SIEMENS

Ingenuity for life

Siemens PLM Software

Data protection in the digital thread

A Siemens and Identify3D perspective

Executive summary

The Siemens and Identify3D technology suite protects confidentiality and integrity of data in the digital manufacturing thread, providing intellectual property protection, manufacturing repeatability and traceability to counter constantly evolving cybersecurity threats.

www.siemens.com/plm

Introduction

With the emergence of digital manufacturing through initiatives like Industry 4.0 and the Internet of Things (IoT), tools used for design, engineering, production and process control are now linked together digitally. The ability to share information in a digital thread has led to advances in collaboration, efficiency and cost reduction throughout the product lifecycle. However, the digital connectivity required between systems and software in the digital thread has exposed the digital manufacturing ecosystem to an abundance of cybersecurity threats.

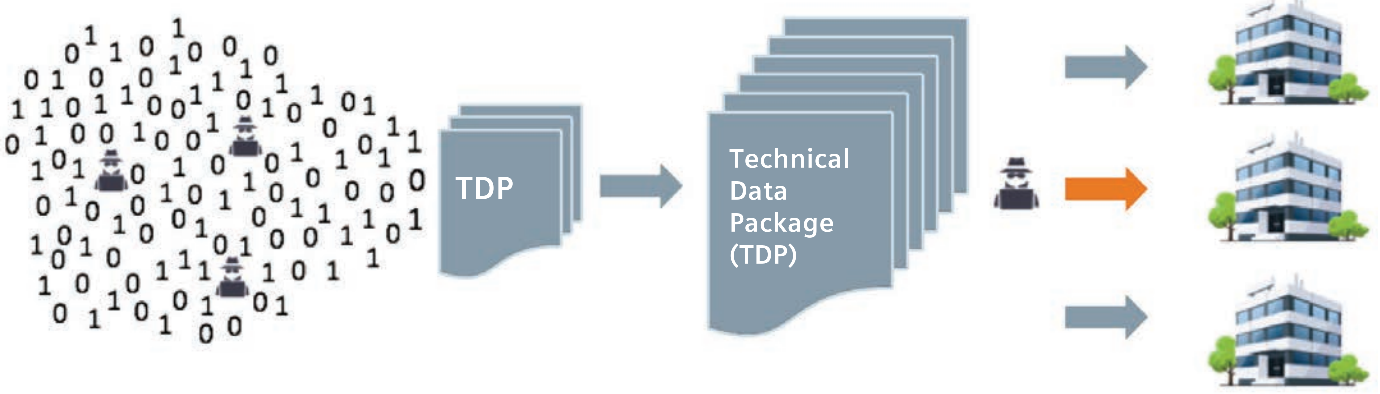
On the design and engineering side, computer-aided design tools like NX™ software from Siemens PLM Software allow for design, simulation, and visualization of individual parts, assemblies and even manufacturing processes. Often, many different tools are utilized in the design process, each requiring interoperability with the other tools in the thread to maximize efficiency.

On the production and manufacturing side of Industry 4.0, many of the devices and machines used in the production flow are capable of receiving and sending digital information to drive the operation of the device or machine, all while still reporting on the data collected during the process. Over the last few decades, computer numerical control (CNC) machines have utilized G-code files to direct the automated sequence of machine control commands. Additive manufacturing (AM) has taken digitization a step further with the ability to simultaneously create a whole array of parts defined by a digital package of information. Meanwhile, sensors and smart devices embedded in machines are collecting massive amounts of data.

Product lifecycle management (PLM) systems and collaboration platforms, like the Teamcenter® portfolio from Siemens PLM Software,[1] are designed to handle the integration of data between enterprise resource planning (ERP), manufacturing operations management (MOM) and electronics design automation (EDA) systems and the accumulation of digital information created by each system in the digital thread. Additionally, PLM systems can link together the design and manufacturing systems to allow sharing of digital information between the two traditionally disconnected business operations.

Data collection systems, like Siemens MindSphere, are allowing companies to collect the wide array of digital data generated by Industry 4.0 and the IoT. With the analytics capabilities built into the data collection systems, customers now have a much deeper understanding of their process flow.

For additive manufacturing, the Siemens Additive Manufacturing Network provides design consultation services and functions as well as manufacturing services for on-demand production. Distributed manufacturing platforms such as this are enabling companies to access production capacity for functional prototypes and serial production parts.



Technical data package

The data set shared between these various systems in the digital thread is often referred to as a technical data package (TDP). With so many integrated tools and devices from design through manufacturing, the size and complexity of the TDPs exchanged between systems is growing exponentially. These increases in applications and systems are driving more complexity in the interface of systems in the digital thread in order to support interoperability between those systems.

Although PLM systems can help manage the TDP of a part, there is still a digital interface required between systems, especially when data is shared by many different companies. This push for interoperability and complexity in digital interfaces is creating massive vulnerabilities for cybersecurity attacks. According to IBM Security, in 2016, 74 percent of cybersecurity attacks on manufacturing systems involved attempts to inject attack vectors at digital interfaces.

Attacks on manufacturing systems may involve the theft of IP. For example, ThyssenKrupp, a German steel and manufacturing plant producer, had their design IP stolen in 2016.[2] According to *Manufacturing Business Technology*, 21 percent of manufacturers have suffered a loss of IP from cyber-attacks.[3] In other cases, attackers have targeted physical destruction of equipment, as in the case reported by the German Federal Office for Information Security (BSI) in which attackers caused a blast furnace in a steel plant to overheat.[4] Also well publicized was the Stuxnet[5] worm that targeted the Iranian nuclear program. In addition to IP theft and physical destruction, attackers have the capability to alter physical parts as detailed by researcher L. D. Sturm, and others.[6] Cybersecurity Ventures predicts that global cybercrime costs will grow from $3 trillion in 2015 to $6 trillion in 2021.[7] In recent years, ransomware attacks have been responsible for shutting down several manufacturing facilities for days at a time.

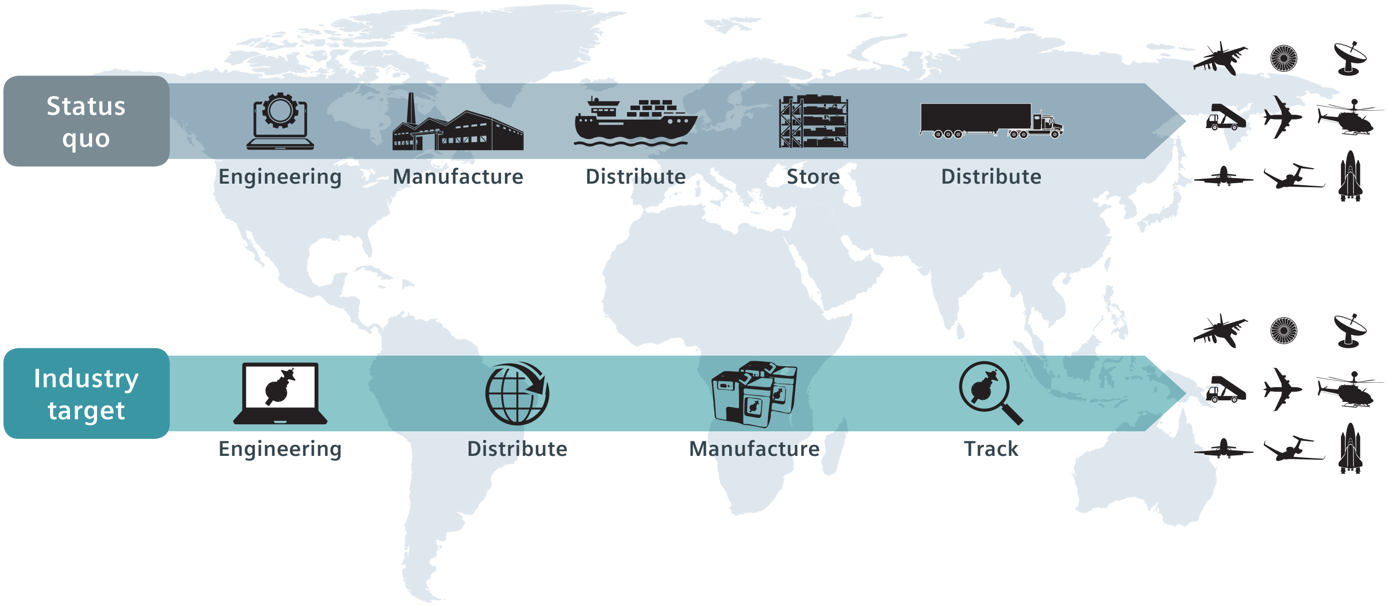
> *"Manufacturing is the most targeted industry for ransomware attacks."*
>
> *Carbon Black*[8]

As cyberattacks increase and the complexity in manufacturing systems and distributed supply chain networks grows, the difficulty of security in the digital manufacturing ecosystem will only increase over time. Cybersecurity Ventures estimates more than $1 trillion will be spent cumulatively over the next five years, from 2017 to 2021.[9] Traditionally, cybersecurity defenses have focused on protecting logical and physical access to devices as well as safeguarding individual devices from exploitation. Certainly, these methods are valuable, and if executed properly will provide very strong defenses. However, the nature of the digital manufacturing thread requires interoperability and communication between devices and systems in different physical locations that are often owned by different entities. A better solution is needed that focuses on the central challenge of protecting TDPs within the digital thread.

This white paper describes a new technology for protecting TDPs in the digital manufacturing thread. The Identify3D application suite protects the confidentiality and integrity of the TDP from creation at the design center to production on the manufacturing device, providing IP protection, manufacturing repeatability and traceability for digital manufacturing. By focusing on protecting the TDP, customers can be assured that their data is protected as the TDP flows between different systems with different owners and varying degrees of cybersecurity protections.

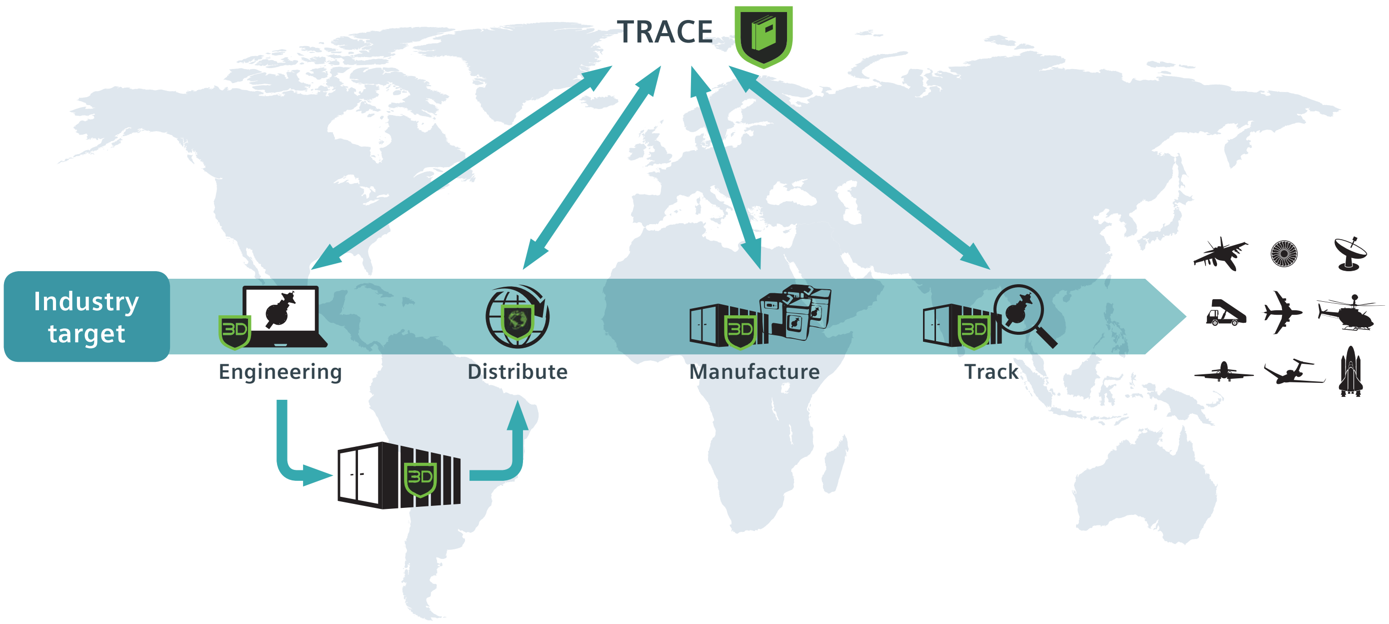
A new solution for data protection in the digital thread

The digitization of manufacturing requires us to rethink our supply chains. Traditionally the supply chain has focused on moving physical items in boxes and containers, but today these physical items have a long and complex digital life that requires data to be moved and managed before physical parts are created. However, there are analogies to the physical supply chain that can be used in the digital thread. The creation of the shipping container helped revolutionize global trade by allowing goods to move easily from warehouses to ports to rail to trucks and eventually to stores. In the digital thread, the TDP must make a similar journey within the digital workflow. The same way a standardized, secured physical container revolutionized the exchange of goods enabling easy and cheaper transit between shipping systems, likewise a digital container must allow for seamless interoperability between applications in the digital thread.



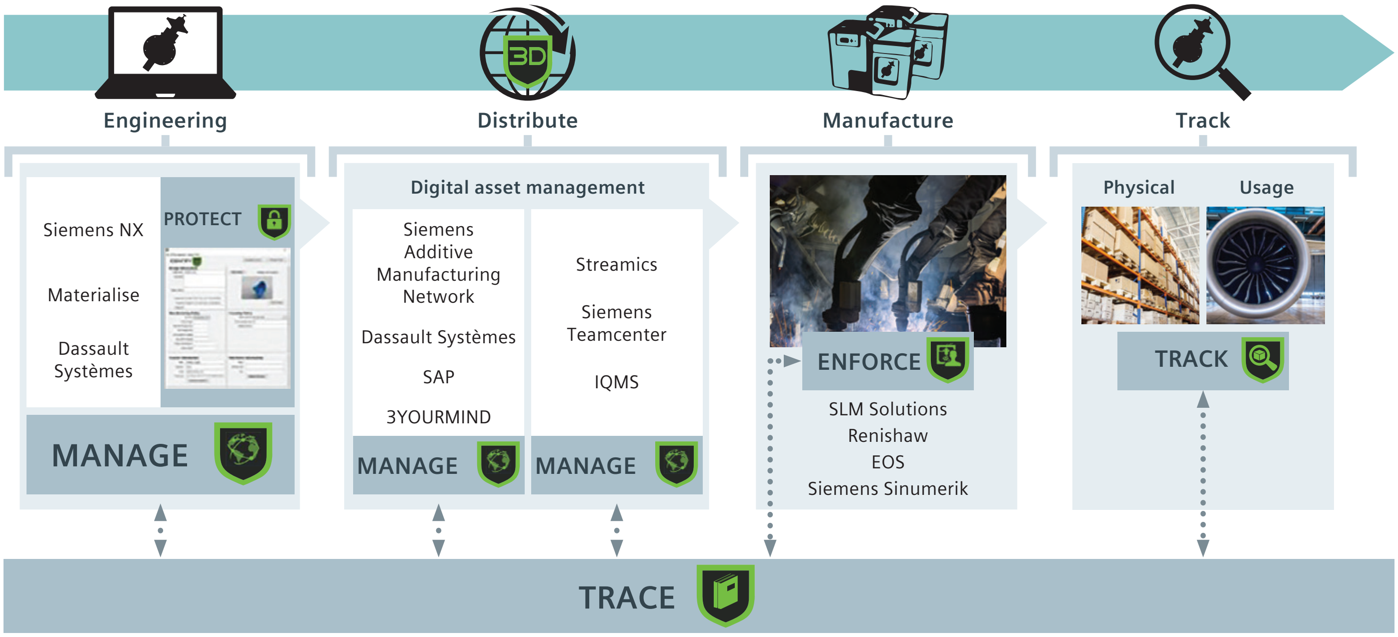
Digital thread

The Siemens and Identify3D ecosystem provides for a secure digital container to move the TDP through the digital workflow. With this solution, interoperability is maintained while enabling full protection of the TDP. No special storage repositories or secure transmission methods are required for the digital container.
The Identify3D Protect™ application creates the secure container while Identify3D Manage™ enables distribution and licensing policies to be created for the usage of the TDP within the container. Through integration with manufacturing devices, Identify3D Enforce™ allows applications and devices to access the TDP based on the licensing policy defined for the container. As the secure container moves through the digital thread, Identify3D Trace™ records all transactions, while Identify3D Track™ links the physical part ID to its digital twin. All these elements are integrated into the Siemens Digital Factory toolset, from CAD, computer aided manufacturing (CAM), and additive manufacturing software applications to machine controllers.



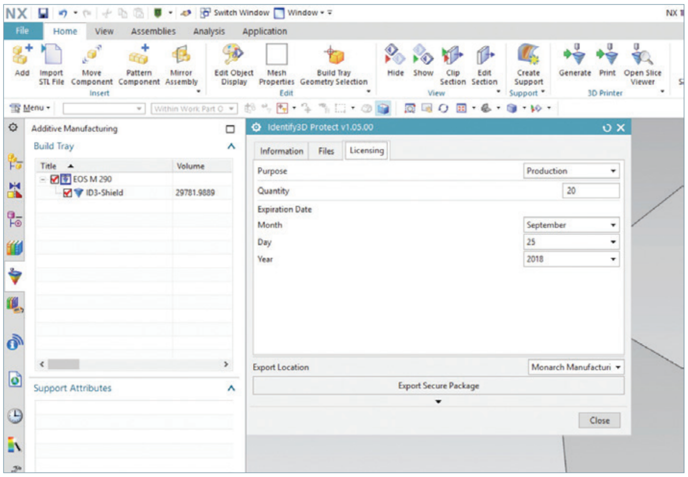
Digital thread – the solution

Identify3D Protect enables industrial designers to store CAD/CAM and AM files used for digital manufacturing in an encrypted digital container, called a Digital Supply Item (DSI), which is digitally signed and coupled with business and production rules. All digital files incorporated in the TDP can be securely stored in the DSI once the package is ready for production. Rules of production and other specifications unique to the original design will be used to create a license for the DSI. Once all aspects of the design are finalized, the files are securely encrypted and digitally signed, and the DSI container is transferred to a digital storage system awaiting distribution and production while the digital license is transferred to Identify3D Protect. Since the DSI container is encrypted and digitally signed, there are no security requirements on the digital storage and distribution of the DSI.



Identify3D ecosystem

Direct integration of Identify3D Protect with NX allows the user to create the encrypted DSI containing CAD files, AM build files or CAM postprocessed files. This integration provides a seamless user experience, as all package names and file descriptions are automatically pulled into the Protect module. Additionally, the registration with downstream Identify3D Manage can be performed directly within NX.



Title	Volume
EOS M 290	
ID3-Shield	29781.9889

Purpose: Production

Quantity: 20

Expiration Date

Month: September

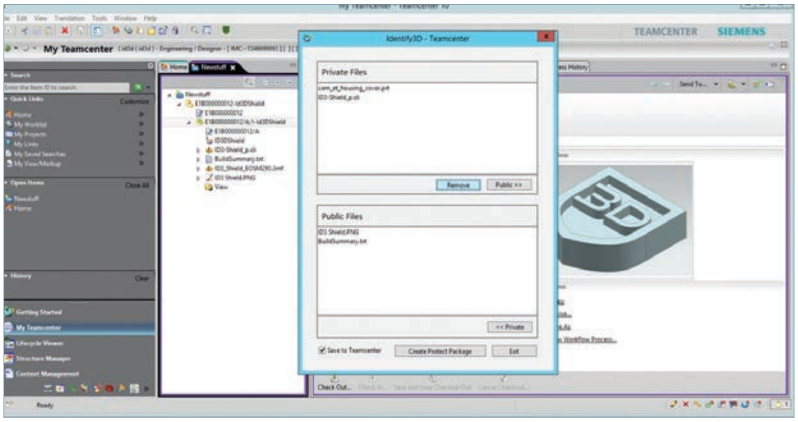
Day: 25

Year: 2018

Export Location: Monarch Manufacturi

Identify3D Protect working directly in Siemens NX

For users of Teamcenter, the Identify3D Protect plug-in can be accessed directly, allowing the user to create the secure DSI container from files within a Teamcenter item revision. Once the DSI container is created, it can then be stored in Teamcenter or sent to a downstream asset storage system, such as the Siemens Manufacturing Execution System (MES).



Identify3D Protect working directly in Teamcenter

When Identify3D Manage receives a license from Identify3D Protect™, a new order is created, which allows the user to facilitate secure and accountable digital distribution. The user has the ability to assign distribution and manufacturing rights of the DSI to any digital distributor or digital manufacturer. In essence, the operability of the DSI within any system can be securely controlled based on the user, the owner of the system, or any digital property associated with the system. When distributing orders, Identify3D Manage™ has the ability to limit the parts producible by the licensee. The Identify3D Manage application is provided in customized forms for engineering, distribution, and manufacturing.

For example, the Siemens Additive Manufacturing Network will work in the distribution mode. An instance of Identify3D Manage will run as part of the network, managing parts as they come in as production orders and go out to manufacturing. This ensures that a customer's data is securely managed within the Siemens' Additive Manufacturing Network as these steps of the additive manufacturing workflow are executed.

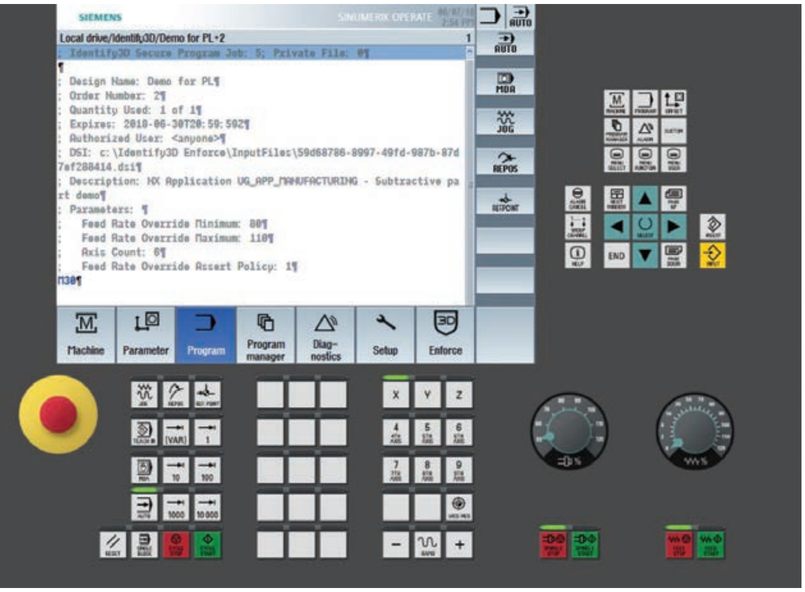
The specific manufacturing machine required to produce the part can be specified according to a make, model, or even individual machine. Any digital parameter used to control the manufacturing of the part can be constrained to a range or value. Any qualifications or certifications associated with the device that is required to assure consistent reproducibility can be specified by the license. The Siemens-Identify3D ecosystem allows complete control over the manufacturing systems allowed to produce by parts, thereby assuring the IP owner of consistent quality.

Strict identity management control is supported as part of the Identify3D license policy. This gives the customer the ability to require that parts be produced only by licensed users defined individually or through groups, roles, or certification status. Not only does this policy allow customers to be assured that users of systems in the digital thread are authenticated by the localized identity management system, but it also gives the customer the ability to require specific users with the right qualification to have access to use the protected files in the DSI on the defined manufacturing system.

Once digital distribution is complete and the part is ready for production, Identify3D Manage will license a manufacturing device that is embedded with the Identify3D Enforce application to produce the part. Identify3D Enforce ensures the security and integrity of the design during production, through verification of the license, the machine settings, and the user and the integrity of the DSI. Only when full verification is complete will the DSI container be decrypted by Identify3D Enforce and the licensed files be provided to the machine controller for manufacturing.

As the part is produced by the manufacturing device, Identify3D Enforce will continually monitor the process to assure that all protected settings and parameters are still within licensed values and ranges. Additionally, the total quantity of parts produced by the device will be tracked, and Identify3D Enforce will assure that no more than the maximum license quantity of the part can be produced by the device.

As of June 2018, Identify3D Enforce is integrated into Siemens SINUMERIK 840D sl CNC controllers to provide a seamless user experience for loading a secure DSI container with encrypted G-code files.



```
; Identify3D Secure Program Job: 5; Private File: 0¶
¶
; Design Name: Demo for PL¶
; Order Number: 2¶
; Quantity Used: 1 of 1¶
; Expires: 2018-06-30T20:59:59Z¶
; Authorized User: <anyone>¶
; DSI: c:\Identify3D Enforce\InputFiles\59d68786-8997-49fd-987b-87d
7ef288414.dsi¶
; Description: NX Application UG_APP_MANUFACTURING - Subtractive pa
rt demo¶
; Parameters: ¶
;   Feed Rate Override Minimum: 80¶
;   Feed Rate Override Maximum: 110¶
;   Axis Count: 6¶
;   Feed Rate Override Assert Policy: 1¶
M30¶
```

Identify3D Enforce integrated into Siemens SINUMERIK 840D sl

Best practices in cybersecurity for manufacturing are outlined by the NIST SP 800-82 publication10 and the IEC 62443/ISA-99 standard.[11] Generally, these involve specifying the important and most vulnerable equipment in a manufacturing site, assigning security levels based on the level of protection required and creating zones of isolation. Additionally, standard cybersecurity practices for individual systems apply, such as keeping software patches up to date, creating audit trails, restricting access, implementing appropriate anti-virus and file integrity checks, and disabling unused ports. Continuous monitoring of systems is important as well, especially if the intrusion is detectable.

Encrypting data at rest is also recommended as a best practice. Certainly, encryption is a very important aspect of data security; however, in order to preserve interoperability between systems in the digital thread, the data must be decrypted at the interface between systems, which introduces a point of vulnerability. Identify3D solves this problem by allowing the encrypted data in the DSI to pass between applications. The encrypted data can then only be decrypted in its plain text form when accessed by the Identify3D Enforce application embedded in a manufacturing device.

Traditionally the most complex issue with encryption systems is managing and safeguarding the required cryptographic keys. The majority of encryption failures is due to poor protection of keys. There are several methods available in the industry to protect cryptographic keys including hardware security modules (HSMs), smartcards and trusted platform modules (TPMs). Based on the security level requirement by the customer, Identify3D will support any of the industry standards for cryptographic key protection including using the Federal Information Processing Standard (FIPS) or Common Criteria-certified devices. Each Identify3D application that utilizes cryptographic keys will have the capability to access those keys from a hardware-protected source.

Implementing the Identify3D ecosystem does not eliminate the need for following the best practices for cybersecurity in manufacturing; rather, following the best practices will enhance the Identify3D level of protection. With a best-practice implementation, the weakest points are the interoperability requirements and threats associated with insiders. Identify3D allows interoperability with encryption, and with the TDP encrypted in the DSI, there is no opportunity for an insider to have access to the TDP anywhere in the digital thread. The Identify3D application suite focuses directly on protection of the TDP to assure confidentiality and integrity of the TDP throughout the digital thread.

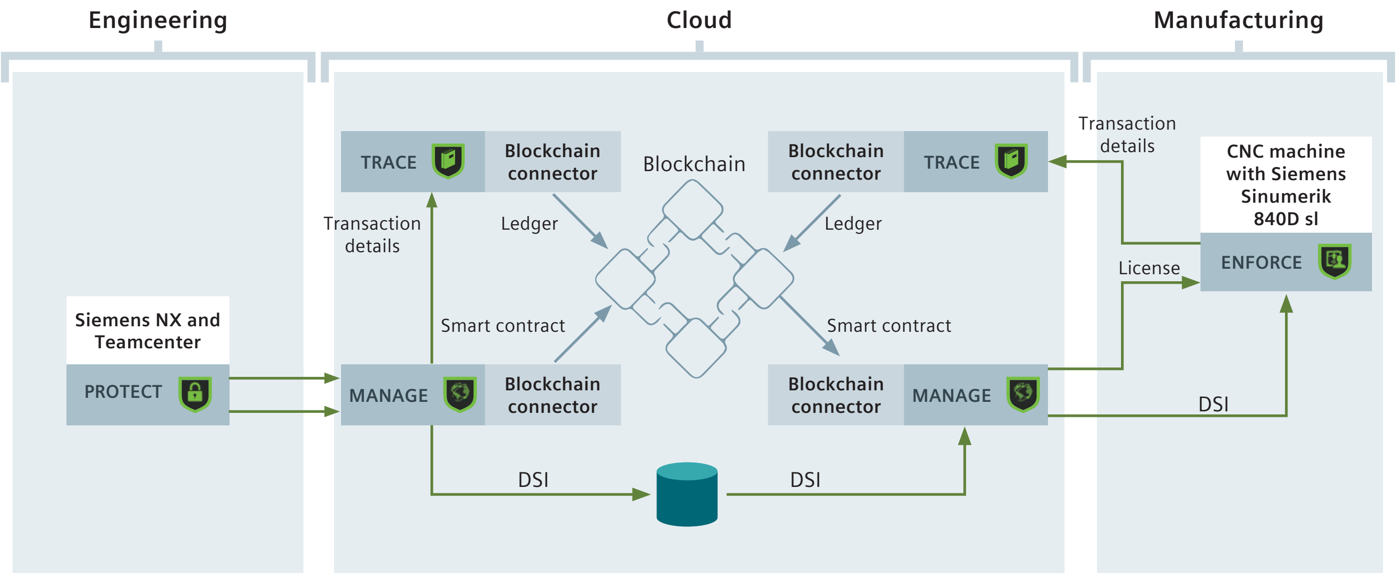
In addition to securing IP and preserving quality within the digital thread, the Identify3D technology will also securely store all operations and transactions of that IP. Identify3D Trace stores a record of each digital transaction involving the DSI. This will allow for an audit record for the digital manufacturing and distribution of each TDP. All data stored in the transactions are encrypted and can be accessed by entities involved in the digital manufacturing of a TDP, at the discretion of the IP owner. When a physical part is manufactured, the identifying number of the part will be recorded by Identify3D Track and added to the Trace ledger providing a link between the digital and physical thread. Additionally, this secure data stored by Trace can be provided to the Siemens MindSphere system or other digital data collection systems for retention.

Blockchain

Blockchain technology can replace centralized and proprietary databases with a decentralized open data repository. Within a blockchain, each participating node can add to the ongoing and constantly updated shared ledger. The shared ledger has strong cryptographic integrity protection that preserves the entire recorded history of transactions within a given blockchain. Additionally, each node can vote on the authenticity of any transaction and reject those transactions that are fraudulent. The decentralized nature of the blockchain means that no single company will have ownership or undue influence on the data recorded in the ledger.

Since each of the Identify3D applications is executed on independent nodes, implementing the Identify3D ecosystem within a supply chain blockchain is straightforward and does not require alterations to the core Identify3D technology. There are several implementations that are feasible, depending on the specific blockchain technology being utilized. For a more complex blockchain like Hyperledger Fabric that allows digital contracts, the entire digital license created by Identify3D applications can be stored in the blockchain and the digital contract can be utilized for licensing. For simpler implementations, a digitally signed hash record of the license can be stored on the blockchain. In either case, a record of the license transaction would be preserved by the blockchain. If the entire license is embedded in the blockchain, then the blockchain itself could serve as the mechanism for transporting the license between nodes. Any confidential information in the license would be encrypted with the licensee cryptographic key, so that the integrity of the transaction would be preserved while still retaining the confidential portion of the IP.

Identify3D enhances the supply chain blockchain by adding records of the digital twin to each physical part created with digital manufacturing technology. This allows the final assembled product to have a complete record of the manufacturing operations as well as the digital design and IP included in the completed product.



Example of Identify3D integration with blockchain

The software/hardware connection

Now with the Identify3D solution integrated into the Siemens digital enterprise suite, users have the capability to protect the confidentiality and integrity of their IP from creation through manufacturing.

For example, an aerospace manufacturer may have a quick-turn requirement for 20 CNC manufactured replacement parts. Since they have already designed and qualified the part, the TDP is stored in Teamcenter as an item revision. The user can select the TDP and create a DSI using Identify3D Protect while restricting the part to be made only on a qualified machine. Next the aerospace manufacturer will authorize the contract manufacturer to produce 20 parts through Identify3D Manage for Engineering.

When the subcontractor receives the authorization, they determine that they must use another subcontractor in order to meet the volume. Therefore, they will use Identify3D Manage for Distribution to authorize their own shop floor to manufacture 12 parts and authorize the subcontractor to manufacture 8 parts.

The contract manufacturer will receive the authorization on Identify3D Manage for Manufacturing running on their shop floor and will have the option of authorizing the three CNC machines that are qualified to produce the part. In this case, the contract manufacturer will assign each machine to produce four parts. The Siemens SINUMERIK 840D sl controller running Identify3D Enforce on each machine will receive the DSI containing the part specific G-code and create a job; then, since each machine has the proper certification, the operator will be able to select the job and produce only four parts.

When the process is complete, the aerospace manufacturer will be able to view a record of the successful completion of the order, including reports for each machine used through Identify3D Trace which may be running in Siemens MindSphere. The aerospace manufacturer will see the subcontractor used by the contract manufacturer and observe reports from the two CNC machines used by the subcontractor.

Conclusion

Industry 4.0 is transforming the way companies manufacture. Like other industries, the manufacturing sector is going through the digitalization of assets and processes, so to some extent, the future is now. However, to really capitalize on the benefits of this digitalization, an enormous volume of data needs to be managed, controlled, and tracked as it moves through the digital supply chain.

Implementation of decentralized manufacturing models with ability to manufacture at the place and time of need can only happen if the right data gets to the right machines at the right time, following a tightly controlled and secure process.

The integrity of both digital and physical supply chains is critical to prevent an overflow of counterfeits, maliciously modified, poor quality, or uncertified parts from going to market. Technology that protects data at rest, manages the data flow through licensing, and keeps inalterable records of movements, like that from Identify3D, will go a long way to enable the secure deployment of these new manufacturing business models.

References

1. https://www.plm.automation.siemens.com/en/plm/digital-manufacturing.shtml
2. https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW
3. https://www.mbtmag.com/article/2017/03/top-cybersecurity-threats-manufacturing-2017
4. http://www.bbc.com/news/technology-30575104
5. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
6. Sturm, L.C., et al. “Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects.” *Journal of Manufacturing Systems* Volume 44, Part 1: July 2017, pages 154-164.
7. https://www.prnewswire.com/news-releases/cybercrime-damages-are-predicted-to-cost-the-world-6-trillion-annually-by-2021-300540158.html
8. https://www.infosecurity-magazine.com/news/nonmalware-attacks-on-the-rise
9. https://www.infosecurity-magazine.com/news/annual-cybercrime-costs-double-6
10. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
11. https://www.isa.org/isa99

Siemens PLM Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Suites 4301-4302, 43/F
AIA Kowloon Tower,
Landmark East
100 How Ming Street
Kwun Tong, Kowloon
Hong Kong
+852 2230 3308

About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Digital Factory Division, is a leading global provider of software solutions to drive the digital transformation of industry, creating new opportunities for manufacturers to realize innovation. With headquarters in Plano, Texas, and over 140,000 customers worldwide, Siemens PLM Software works with companies of all sizes to transform the way ideas come to life, the way products are realized, and the way products and assets in operation are used and understood. For more information on Siemens PLM Software products and services, visit www.siemens.com/plm.

www.siemens.com/plm

71790-A6 7/18 H