A Taxonomy of Cyber Attacks in Smart Manufacturing with NIST Cybersecurity Framework Manufacturing Profile

Bethanie Williams, Marena Soulet, Advisor: Dr. Ambareen Siraj
Department of Computer Science, Tennessee Tech University

Abstract

- A revolution in manufacturing systems is underway with smart manufacturing becoming an integral component of the broader push towards Industry 4.0. As the modern manufacturing industry continues to bridge digital and physical environments through the use of Internet of Things (IoT), cloud systems, data analytics, and machine learning, this integration of physical industrial systems with cyber technology has led to an increase in cyber-physical attacks with ongoing discovery of new security challenges. This paper provides a comprehensive study of common security challenges and attacks faced by smart manufacturing systems today and uses the NIST Cybersecurity Framework Manufacturing Profile as a guideline to address cyber incidents that have occurred within the manufacturing sector.

Introduction

- As the modern manufacturing industry continues to bridge digital and physical environments through the use of Internet of Things (IoT), cloud systems, data analytics, and machine learning, this integration of physical industrial systems with cyber technology has led to an increase in cyber-physical attacks with ongoing discovery of new security challenges.

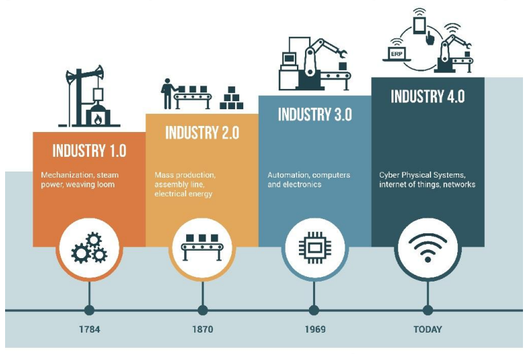
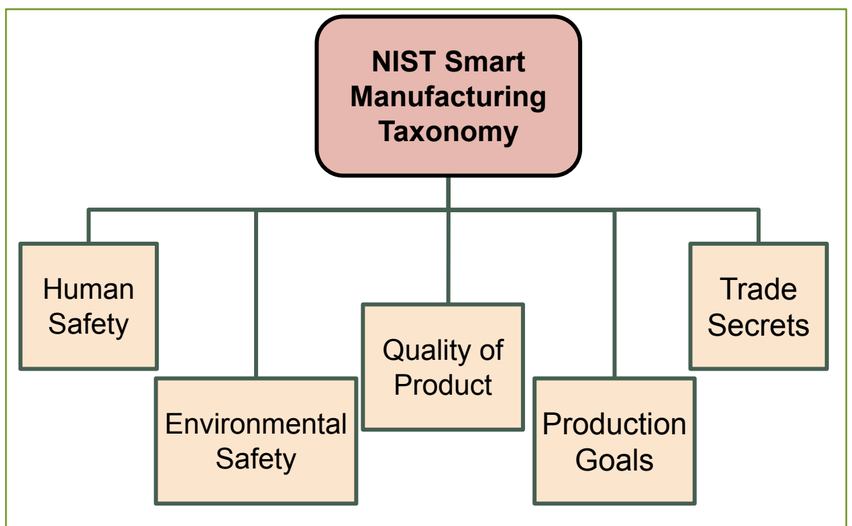


Image Above Taken from [1]

NIST

- **National Institute of Standards and Technology**
  - Supports and develops information security standards and guidelines for industries such as manufacturing
- **Cybersecurity Framework Manufacturing Profile**
  - Provides identification of common business/mission objectives relevant to the manufacturing sector
  - **Manufacturing Objectives**
    - Creates context for identifying and managing cybersecurity risk mitigation pursuits
  - **Categorization Process**
    - Identifies a security measures performance, relevance, and effectiveness for assessing a level of risk

NIST Manufacturing Profile [2]



Proposed Taxonomy with Attributes

Incident	→	A cyber event capable of jeopardizing the CIA goals of information or physical systems.	Actors	→	Groups or individuals who exploit system vulnerabilities to gain unauthorized access and/or cause harm to a system.
Attack Mechanism	→	A method or strategy used to target and compromise a system.	CIA Violation	→	A violation of one or more of the CIA goals: confidentiality, integrity, and availability.
Level of Impact	→	Extent of potential damage caused by a cyber attack.	Type of Threat	→	A potential agent/action that causes: deception, disclosure, disruption, and usurpation

- Maps smart manufacturing cyber attacks based upon the priorities of the manufacturing objectives, security challenges, and the potential impacts on the manufacturing systems
- Lists well-known cyber attacks that have occurred throughout cyber-history and creates awareness about damages caused by the cyber attacks
- Conducts an analysis of publicly available technical publications to establish a baseline for cyber attacks in smart manufacturing
- Recognizes that attacks target organizations to compromise cyber systems with the intention to cause harm to the physical environment
- Identifies a pattern of vulnerabilities found in industrial control systems (ICS) and information technology (IT) systems in manufacturing sector
- Enables manufacturers to develop a proactive approach to mitigate attacks, resulting in increased security in smart manufacturing systems.

Examples of Dimensions

First Dimension: Human Safety

Incident	Attack Mechanism	Level of Impact	CIA Violation	Type of Threat	Actors
Car Shark	Malicious Software	High	Integrity Availability	Usurpation Disruption	Domestic (USA)
Davis-Besse Nuclear Power Station	Worm	Low	Availability	Disruption	Foreign (Czech Republic)
Jeep Cherokee Ignition Switch	Zero-Day Exploit	Moderate	Confidentiality Integrity	Usurpation	Domestic (USA)
Saudi Arabian Petrochemical Plant	Malware	High	Integrity	Usurpation Disruption	Foreign (Russia)

Second Dimension: Environmental Safety

Incident	Attack Mechanism	Level of Impact	CIA Violation	Type of Threat	Actors
Florida Water Treatment Plant	Unauthorized Remote Access	Low	Integrity	Usurpation	Unknown
Australia Wastewater Treatment Plant	Insider Threat	High	Integrity Availability	Disruption Usurpation	Domestic (Australia)
BTC Turkey Pipeline Explosion	Malicious Software	Moderate	Integrity Availability	Deception Usurpation	Russia
US Turbine Control System	Malware	Moderate	Confidentiality Availability	Disruption Disclosure	Unknown
New York Dam	Unauthorized Remote Access	Low	Confidentiality	Disclosure	Iran
Ukraine Power Grid	Malware	High	Availability	Disruption	Russia

Third Dimension: Quality of Product

Incident	Attack Mechanism	Level of Impact	CIA Violation	Type of Threat	Actors
Virginia Tech Case Studies	Code Modification	Low	Integrity	Disruption Deception	Domestic (USA)
Dyn Inc.	Denial of Service (DoS)	Moderate	Integrity Availability	Disruption Deception	Domestic (USA)
Kemuri Water Plant	Malware	High	Confidentiality Integrity	Disruption Disclosure	Foreign Hacktivist Group
WannaCry Virus	Ransomware	High	Integrity Availability	Disruption Disclosure	North Korea

Fourth Dimension: Production Goals

Incident	Attack Mechanism	Level of Impact	CIA Violation	Type of Threat	Actors
Daimler Chrysler Cars	Worm	Low	Integrity Availability	Disruption Usurpation	Morocco
Stuxnet	Worm	High	Integrity Availability	Disruption Usurpation	USA and Israel
German Steel Mill	Spear-phishing	High	Confidentiality Integrity Availability	Usurpation Disclosure	Unknown
Honda Car Manufacturer	Ransomware	Moderate	Integrity Availability	Disruption Disclosure	North Korea
Taiwan Semiconductor Manufacturing Company	Virus	Moderate	Availability	Disruption	North Korea
Norsk Hydro	Ransomware	High	Confidentiality Integrity Availability	Disruption Disclosure Usurpation Deception	Unknown

Conclusion & Future Work

- Smart manufacturing systems are much more vulnerable to cyber attacks than traditional manufacturing systems.
- Given the importance of IoT-based manufacturing systems throughout several industries and economies, identifying and remediating these vulnerabilities is of utmost importance.
- **Future Work:**
  - Improve vulnerability and risk assessments
  - Incorporate mitigation techniques with the NIST standards and framework
  - Create/enhance mitigation and detection techniques

Acknowledgements

- This research was conducted at Tennessee Tech University (TNTech) sponsored by the Office of Research at TNTech and National Science Foundation Scholarship for Service program.

References

[1] (March 31,). Industry 4.0 and Industrial IoT in Manufacturing: A Sneak Peek. Available: https://www.aberdeen.com/featured/industry-4-0-industrial-iot-manufacturing-sneak-peek/.

[2] K. Stouffer *et al*, "Cybersecurity Framework Manufacturing Profile ," *(NIST Internal Report (NISTIR) 8183),* 2019. Available: https://doi.org/10.6028/NIST.IR.8183r1.