INL/JOU-22-69525-Revision-0

BioSecure Digital Twin: Manufacturing Innovation and Cybersecurity Resilience

November 2021

Michael Mylrea, Charles Fracchia, Howard Grimes, Bill Reid, Nathan Case, Wayne E Austad, Gregory Edward Shannon

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/JOU-22-69525-Revision-0

BioSecure Digital Twin: Manufacturing Innovation and Cybersecurity Resilience

Michael Mylrea, Charles Fracchia, Howard Grimes, Bill Reid, Nathan Case,
Wayne E Austad, Gregory Edward Shannon

November 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

[0000-0003-3230-4415] [0000-0002-8956-8609]

BioSecure Digital: Manufacturing Innovation and Resilience

This work was partially funded by the Department of Energy under contract DOE-EE0009046.

Michael Mylrea[1], Charles Fracchia[2],
Howard Grimes[3], Wayne Austad[3], Gregory Shannon[4], Bill Reid[1]

[1] National Resilience Inc., La Jolla CA 92037, USA
[2] BioBright, Boston, MA 02114, USA
[3]The Cybersecurity Manufacturing Innovation Institute/University of Texas at San Antonio,
San Antonio TX 78249, USA
[4]The Cybersecurity Manufacturing Innovation Institute/Carnegie Mellon University,
Pittsburgh PA 15213, USA
Michael.mylrea@resilience.com
Howard.grimes@CyManii.org

Abstract: U.S. national security, prosperity, economy, and well-being requires secure, flexible, and resilient Biopharmaceutical Manufacturing. The COVID-19 pandemic reaffirmed that the biomedical production value chain is vulnerable to disruption and has been under attack from sophisticated nation state adversaries. Current cyber defenses are inadequate, and the integrity of critical production systems and processes are inherently vulnerable to cyber-attacks, human error, and supply chain disruptions. The following paper explores *how* a BioSecure Digital Twin will improve U.S. manufacturing resilience and preparedness to respond to these hazards, by significantly improving monitoring, integrity, security and agility of our manufacturing infrastructure and systems. The BioSecure Digital Twin combines a scalable manufacturing framework with a robust platform for monitoring and control to increase U.S, biopharma manufacturing resilience. Then, the article discusses some of the inherent vulnerabilities and challenges at the nexus of health and advanced manufacturing. Next, the paper highlights that as the Pandemic evolves, we need agility and resilience to overcome significant obstacles. This section highlights an innovative application of Cyber Informed Engineering to developing and deploying a BioSecure Digital Twin to improve the resilience and security of the biopharma industrial supply chain and production processes; Finally, the chapter concludes with a process framework to complement the Digital Twin platform, called the Biopharma (Observe, Orient, Decide, Act) OODA Loop Framework (BOLF) - a four-step approach to decision-making outputs from the Digital Twin.

[0000-0003-3230-4415] [0000-0002-8956-8609]

The BOLF will help end users leverage twin technology by distilling down available information, focusing the data on context, and rapidly making the best decision while remaining cognizant of changes that can be made as more data becomes available.

Keywords: Digital Twin, Critical Infrastructure, Cybersecurity, Resilience, Advanced Manufacturing, Cyber Informed Engineering, OODA Loop

4.0 Introduction

All modern organizations and nations require the health and well-being of their population to function. The COVID-19 pandemic was a grim reminder of how fragile our infrastructure and systems are when the health sector fails to keep us healthy. The United States' national security, economy and well-being requires secure, resilient, and agile capabilities to respond to coronavirus health and economic threats. As a critical national capability for coronavirus events, the current state of cyber-physical security in biopharma manufacturing requires a more resilient approach to improve the security, visibility and control of the rapid disease response, therapeutic resilience, and economic opportunities created by modern digitally supported biological systems. The following chapter highlights a high-impact research and development effort underway to move this sector toward increased resilience, while also improving the competitiveness, integrity, visibility of the manufacturing process via a high-fidelity BioSecure Digital Twin. A Digital Twin is defined as a high-fidelity virtual model or representation of the physical environment, including the data exchange, communication, interaction, and behavior between converged physical and virtual spaces. The virtual or cyber part of the twin collects, aggregates, and analyzes performance behavior data throughout the production life cycle of the physical systems and sensors. The Digital Twin allows digital verification of products to ensure the latest technologies are deployed across the entire manufacturing ecosystem. Machine learning helps distill down and recognize patterns in the data from multiple sources (e.g. sensor, model, domain expertise) to predict behavior and optimize performance. Digital Twin use cases are increasing from GE's Digital Ghost for cyber-physical anomaly detection combined cycle power plants to real-time monitoring and predictive maintenance of aircraft and various defense platforms,[1] from predictive maintenance on the factory floor to dual optimization in manufacturing where the physical

[1] Michael Mylrea, Matt Nielsen, Justin John, Masoud Abbaszadeh (2021, forthcoming), AI Driven Cyber Physical Industrial Immune System for Critical Infrastructures. In W.F. Lawless, D.A. Sofge & R. Mittu (Eds.), *Systems Engineering and Artificial Intelligence.* Springer.

[0000-0003-3230-4415] [0000-0002-8956-8609]

systems provide intelligence for the virtual mirror to continuously evolve.[2]

The proposed BioSecure Digital Twin, **Figure 1** will create an industrial immune system to improve manufacturing to rapidly identify anomalies and mitigate the behavior that deviates from normal operations, both in the cybersecurity dimension and in process fidelity control. It creates a digital infrastructure that is portable and can be deployed as a virtualized testbed for both simulation, analytic, control and optimization. Potential use cases for applying Digital Twin solutions to improve cybersecurity are numerous, from cyber wargaming to enhanced workforce development, where end users can learn and experiment on a high-fidelity twin. In realization of these objectives, this research has the potential to transform and improve biopharma cybersecurity resilience, integrity and monitoring of the supply chain and production lifecycle, while improving:

- **Monitoring and Agility.** Improved monitoring and agility with a high-fidelity Digital Twin will help improve biopharma production system simulation, analytics, optimization, and security.
- **Acceleration, Efficiency and Scale.** The competitiveness of the US bioeconomy on the global stage depends on improving real-time visibility and analytic capabilities of the biopharma production lifecycle. A BioSecure Digital Twin will help realize these acceleration and efficiency objectives in addition to various cybersecurity objectives – pervasive, unobtrusive, resilient, and economical – will drive the U.S. bioeconomy into global leadership position.
- **Cybersecurity, Integrity and Resilience.** Strengthen our national security by developing next-generation defensive capabilities for the critical healthcare and bioeconomy sector.

[2] Tao, Fei, and Meng Zhang. "Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing." IEEE Access 5 (2017): 20418-20427.

[0000-0003-3230-4415] [0000-0002-8956-8609]

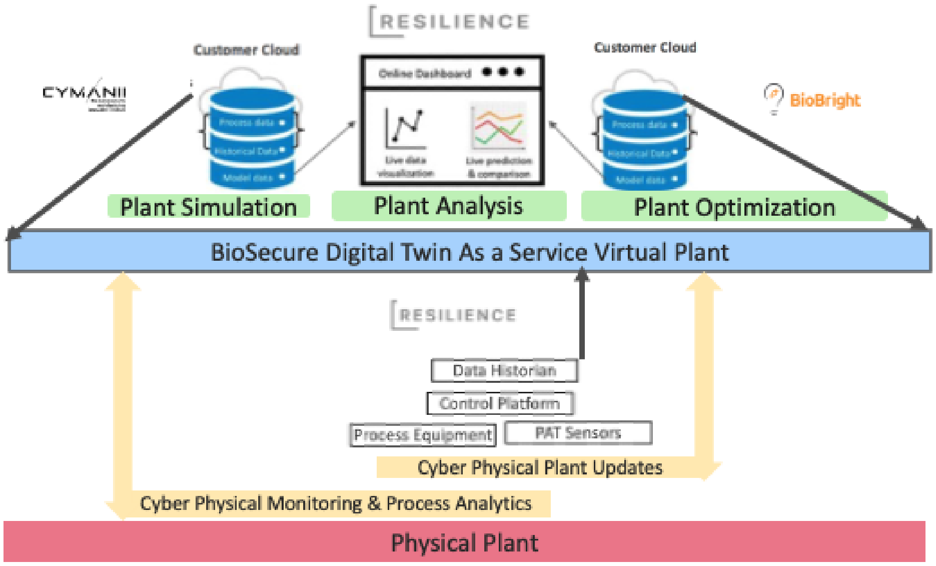


Figure 1. Illustrative BioSecure Digital Twin to improve monitoring and agility, accelerate US bioeconomy competitiveness and most the sector towards cyber-physical resilience.

4.1 Problem

At present, biopharma and other advanced manufacturing platforms are vulnerable to catastrophic attacks, supply chain shortages, human error and other naturally occurring disasters capable of wiping out most of the U.S. bioeconomy. Our bioeconomy is currently estimated at more than 5% of U.S. GDP ($950B) annually, according to Safeguarding the Bioeconomy, a 2020 report from the National Academy of Sciences, Engineering and Medicine. Our nation's ability to respond to pandemic events, compete on the global stage, and realize the full potential of the bioeconomy depends on our ability to monitor, predict, and protect its underlying cyber-physical infrastructure. We must better control the process machine states, strongly verify product integrity through its entire chain of custody and compare machine and workflow states across geographies and history. In realization of these goals, the BioSecure Digital Twin for critical biopharma processes and supply chains will employ CyManII's "Secure BioPharma Architectures" (SBPA) based on the Secure Manufacturing Architectures (SMA) that CyManII is developing and implementing for other manufacturing sectors.

Biopharma infrastructure is vulnerable to a host of adversaries and naturally occurring hazards, from cyber threats to supply chain shortages, from access issues directly related to the pandemic, to simple human errors. The current state of biopharma manufacturing systems and processes vulnerabilities exacerbates these challenges and undermines the preparedness and competitiveness of the US bioeconomy. The vulnerabilities in the

[0000-0003-3230-4415] [0000-0002-8956-8609]

current state and R&D and validated advances for a future state, shown in **Figure 2**, constitute the focus areas of this ongoing research.

BioPharma Operational Technology & Industrial Control Systems. A digital transformation of manufacturing is rapidly digitizing, networking and automating the biopharma-value chain. Today's smart manufacturing systems unlock value in modernizing processes and systems that are increasingly interoperable, connected to cloud and associated microservices at the edge of the control plane. While this modernization has unlocked significant value in process efficiency, it also presents new security challenges for critical production systems and operational technology (OT) never designed to be connected to the Internet. The rapid digital transformation of our critical systems has significantly increased its attack surfaces by combining cyber-physical systems, software and hardware, information technology (IT) and OT. This has created new challenges to identify, monitor and protect these critical systems.[3] A BioSecure Digital twin can help fill these gaps by providing real-time cyber-physical situational awareness and monitoring the cyber threats and anomalies across the cyber-physical, IT and OT attack surface.[4]

However, even as Digital Twin technology helps improve cybersecurity defenses, the attack surfaces of biopharma and other advanced manufacturing has expanded significantly, introducing, and leaving several major cyber gaps. For one, most cyber defenses and monitoring solutions are ineffective in detecting sophisticated attacks targeting operational technology. This is especially true with insider and supply chain attacks, zero-day exploits and other stealthy threats that continue to evade and defeat cyber defenses and intrusion detection systems. These systems originated from securing information technology across a business enterprise and defending against known malware, malicious packets and other attacks that are easy to catalogue in a library as signature heuristics. However, OT found in various biopharma production systems present new challenges as the protocol, malware signatures, and tactics, techniques and procedures used by adversaries also differ significantly. Moreover, manufacturing plants lack basic cybersecurity defenses to identify and monitor their critical cyber-OT assets. Thus, the detection of sophisticated adversaries is limited – usually too late or reactive, only after the damage has been done – enabling them to persist their malicious activities

[3] Mylrea, M. & Gourisetti, S.N.G. (2017), Cybersecurity and optimization in smart "autonomous" buildings In Lawless, W.F. Mittu, R., Sofge, D. & Russell, S. (Eds.) (2017), *Autonomy and Artificial Intelligence: A threat or savior?* New York: Springer.

[4] Michael Mylrea, Matt Nielsen, Justin John, Masoud Abbaszadeh (2021, forthcoming), AI Driven Cyber Physical Industrial Immune System for Critical Infrastructures. In W.F. Lawless, D.A. Sofge & R. Mittu (Eds.), *Systems Engineering and Artificial Intelligence*. Springer.

[0000-0003-3230-4415] [0000-0002-8956-8609]

in critical systems and networks often without being detected.

To overcome these limitations, solutions must advance from security to resilience and provide more holistic cover for critical OT in critical manufacturing. Cyber defense of critical infrastructure continues to evolve, but cyber adversaries often have the upper hand as their offensive tools improve and the attack surface available to them expands. Cyber challenges remain for policies, technology, and people (workforce and expertise). To change this equation, new paradigms, formal methods, and advances in threat mitigation technology need to be developed. Even as cyber defense technology improves, workforce development, especially in the area of OT cybersecurity, remains a major gap. The confidentiality, integrity and availability triad that has defined cybersecurity in the last 20 years continues to be pressured by the digital transformation underway. The digital transformation in the biopharmaceutical sector has prioritized interoperability, connectivity and the move towards automation often leaving core cybersecurity concerns behind. As we digitize, automate, and connect systems in critical infrastructure to the internet, this also expands the cyber-physical attack surface, which we must protect or risk losing the dominant opportunity in the global bioeconomy.

To improve the current state of the art in biopharma cyber-defense requires moving beyond the cybersecurity triad paradigm in favor of cyber resilience. A BioSecure Digital Twin will help improve the ability to identify, detect, respond, and recover to cyber threats and vulnerabilities in sub-second times. Cyber resilience requires both a hardened perimeter as well as the ability to neutralize sophisticated attacks once they have been found. In short, a defense in depth approach must be adapted for use in the critical sector of the bioeconomy.

Advances of innovative threat mitigation solutions help to move the industry towards cyber resilience. However, the design and implementation of these advances, such as machine-learning algorithms, requires the distillation of large data sets to be intelligently fused with operations. The form of the cyber-defense technology needs to be complemented by a process function in a way that helps transform data into intelligence and production insight. Through this information fusion, human-machine teams can increase both their autonomy and effectiveness to evolve their defenses to be more cyber resilient in response to sophisticated and evolving threats. The effective design and deployment of the next generation BioSecure digital twin to mitigate threats in a more effective and autonomous way also requires prioritization. To effectively develop and deploy a digital twin we perform an applicability and gap analysis via a framework of Consequence-driven Cyber-informed Engineering (CCE), a methodology focused on securing the nation's critical infrastructure systems.

4.2 Applying Cyber-informed Engineering (CIE) to Effectively Develop and Deploy a Digital Twin for BioPharma Manufacturing

Applying CCE framework is important as it recognizes that the biopharma manufacturing is inherently vulnerable and that a skilled and determined adversary has the capability to sabotage a manufacturing system, process, and infrastructure. Consequence-driven Cyber-informed Engineering is a rigorous process for applying CIE's core principles to a specific

[0000-0003-3230-4415] [0000-0002-8956-8609]

organization, facility, or mission by identifying their most critical functions, methods and means an adversary would likely use to manipulate or compromise them and determining the most effective means of removing or mitigating those risks. The Cyber-Informed Engineering (CIE) framework and body of knowledge drives the inclusion of cybersecurity as a foundational element of risk management for engineering of functions aided by digital technology. CIE emphasizes the removal of potential risk in key areas, as well as ensuring resiliency and response maturity within the design of the engineered system. CCE walks an organization through core components of CIE in CCE's 4-phase process (shown in **Figure 2**[5]) to evaluate, remove or mitigate weaknesses in their critical functions.

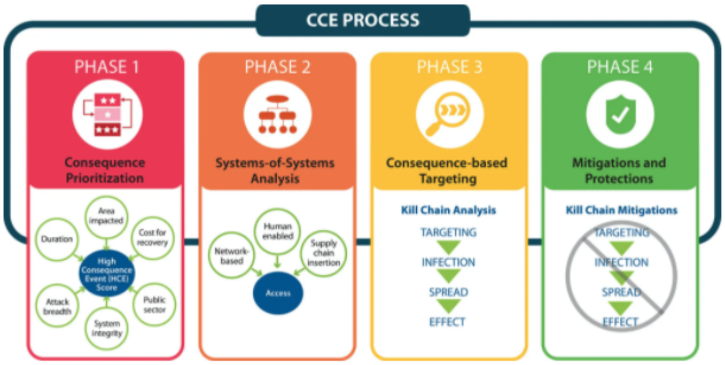


Figure 2. Outlines CCE process in a way that can help guide effective Digital Twin deployment.

Exploring Digital Twin use cases through a CCE framework provides valuable insight into how to deploy a BioSecure Digital Twin, thus providing manufacturing stakeholders a more focused bottom-line approach to: a) determine most critical functions Identify methods an adversary could use to compromise the critical functions; b) evaluate complex systems; and c) apply proven engineering, protection, and mitigation strategies to isolate and protect the most critical assets.[6] This becomes a valuable framework in determining the use case, what is being modeled and how to effectively deploy a Digital Twin to secure critical manufacturing systems and infrastructure.

Consequence Prioritization. Deploying a Digital Twin for every production system and associated network would degrade the fidelity of date and ability to model, analyze and effectively draw insight and intelligence from the operation. Leveraging CCE requirements a comprehensive design can be developed for a BioSecure Digital Twin. During the design phase it is essential to scope the target system and define the sub-

[5] Idaho National Laboratory. Cyber-informed Engineering Website. Accessed on July 28, 2021, at https://inl.gov/cce/

[6] Bochman, Andrew A., and Sarah Freeman. *Countering Cyber Sabotage: Introducing Consequence-driven, Cyber-informed Engineering (CCE)*. CRC Press, 2021.

systems that are prioritized based on their potential consequence (Show in Figure 3[7]) or impact if the system was sabotaged or taken offline.

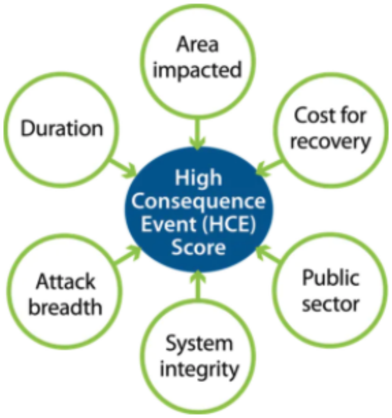


Figure 3. Consequence Prioritization helps focus the Digital Twin on modeling and related use cases to predict and prevent cyber events that have the greatest potential impact.

For example, if a production system produced a vaccine that was sabotaged, and no alarms or malicious behaviors were detected the damage could be catastrophic resulting in loss of life, reputation, and prohibitive damage that shut down most manufacturing plants. Digital Twin consequence driven prioritization will leverage domain expertise to determine vulnerabilities that could be exploited to cause such an event and use a supervised machine learning approach to determine what the behaviors look like behind the anomaly that would lead to such an event. With the understanding of what normal operations look like combined with a detailed understanding of anomalies from faults, cyber-attacks, naturally occurring ambient changes and degradation curves, you can start training the Digital Twin and establish boundary conditions for modeling and simulation for improved detection and mitigation of stealthy cyber-attacks.

Systems of Systems of Analysis. After the consequence analysis helps select the production environment, systems of system analysis of the BioSecure Digital Twin model need to be tested, exercised, and trained to define the system's boundary conditions. A range of normal and abnormal space is selected with various levels of actable deviation based on naturally occurring ambient conditions and other norms within the operating manifold.

[7] Freeman, Sarah G., Curtis St Michel, Robert Smith, and Michael Assante. *Consequence-driven cyber-informed engineering (CCE)*. No. INL/EXT-16-39212. Idaho National Lab. (INL), Idaho Falls, ID (United States), 2016.

[0000-0003-3230-4415] [0000-0002-8956-8609]

Consequence-based Targeting. A high-fidelity model of cyber-attack versus fault analysis within the operating spaces is essential to help reduce false positives and improve the accuracy of the Digital Twin's detection capability. Consequence based targeting test, exercise and trains the machine learning algorithms against different scenarios to determine paths, targets, access, and information an adversary would need to achieve the events. This Kill Chain Analysis can be reversed engineered to further test the algorithms for defenses against stealthy attacks. Machine learning algorithms developed from these attacks is intended to differentiate between a naturally occurring system fault, degradation, human error, and attacks. Historical data obtained from BioPharma manufacturing environment is reviewed to establish the key system monitoring nodes for detecting and localizing events, which is especially important in a transient closed loop system with a lot of stochastic behavior.

Mitigation and Protections. Kill chain analysis than supports associated mitigations by establishing the decision boundary between the normal and abnormal operating space. This can help improve performance predictions that are generated based on this optimal decision boundary. The optimal decision boundary may also evolve as the cyber threat is complex, non-linear, and rapidly evolving. It is essential that boundary and learning algorithms are updated over as the system evolves via real-time learning and adaptation algorithms. Performance and data-fidelity of the BioSecure Digital Twin needs to be continuous reviewed and continuously monitored throughout the biopharma production lifecycle.[8] We perform the kill chain analysis and mitigations it is important to understand system level vulnerabilities and security gaps found in BioPharma production systems.

4.3 Biopharma System Level Security Gaps

Technology Gaps. The following four are areas in technology gaps that need to be closed: (i) Unlike IT solutions which are easy to enumerate and inventory by scanning, operational technology includes a large and diverse attack surface that is often connected through both internet protocol (IP), serial, bluetooth, and other connections. (ii) Proprietary protocols initially designed for intellectual property purposes are often vulnerable by design as vendors prioritize functionality, ease of use and cost over security. (iii) Firewalls, network, and host intrusion detection systems are rarely implemented by the vendor and left to be the customer's responsibility. Thus, even moderately sophisticated attackers using brute force, polymorphic, AI-generated, or insider attacks are virtually impossible to detect with current field-accepted technologies Zero-day exploits targeting operational technology are very difficult to block with most existing attack detection solutions let alone taking into account the hundreds of custom software, firmware and hardware solutions deployed in the field by vendors who have not historically considered the cybersecurity attack surface. (iv) And resource intensive tuning

[8] Michael Mylrea, Matt Nielsen, Justin John, Masoud Abbaszadeh (2021, forthcoming), AI Driven Cyber Physical Industrial Immune System for Critical Infrastructures. In W.F. Lawless, D.A. Sofge & R. Mittu (Eds.), *Systems Engineering and Artificial Intelligence.* Springer.

can be required for AI defense critical solutions to be integrated into existing technology stacks for Security Information and Event Management (SIEM).

Process and Policy Gaps. As AI solutions improve attack detections it will increase the speed, size, and fidelity of logging critical machine state integrity as well as other network and system outputs. Thus, monitoring policies and process updates need to intelligently distill and fuse these findings for this data to create actionable cyber intelligence. Often, cyber defenders have policies and processes in place to monitor and log their critical cyber assets as defined by FDA requirements; however, they often do not read these logs. Moreover, additional networks or systems that are connected to these critical cyber assets can provide an attack pathway if they are not secured and are not currently considered strongly enough when demonstrating ongoing compliance to pharmaceutical quality as defined by FDA.

An additional major gap in policy is FDA's current definition of what constitutes a "medical device". Currently, devices used in the biopharmaceutical production workflow are not considered part of the Center for Devices and Radiological Health (CDRH) purview, instead falling under the Center for Biological Evaluation and Research (CBER) [9,10]. In practice, this leaves a gaping hole in the evolving security measures applied to devices that are crucial to biopharmaceutical production and national disease response. We strongly recommend that the department of Health and Human Services (HHS) give FDA's Center for Biological Evaluation and Research (CBER) the resources to build strong –and perennialized- cybersecurity expertise. Without it, we are condemning ourselves to a two-speed security improvement regime and a lack of understanding of unique biopharmaceutical and bioeconomy threats.

Table 1. Current and Future State.

Current State	Future State
Critical production systems are not monitored	The BioSecure Digital Twin monitors every step in the supply chain and the production process
Currently systems use insecure architectures	Secure BioPharma Architectures ensure that the biosecure digital twin, and the underlying physical processes, are cybersecure
Current Systems Lack Security Controls and Contain Multiple Vulnerabilities	The Secure BioPharma Architectures introduce security controls while detecting and mitigating cyber vulnerabilities
Systems lack basic cybersecurity analysis tools	CyManII will develop and implement integrous tools for biopharma on systems deployed by National Resilience and BioBright.
Systems have NO traceable	The Secure BioPharma Architecture introduces

[9] https://www.fda.gov/medical-devices/classify-your-medical-device/device-classification-panels

[10] https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device

[0000-0003-3230-4415] [0000-0002-8956-8609]

Bio Integrity	CyManII's "cyber physical passport" to create supply chains that are rooted in trust and data integrity

We further recommend that the Biomedical Advanced Research and Development Authority (BARDA) and the office of the Assistant Secretary for Preparedness and Response (ASPR) be given the resources to build similar core competency and understanding of digital biosecurity and cybersecurity concerns. These resources must be made perennial in the form of an office for cybersecurity or digital security. This does not need to be expensive by including a small staff of 4-5 people each, but it needs to be dedicated offices reporting to the director and assistant secretary respectively to ensure the appropriate responsiveness and escalation to mitigate attacks.

The resources outlined above should engage in an inter-agency process to leverage knowledge from the Department of Defense (DoD) and Department of Homeland Security (DHS) adapt them to their unique biomedical sector needs and threats.

People Gaps. Machine learning algorithms that have high-false positive rates create prohibitive operations and maintenance requirements for security teams. Cybersecurity teams have been traditionally IT focused, however, the convergence of IT/OT in critical infrastructures has increased the responsibilities and created new workforce development challenges for them. Some innovative new tools require training, but adding another tool creates information fusion challenges. Finally, AI solutions that are tuned and learn what is normal on networks and systems that are already infected may be providing a false sense of security to their operators. Advances in invariant learning and humble AI explored in this chapter highlight how researchers are overcoming these gaps.

4.4 Contribution to Digital Twin R&D, Testbeds, and Benefits

The BioSecure Digital Twin accomplishes two important outcomes. First, it significantly and efficiently improves bio-integrity of the U.S. biopharma manufacturing sector. Second, it results in greatly improved operational cybersecurity in the U.S. biopharma manufacturing. It does this by a) making critical production systems more visible in both the biological and cybersecurity dimensions, b) enabling continuous and improved parallel modeling, integrity, analytics, and control of biopharma processes, c) introducing secure BioPharma architectures that will move the biopharma manufacturing sector toward cyber-physical resilience, d) providing a strong, cryptographically auditable trail designed to provide multiple, out-of-band, parallel paths for traceable audits of processes, and e) developing continuous testing of quality, integrity, and security through the entire production lifecycle. These areas are explained in more detail below.

The BioSecure Digital Twin Project advances effective and efficient bio-integrity and cybersecurity for the biopharma industry that is critical to coronavirus detection and response. It also builds on the cybersecurity innovations being introduced by The Cybersecurity Manufacturing Innovation Institute in developing and implementing cyber-inspired, secure by design architectures that will protect and enhance U.S. manufacturers. **Table 2** describes how the R&D and Testbed contributions enable us to respond effectively to the Coronavirus challenges and associated benefits with each of our project objectives. These P drive the outcomes for BioSecure Digital Twin.

Table 2. Project Objectives. Our objectives drive outcomes based on our 5 tasks.

BioSecure Digital Twin - Project Objectives for Coronavirus R&D					**Summary Outcomes**
A. Visibility into Cyber & Physical Processes	**B. Parallel Modeling & Analysis**	**C. Secure BioPharma Architectures**	**D. Traceable & Secure Audit Trails**	**E. Continuous Quality & Security**	High fidelity process controls. Detect and mitigate both anomalies and vulnerabilities. Accelerate new production processes. Introduce trust, integrity, & resilience for Bio Manufacturing. Optimize production across sites, geographies, and CDMOs.
Make critical productions systems for coronavirus detection, treatment, and prevention visible for both physical quality & cybersecurity.	Enables continuously-improved parallel modeling, integrity checks, performance analytics, and control of biopharma processes used in coronavirus.	Create new secure biopharma architectures and systems that will move bio manufacturing for coronavirus response and health-care therapeutics towards cyber-physical resilience.	Provides cryptographically auditable trail designed to preserve data lineage and provenance for both physical and cyber properties in corona virus therapeutics.	Establish continuous testing of quality, integrity, and security through the production lifecycle of coronavirus detection, treatment, and prevention products.	
BioSecure Digital Twin created using Secure by Design Lifecycle and CyManII's SMA Framework 1. Requirements ↔ 2. Design ↔ 3. Build ↔ 4. Testing ↔ 5. V&V					

(A) Visibility into Cyber-Physical Processes – Benefits. Make critical production systems visible in both the biological and cybersecurity dimensions. In the biological dimension it enables a continuous quality approach that is data-driven and real-time linked to high fidelity process models. In the cyber dimension it provides strong logging, dramatically improves attacker detection based on physical behaviors, and makes it harder for unsophisticated attackers to have an impact.

This contribution directly addresses the fact that no monitoring of critical production systems currently occurs. Monitoring in the biomanufacturing sector largely follows historical definitions of pharmaceutical quality, with an emphasis on paper records and strong change management processes. This is like what CyManII is addressing in eight other manufacturing sectors with our integrated technical approach. While essential, these processes have not taken advantage of modern monitoring technologies and capabilities. This has biological implications such as long lead times (often several days) to identify root cases for batch deviations, difficulty in comparing real-time conditions with all historical batches, and near-total reliance on individual staff's historical experience and memory. In the cyber domain, this lack of modern monitoring represents an enormous

[0000-0003-3230-4415] [0000-0002-8956-8609]

advantage for adversaries: it makes detection difficult; attribution is significantly more complex; lateral movement by attackers within networks is simplified; and adversaries can use less sophisticated methods. This high fidelity cyber-physical visibility also provides the following benefits:

1. **Improved Scale-Up Process Characterization.** By continuously collecting and processing data from all digital instrumentation that underpins the biological scale-up process, we enable an unprecedented level of process characterization. This in turn enables us to improve the state-of-the-art in batch comparison, inter-operator variabilities, identification of anomalies and differences in batch conditions (PV, RPM, feed timing, feed nature, feed concentration, respiratory parameters, etc). Our approach provides data-driven feeds for all the digital data collected from the process in near real-time thus making the process analyzable and machine learnable in a way that was not previously possible.

2. **Transform Digital Biosecurity Monitoring and Attacker Detection.** By collecting all the biological scale-up process data, we enable a new level of data-driven digital biosecurity monitoring. With this process data at our disposal in a reproducible way (API, structured data), and at scale (100's of instruments), we can create digital tripwires to identify, characterize and rapidly respond against attackers who attempt to infiltrate these key processes. The combination of process and traditional cybersecurity endpoint data enables us to develop true digital biosecurity detection mechanisms leveraging features that cross the cyberphysical / cyber-biological domains.

(B) Parallel Cyber-Physical Modeling & Analysis – Benefits. Enable continuously improved parallel modeling, integrity checks, performance analytics, and control of processes used in coronavirus pharmaceuticals.

Our proposed solution creates a framework that is both secure by design and aligned to the needs of the modern industrial biological age. Our framework incorporates the need of process and workflow biologists at its very core, striking a balance between security and useability in the facilities. This is important as legacy biological instrumentation will continue to be a source of vulnerability for several years until all vendors make cybersecurity an important part of the design lifecycle. Therefore, our proposed solution creates a digital twin that operates in "shadow mode" to the physical process but can inform and protect the workflow scientists are operating. The major benefits of a BioSecure Digital Twin that enables parallel modeling, integrity, analytics, and control of the biopharma process are:

1. **Security Lifecycle Support.** Our biosecure digital twin also enables improvements in design through advancing modeling and analytics of critical processes. For example, the impact of patching a system or adjusting a batch volume can be understood via modeling simulation on a high-fidelity system without making physical changes to a live batch process.

2. **Adapt to the Constraints of the Biomanufacturing Workflows**. Our proposed solution provides real-time access to a digital twin of the physical processes that

[0000-0003-3230-4415] [0000-0002-8956-8609]

scientists are running. It enables them to run and compare models "in silico" to interrogate future states without placing any new requirements or workflows changes in their environment. The BioSecure Digital Twin is automatically populated with new data in the background by the secure infrastructure. New models and analyses are also updated in the back end and made available to the scientists via a series of web-based dashboards.

(C) Secure BioPharma Architectures – Benefits. Create a framework and build process that is secure by design, resilient, and aligned to the needs of the industrial biological technology lifecycle. A major factor that leads to structural insecurity of the biomanufacturing and public health response sectors is the lack of security attention that is paid to the key infrastructural devices and systems. These instruments and systems have a long shelf-life (10+ years), high CAPEX ($1M+ per many instruments), and software is often treated as an afterthought by the vendors. Vendors often subcontract the software development to the lowest bidder and to teams established in countries (Eg: Ukraine, China, India, Singapore, Bulgaria, etc.) that pose additional threat concerns, and software quality – let alone security – is almost never considered. BioBright and CyManII national lab partners have identified and responsibly disclosed many these vulnerabilities with relevant authorities in these areas. To add to this challenge, the historical focus on pharmaceutical quality led to the development of rigid processes that are woefully inadequate to the digital age. Processes that ensured integrity in a paper notebook paradigm have become leverageable and mortal vulnerabilities in the digital age of automation. This has led to a crisis of trust in modern biopharmaceutical workflows.

Current systems were not designed with cybersecurity in mind and are now interconnected with more systems and control data. Finally, the signature heuristics in current intrusion detection systems and firewalls don't recognize sophisticated attacks, such as insider exploits that enable privileged insider access to critical supply chains and production systems. The average amount of time to detect an organization has been hacked is currently 280 days. In the biopharmaceutical field, due to its complex logistics, 280 days can represent the success or failure of a drug candidate: and in the case of smaller, more innovative companies, the very survival of that enterprise. The problem is compounded by the lack of biosecure and bio-aware monitoring or detection tools, effectively affording adversaries unimpeded and undetectable reign of attack. By developing Secure BioPharma Architectures and Systems we will provide:

1. **Effective Operational Cybersecurity**. Secure BioPharma Architectures and Systems will move biopharma manufacturing sector towards cyber-physical resilience with real time monitoring. Instead of a detection signature being a 1 or 0 heuristic, we are taking a more holistic approach to monitoring anomalies by examining the metadata from bioreactors as well as the physical signatures (ambient, frequency, voltage) that are very difficult to spoof. When considering the stochastic nature of biology, together with cyber and physical signatures, it is very difficult for a human to analyze these prodigious data sets and find patterns. The proposed approach leverages a machine learning (ML) algorithm to luminate these patterns. Thus, the complexity of these systems can create the next

generation of defense as certain behaviors become impossible and can quickly be detected, localized, and mitigated, including faults, attacks, human error and even naturally occurring changes in ambient conditions.

2. **Enhanced Security Controls.** Meaningful and verifiable security controls and systems are non-existent in the biomanufacturing field, instruments are riddled with exploitable vulnerabilities and historical data integrity controls are easily circumventable. Existing verification and validation procedures (including paper backups) are vulnerable. In one incident, that this team has dealt with, the technological means used to produce and print the paper trail was relying on outdated and vulnerable digital platforms. This poses an existential threat to the trustworthiness of even paper batch records. In addition, all the digital process data is easy to exfiltrate, manipulate and destroy. By creating robust security controls by design, the proposed BioSecure Digital Twin improves control and redundancy of critical systems.

(D) Secure and Traceable Audit Trails – Benefits. Produce a Biosecure Digital Twin that provides a strong, cryptographically auditable trail that is designed to provide multiple, out-of-band, parallel ways to audit a process.

Today's reality is that the industry cannot track, trace, or validate the integrity of production lifecycle with a level of assurance adequate for today's threat landscape. Moreover, existing regulatory guidance and compliance processes have not adapted to digital threats and can in fact cause major downtimes and further exacerbate cybersecurity attacks. For example, existing security solutions that monitor production systems for vulnerabilities may create new validation requirements if they change the logs or function of the system. Finally, it is often impossible to attest that a security control is in place and working without continuously testing those controls. We shall address this with:

1. **Traceable Bio Integrity.** Developing continuous testing of quality, integrity, and security through the production lifecycle. This proposal will help produce a framework that other manufactures can use to design, deploy, and manage systems with a defense-in-depth approach improving resilience as well as data integrity and non-repudiation. It will be possible to root supply chains in trust.

2. **Seed for a Secure Standard for Data Collection & Auditing.** The BioSecure Digital Twin design provides strong primitives and capabilities that can – with proper federal collaboration and input (eg: NIST, FDA, ASPR, BARDA and DARPA) – be evolved into industry standards that would represent a giant leap in the resilience and verifiable auditability of biological processes. These contributions would help FDA's Center for Biologics Evaluation and Research and Center for Drug Evaluation and Research create strong and auditable trust for all coronavirus countermeasures.

3. **Next Generation – Real Time Audits.** Next generation regulation and audit of these system by FDA and other regulators could leverage a high-fidelity virtual representation of the physical state of the machine to improve efficiency and

visibility of audits remotely and in real time.

(E) Continuous Quality & Security – Benefits. These contributions improve the understanding, identification, and control of bio-physical anomalies inducible from cyber threats to bio-digital systems. Identifying, baselining, and monitoring what normal looks like using Digital Twins enables improved analytics and anomaly detection. Overcoming this complexity with improved understanding and control of sophisticated sensor suites in production systems also provides new opportunities for production efficiencies through predictive prognostics and inherent functional expandability providing win-win incentives for manufacturers to adopt such systems. **In realization of these goals, the** Biosecure Digital Twin will improve the current state of the art in several ways:

1. Trust and integrity of processes will be enhanced via preventative maintenance and by enabling continuous data quality assurance.
2. Introducing predictive quality analytics by collecting ground truth data at scale and leveraging modern, secure data-driven systems for building novel predictive models.
3. Applying cyber-physical anomaly detection to biopharma thus improving the ability to adjust machine settings to improve the output quality.

BioSecure Digital Twin enables continuous and predictive quality by monitoring the state of the industrial equipment (asset condition monitoring) and predicting failures (predictive maintenance), while also monitoring quality of manufactured product during all the steps of production, adding computer vision and ML. In **Figure 5**, a cyber physical anomaly detection engine will ingest DarwinSync metadata collected from critical production systems and analyze various out-of-band signals that deviate from what normal looks like. These anomalies will be detected, analyzed, and continuously train the detection and mitigation ML algorithms. To improve the accuracy and better understand the cause of the behavior that triggered the anomaly, we will perform inferential correlation in comparing commands from production workstations with the physics dictated by supervisory control and data acquisition system (SCADA) to the controllers (cyber and physical). These will be compared with quality measurements from the bioproduction process examining anomalies, such as spikes in glucose, metabolic and other biologic stochastic changes. This stochastic complexity when run through inference can improve the explainability and measurement of quality as there are certain events or outputs that can be ruled out as we understand what normal likes like in the biology, cyber and physical.

[0000-0003-3230-4415] [0000-0002-8956-8609]

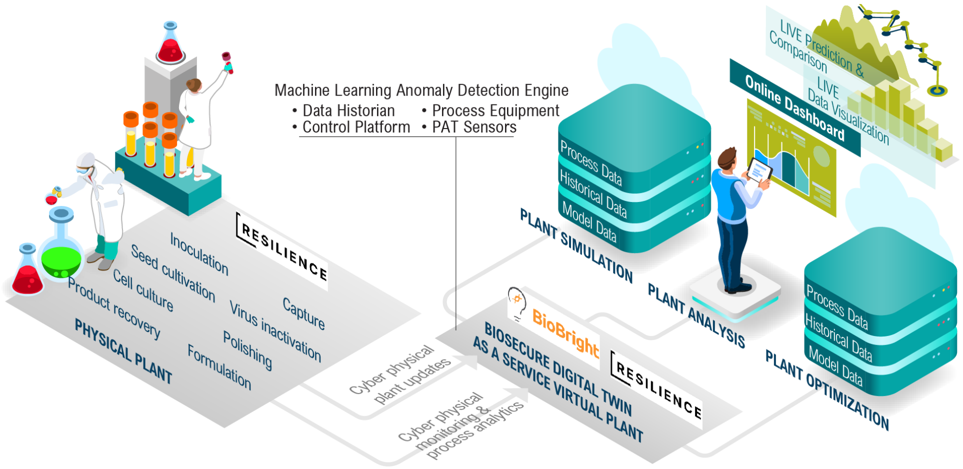


Figure 5. Cyber Physical Anomaly Detection of Machine State Integrity Reference Architecture.

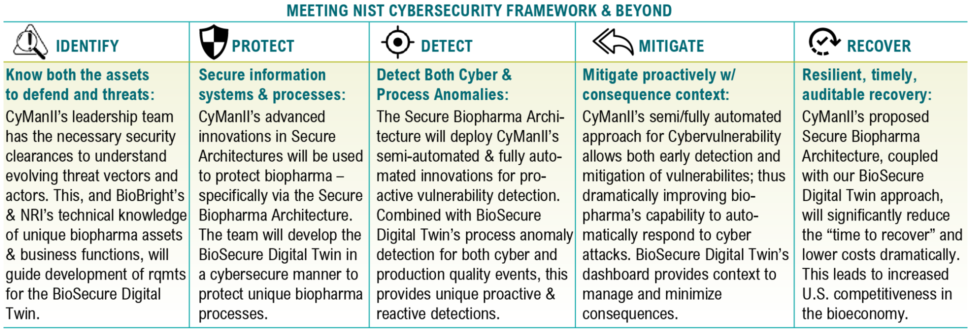
A BioSecure Digital Twin will also help improve analytics and understanding of physical outputs that should never result from certain digital commands and/or functions. This can prevent stealthy replay, supply chain and man-in-the middle attacks as well as human error, while improving production efficiencies and continuous monitoring of machine state integrity and quality of production. Actionable insights on the machine state integrity also helps improve predictive quality analytics of biopharma production process. By collecting, aggregating, analyzing, and running ML inference we can rule out certain faults vs attacks vs environmental vs human error, giving us a higher fidelity view into the machine state integrity and quality of product. There is value beyond the technology and platform, but in the formal methods and framework that enable us to perform the inference, measure what normal looks like and scale a digital twin or physical attestation in virtual form.

Building a framework around this model will help scale and advance security and integrity monitoring to the biopharma sector. Solving this problem requires advances in the current state of the art in control, optimization, and monitoring. Anomalies can be caused by numerous factors and thus detection alone is not a sound solution. To prevent prohibitive false positives and improve actionable and even predictive insight, we need to understand the behavior –including biological in nature- behind the anomalies and have the ability to detect, localize and perform remedial action in more predictive way. This is key to improving integrity and quality in biopharma manufacturing. This capability can help prevent manipulation and error in manufacturing COVID-19 and future vaccines or biopharmaceutical countermeasures. Moreover, this would also help detect stealthy supply chain attacks that continue to target the biopharma manufacturing value chain with increasing frequency and sophistication. Currently, these production systems lack basic encryption, authentication and/or ability to detect these potentially catastrophic attacks.

4.5 Alignment to U.S. Government Cybersecurity Goals for Critical Infrastructure

BioSecure Digital Twin research is in strong complement to several critical U.S. government cybersecurity for critical infrastructure priority areas. The Cybersecurity Manufacturing Innovation Institute (CyManII) is supporting this effort in realization of their mission is to secure the future of U.S. manufacturing, economic vitality, and energy efficiency by developing the future state of "secure by design" for manufacturing automation, advanced supply chain networks, and the digital threads in the engineering design ecosystem.

The BioSecure Digital Twin will improve the ability to identify, protect, detect, respond, and recover to critical cyber threats and vulnerabilities targeting the biopharma manufacturing systems and infrastructure. The following **Figure 6** below highlights specific areas where the BioSecure Digital Twin supports and extends the NIST Cybersecurity Risk Framework.



MEETING NIST CYBERSECURITY FRAMEWORK & BEYOND

IDENTIFY	PROTECT	DETECT	MITIGATE	RECOVER
Know both the assets to defend and threats: CyManII's leadership team has the necessary security clearances to understand evolving threat vectors and actors. This, and BioBright's & NRI's technical knowledge of unique biopharma assets & business functions, will guide development of rqmts for the BioSecure Digital Twin.	**Secure information systems & processes:** CyManII's advanced innovations in Secure Architectures will be used to protect biopharma – specifically via the Secure Biopharma Architecture. The team will develop the BioSecure Digital Twin in a cybersecure manner to protect unique biopharma processes.	**Detect Both Cyber & Process Anomalies:** The Secure Biopharma Architecture will deploy CyManII's semi-automated & fully automated innovations for proactive vulnerability detection. Combined with BioSecure Digital Twin's process anomaly detection for both cyber and production quality events, this provides unique proactive & reactive detections.	**Mitigate proactively w/ consequence context:** CyManII's semi/fully automated approach for Cybervulnerability allows both early detection and mitigation of vulnerabilites; thus dramatically improving biopharma's capability to automatically respond to cyber attacks. BioSecure Digital Twin's dashboard provides context to manage and minimize consequences.	**Resilient, timely, auditable recovery:** CyManII's proposed Secure Biopharma Architecture, coupled with our BioSecure Digital Twin approach, will significantly reduce the "time to recover" and lower costs dramatically. This leads to increased U.S. competitiveness in the bioeconomy.

Figure 6. Highlights how the BioSecure Digital Twin supports and extends the NIST Cybersecurity Risk Framework

4.6 Project Impact, Outcomes, Dissemination

The BioSecure Digital Twin will create an Industrial Immune System to Improve Manufacturing able to rapidly identify anomalies and mitigate the behavior that deviates from the norm, both in the cybersecurity dimension and in process fidelity control. It creates a digital infrastructure that is portable and be deployed as a virtualized testbed for both cyber wargaming and enhanced workforce development.

In the biological dimension, the BioSecure Digital Twin will a) provide enhanced process control techniques that leverage all digital data sources b) create reproducible and portable reference infrastructure deployable to any biomanufacturing facility in the US, c) enable higher quality and faster training of biomanufacturing staff, and d) generate a novel dataset that represents scale-up biomanufacturing processes with unprecedented fidelity in time and detail. In the cyber dimension, the BioSecure Digital Twin will a) create models capable of detecting cyber intruders and attackers in biomanufacturing environments, b) create an infrastructure capable of alerting key operators when these events are triggered, c) create a reference implementation portable and deployable to any US biomanufacturing facility. Through these contributions, the BioSecure Digital Twin will provide the ability to produce medical countermeasures more reproducibly, with higher assurance and in a more distributed manner. It strengthens the resilience of the biomanufacturing infrastructure at the local and national level by providing increased cybersecurity alerting and control. Finally, this proposal creates portable infrastructure and virtual testbeds that enable high-fidelity scenario building (incl. red/blue teaming) and increase the quality and speed of workforce development. This leap in integrity is necessary for our country's ability to prevent, prepare, and respond to the coronavirus pandemic in the face of increased adversarial interference.

4.7 Responding to the Current Coronavirus and Preparing the Next Potential Pandemic

In addition to the BioSecure Digital Twin, we are developing a BioSecure OODA (Observe, Orient, Decide, Act) Loop Framework (BOLF) to be used for the evaluation metrics shown in **Table 3**. This will include a scalable and exportable methodology to measure improvements in cycle time to observe–orient–decide–act to identify, detect and mitigate all hazards in the manufacturing process, both human error and computation, fault, and cyber-attack.

Table 3. Outcomes Evaluation.

Outcomes	Technology	People & Process
Improve Manufacturing Cybersecurity, Integrity and Resilience. The proposed BioSecure Digital Twin provides an Industrial Immune System to rapidly identify anomalies and mitigate maliciously-induced behavior. This meets a national advanced manufacturing need in Pandemic response and is timely because U.S. production is under attack and vulnerable to supply chain and natural hazards that limit an effective response.	We will measure **both the time and accuracy of the Digital Twin** to identify, detect and mitigate manufacturing anomalies and associated hazards. The accuracy will examine the number of false positives detected by ML algorithms with the goal of achieving 98% accuracy and improve awareness of machine state and process integrity. Training sets will be harvested from a) real facilities' attacks, b) virtualized twin environments with in-vitro exploits.	**Dissemination.** We will implement this technology in key biopharma clusters including those on the front lines of the Pandemic response. We will share successes via BIO-ISAC and NIIMBL and CyManII's large consortium of critical manufacturers

Accelerate and improve Efficiency and Scale of biopharma manufacturing process. The proposed BioSecure Digital Twin provides the ability to experiment and perform real time analytics to enhance the industrial competitiveness and economic growth through improving real-time visibility and analytic capabilities of the production lifecycle. It enables researchers to experiment, scale and find other operational efficiencies and gaps without impacting production systems in the loop.	The proposed effort will improve resilience critical systems and processes by detecting and mitigating stealthy cyber-attacks, faults, human error, and other hazards that current defenses can't detect. **We will measure the number of stealthy attacks and hidden faults detected**, the mean time to detection as well as the cost savings from being able to test patches and diagnostics to a system without taking them offline.	**We will measure the cost savings** from hardware in the loop, number of people trained on the twin as well as risk mitigation in having this redundancy.
Lower Cost and National Test Bed Access. The proposed solution considerably lowers the capital costs and increase access to lab and test bed facilities as they are available in a virtual form for experimentation, process improvement and other critical analytic capabilities.	The proposed solution **enables access to critical lab and test bed infrastructure** to NRI and BioBright manufacturing stakeholders as well as a CyManII's and NIIMBL's consortium of academic institutions and students	We will **measure these cost savings** and highlight how secure cloud, virtualization, and advanced monitoring testbeds advance U.S manufacturing capabilities.

4.8 Conclusion

The BioSecure Digital Twin research and developed discussed in this chapter is an imperative response as the frequency, severity and sophistication of attacks has increased exponentially during the pandemic. Current digital biosecurity and monitoring deficiencies allow nation state backed adversaries low-cost and deniable cyber-attacks with a huge impact on public health. The COVID-19 crisis has accelerated the convergence of these two fields and coincides with the emergence of high impact and persistent digital biosecurity attacks. Even relatively simple attacks can cause daily losses in the millions of dollars and can easily cause months of downtime due to circumstances and constraints unique to the bioeconomy. Unfortunately, the entire bioeconomy is currently vulnerable to a wide range of attacks that include targeted ransomware, biological industrial control system vulnerabilities, and bioeconomy-specific laboratory instrumentation vulnerabilities. Unchecked and insecure, our adversaries can hold U.S. citizens hostage to future pandemics or any other public health event, crippling our economy and global competitiveness. While the BioSecure Digital Twin is not a panacea, it presents an innovative approach to move our nation's manufacturing towards resilience.