traces digital parts for authenticated and authorized users, as they move between traditionally segregated manufacturing networks and interlinked business and military IT networks. Another solution is a secure file transfer mechanism that encrypts files and adds constraints so that they will print only a certain number of parts on a specific printer or expire after a defined date.

Deployment

The final three links in Colibrium Additive's **Chain of Trust** support secure access control, monitoring and auditing, and patching and updating. Although these are customer responsibilities, we follow the guidance of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which encourages OEMs to take ownership of customer security outcomes. We provide tools that enable users to manage these links.

Access control
All enterprise networks use a combination of restrictions and permissions to control who is allowed to do what. On an industrial network, for example, only authenticated users may be allowed to send a model to a printer or view printer analytics. It may require a different level of permission to edit a digital model. Access control also ensures all actions are auditable.

There are many third-party identity systems to manage system access. Colibrium Additive has assessed and validated several leading solutions to ensure they fulfill their mission without interfering with printer operation.

Most manufacturers already manage access on corporate networks. Colibrium Additive is ready to advise companies on how to harden their industrial networks, manage its interface with corporate networks, and ensure the **Chain of Trust** extends to their own critical suppliers.

Monitoring and auditing
Most hacks happen in digital time, before a human could respond. Defense in depth seeks to present enough security layers to slow cyberattacks down to human time. This enables the system's integration with security information and event management (SIEM) tools to log, monitor, detect, and alert our customers' security professionals. Once the SIEM flags security events, anomalies, unexpected access, or data movement, security teams can intervene to prevent disruptions and slow their proliferation through the network. Auditing tools also enable security professionals to analyze successful exploits and prevent them in the future.

We have evaluated several leading SIEM agents to ensure they work properly with our printers and that all alerts go to a centralized location for analysis and alerting.

Patching and updating
Software is always evolving. Industrial operating systems add new features. Security software evolves more capabilities. Changes to software require a secure process to manage the patches and updates needed to keep software current.

Colibrium Additive validates relevant Windows updates and patches on its own systems first. We do this by installing them on our printers and testing to ensure the printers still function as intended, including performance benchmark testing. We also test our own code for bugs and vulnerabilities as part of our continuous build infrastructure. Printer operators can then install updates to remove bugs, improve security, and add new features.

Future-proofing security

We believe our nine-link Chain of Trust represents today's state of the art in industrial digital security. Yet, it is not enough. Threats are constantly evolving, especially threats from advanced persistent threats (APTs).

A cybersecurity system that appears 100 percent secure today may hide a vulnerability that will be discovered the next day and another the day after. Therefore, the best security solutions include a defense in depth that stops or slows attacks at every link in its Chain of Trust—while constantly evolving to meet future threats.

How can cyber defenses evolve? We believe this starts with a Software Development and Security Life Cycle (SDSLC) approach and a secure-by-design mindset, which incorporates best practices for secure software, hardware, and application development. It builds on such well-known industry standards as IEC 62443 and NIST 800-171, 800-82, and 800-53, which define cybersecurity for IT networks, for industrial control and automation systems, and cover regulations **such as NERC Critical Infrastructure Protection (CIP),** which addresses monitoring and managing America's electrical grid. It also builds on multiple Department of Defense cybersecurity standards.

We have built these best practices into our own Software Development and Security Lifecycle (SDSLC) that is integrated into our quality management system. This set of procedures, which leverage updated tooling and automated testing, clearly defines how to integrate security into our formal design review process in ways that generate measurable capabilities and deliverables into the final product.

Among the key tasks in Colibrium Additive's SDSLC are:

Base Security Requirements
Setting security requirements. Development teams follow a defined set of security requirements that are audited during design reviews.

Threat modeling
Using Microsoft's STRIDE model, our software architects identify and mitigate threats early in development. STRIDE refers to the broad range of threats, including spoofing (using someone else's authentication data), tampering (modifying data or communications), repudiation (performing illegal actions without leaving an audit trail), information disclosure (exposing data), denial of service (overwhelming servers to keep out legitimate users), and elevation of privilege (gaining administrative access to a system).

Rapid security assessment
Using a "Red Team" of authorized hackers to review the proposed software solution and identify security gaps early in the development process.

Security testing
Developers often combine proprietary and open-source code to create applications. We use static application security testing (SAST) to check for vulnerabilities early in proprietary code development and software composition analysis (SCA) to scan for security gaps in open-source software.

Penetration testing
One of the best ways to ensure software security is to attack it. We use hands-on Red Team experts and the latest hacking methods and techniques to ensure application quality.

In Summary

Internally, we call our methodology “hygiene.” It is part of our daily routine, like washing our hands before dinner or brushing our teeth at night. By treating security like hygiene, we make it easier for our printers and their industrial operating systems to scale security solutions to keep up with evolving threats. And we continuously learn from ongoing security testing and audits of hacks on existing systems.

It is as much a part of our development process as improving the speed, capacity, and print quality of our additive equipment. Only with a secure-by-design mindset can we ensure that additive technology delivers on its promise as a paradigm-breaking factory in a box.

Visit **www.colibriumadditive.com** and contact us to discuss your cybersecurity strategy.