INL/JOU-22-67545-Revision-0

PURE Biomanufacturing: Secure, Pandemic-Adaptive Biomanufacturing

September 2022

Changing the World's Energy Future

Gabriela F. Ciocarlie, Bo Yu, Duminda Wijesekera, Charles Fracchia, Dongyan Xu, Thomas R. Kurfess, Lisa Strama, Michael Mylrea, Bill Reid, Wayne E Austad, Gregory Edward Shannon, Howard D. Grimes

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

INL/JOU-22-67545-Revision-0

PURE Biomanufacturing: Secure, Pandemic-Adaptive Biomanufacturing

Gabriela F. Ciocarlie, Bo Yu, Duminda Wijesekera, Charles Fracchia, Dongyan Xu, Thomas R. Kurfess, Lisa Strama, Michael Mylrea, Bill Reid, Wayne E Austad, Gregory Edward Shannon, Howard D. Grimes

September 2022

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-EE0009046

PURE Biomanufacturing: Secure, Pandemic-Adaptive Biomanufacturing

Howard D. Grimes and Gabriela F. Ciocarlie | Cybersecurity Manufacturing Innovation Institute, University of Texas at San Antonio
Bo Yu | George Mason University
Duminda Wijesekera | George Mason University and Cybersecurity Manufacturing Innovation Institute
Greg Shannon and Wayne Austad | Idaho National Laboratory and Cybersecurity Manufacturing Innovation Institute
Charles Fracchia | BioBright
Dongyan Xu | Purdue University and Cybersecurity Manufacturing Innovation Institute
Thomas R. Kurfess | Georgia Tech
Lisa Strama | National Center for Manufacturing Sciences
Michael Mylrea and Bill Reid | National Resilience

Biopharmaceutical production systems and processes are vulnerable to cyberattacks from sophisticated adversaries. Therefore, it is imperative to start building biopharmaceutical manufacturing systems that offer verifiable formalism and transform the current state of security across all production stages.

COVID-19 has vividly underscored the vulnerability of global manufacturing operations and supply chains. Biopharmaceutical production systems and processes, in particular, have proved to be vulnerable to cyberattacks from sophisticated adversaries. COVID-19 virus particles—like cyberadversaries—are complex, nonlinear, and rapidly evolving. The risks across all critical infrastructure sectors are growing at a staggering pace, and biomanufacturing has critical consequences for economies and national security impacts. Hence, there is a need for improved visibility and control to achieve robust cyber- and physical security in the coronavirus countermeasure production process that broadly translates to the future transformation of biopharma manufacturing.

The U.S. bioeconomy is estimated at more than 5% of the country's gross domestic product (US$950 billion), according to "Safeguarding the Bioeconomy," a 2020 report from the National Academy of Sciences, Engineering, and Medicine. The country's supply chain as well as its reputation and revenue streams are at stake. Most importantly, the need to safeguard human lives requires us to protect and retain the integrity of our processing machines, production, and distribution workflows through the entire chain of custody. Currently, biopharma cybersecurity[10, 12] is subject to the following:

- *Increasing threat volume*: Adversaries continue to target the biopharma supply chain with increasing frequency and sophistication. Health care and manufacturing are the two largest sectors targeted by cyberattacks. Malevolent parties are continually evolving their tactics, techniques, and procedures. Stealth attacks, such as zero-day, polymorphic ransomware, side-channel, and adversarial artificial intelligence attacks, to name only a few, are very difficult to detect in time on modern IT and operational technology (OT) systems even with sophisticated monitoring.
- *Lack of security*: Exacerbating the challenge is that the industry and its production systems are often vulnerable by design and operation, lacking security, auditability, and verifiability. A historical focus

Digital Object Identifier 10.1109/MSEC.2022.3160465
Date of current version: xxxxxx

on pharmaceutical quality led to the development of rigid processes that are inadequate in the digital age. Processes that ensured integrity in a paper notebook paradigm have become mortal vulnerabilities in an age of automation, shattering the trustworthiness of modern biopharmaceutical workflows. Systems were not designed with cybersecurity in mind and are now interconnected with more networks and critical control data.

- *Lack of security controls*: Meaningful and verifiable security controls are inadequate in the biomanufacturing field: instruments are riddled with exploitable vulnerabilities, historical data integrity controls are easily circumvented, and existing verification and validation procedures (including paper backups) are difficult to verify and easy to manipulate.
- *Stochastic nature of living systems*: The use of living systems in manufacturing applications is vulnerable to availability and integrity attacks as well as human error due to the stochastic nature of molecular reactions and the potential for adverse deviations to arise in biological production processes. Improvements in explainability, availability, and integrity attestation are needed to shore up this critical component of biomanufacturing. These should be combined with agile and rapid supply chains and the production of stable cell lines and other biological mediums needed for rapid response to pandemics and other biologic events.
- *No traceable integrity*: Today's reality is that the industry cannot track, trace, and validate the integrity of the production life cycle with an acceptable level of assurance. Moreover, regulatory guidance and compliance processes have not adapted to the digital era and, in fact, can cause major downtimes and further exacerbate cybersecurity attacks.
- *Conventional cybersecurity approaches are ineffective*: Signature heuristics in intrusion detection systems and firewalls do not recognize patterns and malware (especially for stealth attacks), insider and supply chain exploits enable privileged access, and the average time to detect an adversary in IT systems with monitoring is about 280 days, which is 280 days too long. With critical biopharma manufacturing and associated OT systems, the problem is much worse. There is currently no monitoring or detection that is capable of protecting against sophisticated attacks.

The future state of biopharma cybersecurity needs to solve industry-relevant, advanced manufacturing challenges around cyberphysical simulation, analytics, optimization, and security; be pandemic-adaptive to the stochastic nature of biology and adverse molecular reactions; enhance industrial competitiveness and economic growth; and strengthen national security by developing next-generation defensive capabilities for the critical health-care and bioeconomy sector.

PURE Biomanufacturing

Securing manufacturing, and biomanufacturing in particular, must be a top priority. We face an opportunity for pervasive strategic overmatch via technology innovation inserted into biomanufacturing systems. Supply chains need to be PURE: pandemic adaptive, including operational modes that accommodate pervasive physical (social) distancing and remote work; usable and accessible by authorized personnel (e.g., biochemists and engineers); resilient, agile, and able to withstand physical world challenges, such as pandemics, electrical grid failures, and cyberattacks; and economical so that resiliency and security are maintained at all levels of the supply chain, including small and medium-size manufacturers (see Figure 1). The first step is to undertake a nationwide effort to strengthen and diversify supply chains and manufacturing operations. We must vary and digitally integrate supply chains to make them more robust, resilient, and responsive. As summarized in *Foreign Policy*,[5] a report by Dun & Bradstreet estimates that 51,000 companies around the world have one or more direct suppliers in Wuhan, China, and, globally, at least 5 million companies have one or more tier 2 suppliers in the Wuhan region.[9]

A limited number of primary suppliers does not provide a sufficient level of resilience against acute events and concentrated global demand, as witnessed with masks, needles, and vials at the beginning of the COVID-19 pandemic. Instead, multiple trusted suppliers, dispersed globally, should be cultivated to respond to emerging needs. Supply chains and their operations need to embrace the digital thread to meet more agile and responsive needs (i.e., a communication framework that connects traditionally siloed elements in biomanufacturing processes and provides an integrated view of one asset throughout the production life cycle). This highlights the need to create innovation pipelines that can be quickly accelerated, decelerated, and repurposed in response to shifting national priorities. The result would be a flexible facility with built-in innovation serving to propel U.S. manufacturers to global leadership.

It may be the case that we need to provide pharmaceutical stockpile and inventory diversity in new ways (together with the U.S. Strategic National Stockpile) and an orchestrated effort to develop guidelines that 1) recognize necessary raw materials; 2) ascertain essential designs, templates, and data; 3) identify critical elements of physical infrastructure; 4) aggregate technical expertise and biomanufacturing capabilities that

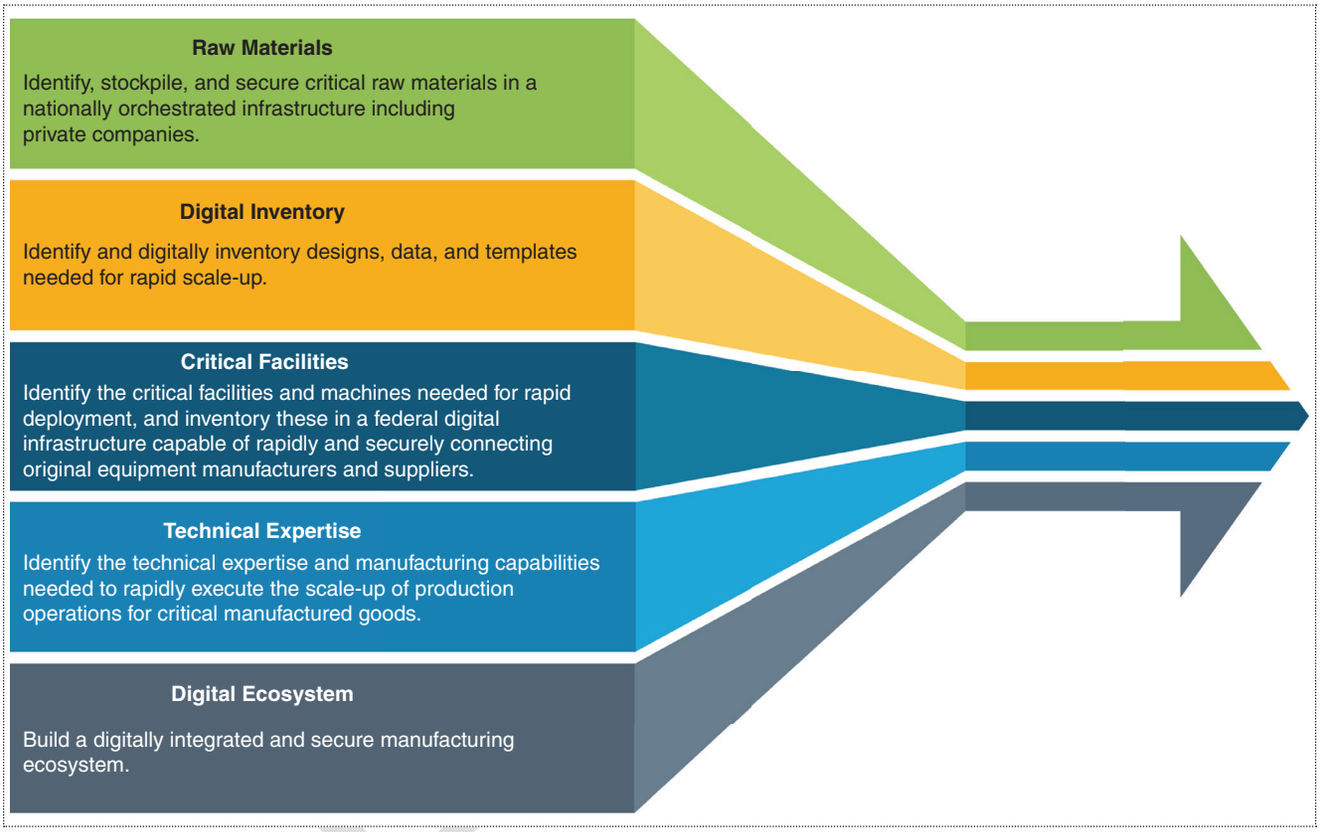

Figure 1. PURE biomanufacturing ensures that resiliency and security are maintained at all levels of the supply chain, including small and medium manufacturers.

can be deployed during emergencies; and 5) formally verify and red-team all digital infrastructure underpinning coordinated responses at federal, state, and local levels (the "Case Study: Paracetamol Production Line" section illustrates how to formally model a production line). This nationwide effort should also develop a plan for mobilizing stockpiles, inventories, and logistics associated with quickly ramping up production. It must also consider the necessary elements, quantities, and modes of secure storage.

Data Integrity: Improve Biomanufacturing Data Integrity

The digital transformation driving biopharma manufacturing has unlocked incredible value to improve scale, the efficiency of production, drug discovery, and even the quality of products. However, there is a need to improve the integrity and availability of digital data, which are easy to manipulate, exfiltrate, and destroy. This is imperative, as quality underpins the manufacturing process, and various frameworks help guide data integrity to be attributable, legible, contemporaneous, original, and accurate (ALCOA), as defined under the ALCOA quality framework. Data integrity needs to be improved to help ensure that the digital transformation does not create new vulnerabilities that can be exploited intentionally and through human error in the unpredictable biological process. One recommendation to realize this goal is to make digital data in the biomanufacturing process self-intelligent, self-protective, and self-aware. One example in the applied space is demonstrated by Keyavi data, which apply advances in layered encryption to improve the dynamic, real-time governance of policies and rule sets that are encrypted and responsive through their chain of custody.

This will help improve the machine state integrity of bioreactors, enabling advances in data provenance and nonrepudiation through the manufacturing process, which will advance the quality and integrity of data through the process life cycle. This will help prevent the spoofing of measurements at the sensor level and man-in-the-middle attacks that manipulate data in transit. Self-protecting data could help enforce the ALCOA framework in a more dynamic way during the manufacturing process by denying adversaries the use of information by default, tracking and tracing data through the production life cycle via improved provenance and nonrepudiation. Finally, visibility in metadata from bioreactors

will improve the fidelity of the biologic process by examining integrity during batch process characterization.

Raw Materials: Identify, Stockpile, and Secure Critical Equipment and Materials in a Nationally Orchestrated Infrastructure

It is economically and technologically disadvantageous to stockpile finished products, especially if they are unused. Rather, we should establish the priorities necessary to respond to health disruptions. This effort should also provide recommendations to the legislative and executive branches of the federal government for critical raw materials and infrastructure. The federal government should direct the Office of the Assistant Secretary for Preparedness and Response to fund the creation and cybersecurity assessment of all the necessary digital infrastructure for pandemic response. An emphasis should be placed on bolstering the resilience of biomanufacturing applications with more agile supply chains and the production of stable cell lines and other biological mediums needed for rapid responses to pandemics and other biologic events. Adaptable and resilient supply chains can be bolstered, in part, by adding modularity that enables the swapping of production organisms and cell lines within existing bioreactor infrastructure. This combines with the availability challenge to produce stable cell lines and manufacturing capacity to rapidly scale up and respond to biothreats on a commercial scale.

Digital Inventory: Identify and Digitally Inventory Designs, Data, and Templates Needed for Rapid Scale-Up

Digital designs that represent a complete product can be continually updated to incorporate innovations so that state-of-the-art systems and capabilities are immediately deployable. These designs, data, and templates will need to be cybersecure to protect intellectual property and must be tested and verified to satisfy U.S. regulatory standards well in advance of their deployment. Particular care must be paid to the portability of such infrastructure and data, as they will enable exponentially greater iteration cycles in times of need. These data should include provisions to share success and failure yields for classes of products. More detailed data can also be retained in a cryptographically secure manner, to be unsealed only when needed by the invocation of the Defense Production Act or a similar trigger. This would balance the need for IP production with the national interest. The resulting sharing of methods and detailed past batch results by cell line, backbone, target product, and product class, in all likelihood, would significantly cut production times and boost yields across the industry.

Critical Facilities: Identify Critical Facilities and Machines for Rapid Deployment and Inventory Them in a Federal Digital Infrastructure

A federated approach should produce recommendations for the type and number of critical facilities and machines that are needed to quickly ramp up automated production. Inventorying this infrastructure ensures that we know where the necessary assets are located and how we can aggregate them for maximum efficiency. Furthermore, these facilities must be tested on a regular basis to verify their ability to produce the necessary materials with the requisite quality. Such tests must be conducted end to end for a variety of products and key backbones for rapid pandemic responses. This approach would help identify which facilities have the best knowledge and processes to scale up a variety of prophylactic countermeasures.

An alternative would employ a market-driven supply chain network that self-organizes and automatically generates manufacturing plans that the involved parties agree on. This is particularly important when considering single- and multigovernment coordination in response to a pandemic-level threat. In industry, this could be successfully done for precompetitive components of a system that are considered common burdens. For example, it is conceivable that companies, which otherwise compete on products, have an interest in identifying and improving the sources of fault in a resin or single-use bag. This is an acute problem due to the centralization, brittleness, and complexity of the biomanufacturing supply chain.

Technical Expertise: Identify the Technical Expertise and Manufacturing Capabilities Needed to Rapidly Scale Up Production

These assets are inventoried in the same centralized digital infrastructure along with facilities and machines and can be aggregated and mobilized for maximum efficiency. In essence, we need to create flexible factories coupled with nationally inventoried raw materials, digital designs, infrastructure, and expertise that can be rapidly deployed and activated on demand. This digital infrastructure will also help the coordination of several facilities and, in particular, their interdependent scheduling for the performance of several key steps, such as scale-up, downstream processing, and fill–finish operations.

Digital Ecosystem: Build a Digitally Integrated and Secure Manufacturing Ecosystem

Companies scrambling to produce and distribute vaccines during the COVID-19 pandemic highlighted the need for a digitally integrated manufacturing ecosystem.

For instance, automotive companies made valiant attempts to change their production lines from cars to respirators. This is not unlike efforts during World War II, when car factories churned out bombers. However, biomanufacturing factories must be able to pivot their operations in a few days or weeks at most, rather than months or years.

While digital automation has optimized the visibility and control of industrial production processes, it has also introduced vulnerabilities. Digital systems that support the bioeconomy are susceptible to theft,[3] manipulation,[2] and disruption.[1] The critical step in securing the bioeconomy's workflows and supply chains is an improved ability to monitor operations and establish trustworthy and attested signals of baseline operation. Absent that capability, the biopharma manufacturing workflows that underpin the U.S. bioeconomy will remain vulnerable to attack, disruption, and manipulation and impossible to trust.

There are two critical factors to accelerate future vaccine production. First, the components that are needed must be sourced from a diversified and resilient supply chain with a reduced dependence on one country, such as China. That supply chain must be able to take the digital designs of the various components and scale up production to meet demand across multiple and potentially competing commercial performers. Second, a location must be ready to receive components, assemble them, and test and validate final products. When a vaccine shipped, for instance, it would have a "digital passport" certifying that every component was made to specification and that it was produced to meet all required standards. Every artifact in the passport would be associated with an agent (e.g., a machine or user) as well as a record of its creation and subsequent operations on it, including the embodied energy.

All passports would be signed by agents at creation. The indexed manufacturing data would enable per-product verification and validation. Furthermore, a cyberphysical ledger infrastructure for the entire supply chain network would be employed to record the presence of operations on every artifact and maintain its "passport" validity. Based on the ledger's records, advanced equipment and product management functions could be developed (e.g., counterfeit detection, product recalls, and supply chain rerouting for energy efficiency) using privacy-preserving capabilities. We would then have a supply chain and manufacturing process that was "rooted in trust" and technically auditable in a tamperproof or cryptographically tamper-evident manner. The challenge to creating such an architecture, though, remains the ability to instrument the supply chain network while ensuring security guarantees across the full processes.

Expounding on this example, it is not necessary to have a large stockpile of respirators stored in warehouses and ready for distribution. The storage of complex products such as these is costly; respirators degrade over time and become outdated. Rather, manufacturers must rapidly produce new machines when needed and ship them without delay. For components that can be readily made, one might simply stockpile the tooling. For example, molds for polymer parts could be stockpiled. When the parts are needed, the molds could be rapidly used. Taking this concept one step further, the designs of the molds could be digitally stockpiled so that the forms could be rapidly manufactured via traditional processes and next-generation technologies, such as 3D printing (additive manufacturing).

Ultimately, parts that lend themselves to digital inventorying will be stored in a cyberwarehouse, and those that are not easily and rapidly manufactured will be stockpiled. Examples of parts that could be digitally inventoried are the specialized connectors used in a respirator, whereas components such as motors might be physically stockpiled. Over time, as manufacturing technology advances, even more complex components, such as motors and elements of motors, might be digitally inventoried. However, we must dedicate the necessary resources to prepare adequately for these scenarios, which includes the creation of digital warehouses and their cyberverification ahead of the next pandemic.

Pursue Manufacturing Innovation With Security Guarantees

To enable innovation and competitiveness in advanced biomanufacturing and protect U.S. innovations and assets, we must secure supply chains and manufacturing operations. A pandemic-adaptive biomanufacturing architecture is necessary to support the orchestration of individual manufacturing automation systems so that local PURE production standards are practiced. Parts must be genuine and certified to precise specifications. Equally critical is protecting manufacturing facilities from cyberattacks that could threaten—and have hampered—production capabilities. Any of these scenarios could prove disastrous by harming people and curbing the country's ability to respond to an emergency.

This PURE architecture must introduce sound cryptographic techniques to transform the physical identities of parts and products into robust digital passports. With the advent of digital, machine, and expertise inventories, we can create, upgrade, and sustain flexible factory operations to efficiently, effectively, and rapidly scale up production. Thus, a PURE digital manufacturing architecture enables pandemic-adaptive, resilient, and trusted supply chains. It is important that vaccines developed by our researchers be reliably scaled up to

hundreds of millions and even billions of doses. Every vaccine must be genuine, produced to an exact formula, and free of tampering (the "Case Study: Paracetamol Production Line" section illustrates the complexity of formal modeling to prevent attacks). In today's biosecurity environment, vaccine production facilities must adopt a well-conceived digital architecture to become secure, more efficient, flexible, and resilient. Their survival and the health security of the nation depend on it.

Creating and maintaining physical, digital, and workflow expertise enables distributed modular manufacturing and quick pivots on the factory floor in response to pandemics. Performing instantiations of these processes enables analysis of the tradeoffs between granularity for stockpiling and production cycle time and lays the foundation for more distributed and resilient production capacity. By inventorying the basic building blocks for physical and digital elements, we construct the basis for a root of trust in the physical and cyber worlds. Thinking beyond the single instantiation model, this integrated facility approach creates a pathway to spin up new products. The secure digital monitoring of the supply chain provides the ability to reprogram everything and adapt the granularity to the current state of the entire supply chain network within hours. We are securely "automating the automation."

PURE must leverage advances in digital twin technology that significantly improve data collection, integration, and analysis of advanced manufacturing in other sectors for diagnostics (failure analysis) and prognostics (predictive analysis) to ensure that all faults are handled in an acceptable manner. If these emerging concepts are successfully extended to the biophysical–cyber domain, they would permit biopharma manufacturing to rapidly detect and address issues in an otherwise insecure ecosystem that is currently a transitional mix of legacy and futuristic technologies. This will translate into improved competitiveness and resilience for U.S. biopharmaceutical manufacturing, which is complex, stochastic, and vulnerable to cyberattacks from multiple nation–state adversaries.

Like other domains, biopharma manufacturing does not exist in an isolated sector. Manufacturing is inherently a cross-sector, multidisciplinary area and requires integrated and robust security across a factory's digital automation, supply chain, and quality checks. This is also true of the integrity of the full "digital thread" of information, from disease sequencing, therapeutic concepts, and biologic design to pharmaceutical production and the logistics of packaging and distribution. To achieve resilience in today's cyberthreat landscape, security solutions must limit their attack volume, defined as the external attack surface area × internal supply chain/latent vulnerabilities, across an increasingly interconnected ecosystem of sectors and cyberphysical domains. Vulnerabilities are central to the challenges of information cybersecurity as well as cyberphysical process security, where complex external attack surfaces are combined with internal cyberphysical process vulnerabilities (known, latent, and supply chain inserts) with high-impact physical consequences.

Nullifying vulnerabilities early in the digital life cycle is the foundational component of preventing successful attacks as we deploy new technologies, even new security (and prognostics) technologies, such as digital twins. The PURE architecture is intelligent in self-monitoring and learning about past and ongoing operations, supplies, and demands; predicting and raising alarms about "the unexpected" (e.g., supply shortages, quality degradation, and manipulation); and proactively proposing supply chain repurposing/rerouting plans that minimize cyber, physical, and economical risks and disruptions.

Case Study: Paracetamol Production Line

We use the production of paracetamol[7, 14] as an example drug manufacturing workflow. Any cyberphysical attack that leads to an alteration in the production process becomes a safety concern. However, by formalizing the production model, we can verify the correctness of the process. We note that the case study does not reflect all aspects in the PURE biomanufacturing architecture; it focuses only on the production stage and benefits of correctness verification of the manufacturing process.

Modeling the Paracetamol Production Line

Paracetamol-d4,[7] with a molecular structure of $C_8H_9NO_2$, also known as *acetaminophen* (and sold under the brand names Tylenol and Panadol), is a common medication used to treat fevers and mild-to-moderate pain. Globally, it is one of the most commonly produced generic drugs. Its workflow is common among facilities in many countries, and it is governed by Code of Federal Regulations 12.221,[6] which specifies mandated and recommended safety precautions, including procedures to be followed by personnel managing the production line. All biopharma producers have to satisfy the federal mandate and any other subject-specific recommendations and industry standards. We now formalize the common workflow for paracetamol—also graphically described in Sharma et al.[15] and verbally in Ajala et al.[4]—using Yet Another Workflow Language (YAWL),[8] an executable workflow language and execution environment. We also need a formalized workflow to describe the quantities of chemicals used in the production steps, as shown in Table 1.

The top-level workflow, given in Figure 2, describes the main stages (starting at the left and flowing to the

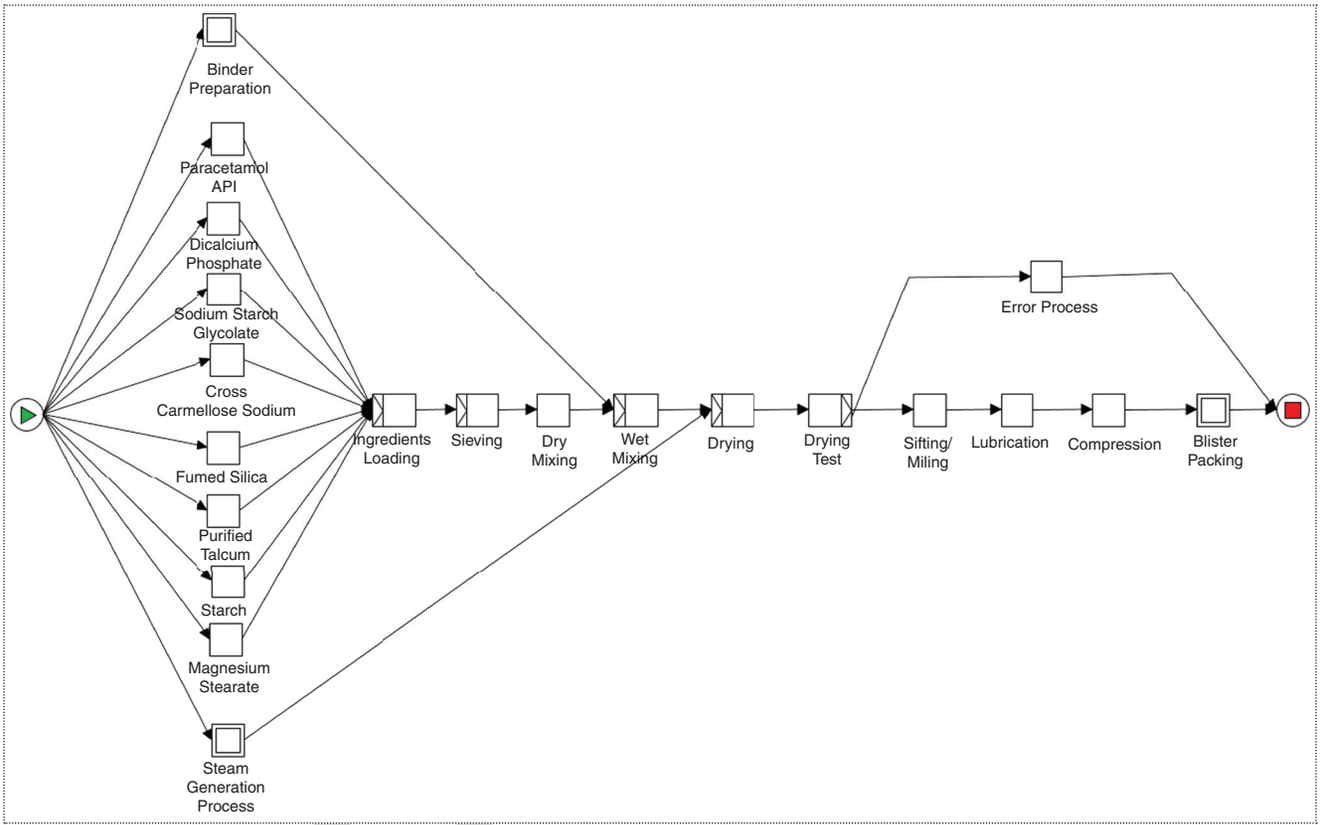

Figure 2. The high-level paracetamol production workflow. API: application programming interface.

right), consisting of ingredient loading, sieving, dry mixing, wet mixing, drying, drying testing, sifting and milling, lubrication, compression, and blister packing. As an executable workflow engine, YAWL has its own artifacts, such as the green arrow at the leftmost position, to enable the process to start executing, and the red square at right, ending or handing over control to a calling workflow. The tall vertical line shows many inputs; some are human, through a controller application programming interface, while others are input chemicals, including dicalcium phosphate, sodium starch glycolate, croscarmellose sodium, fumed silica, purified talcum, starch, and magnesium stearate. The plant also needs steam-purified water and steam for later stages.

First, calcium phosphate, croscarmellose sodium, sodium starch glycolate, starch, purified talcum, fumed silica, dicalcium phosphate, and magnesium stearate are loaded into a ready mixer granulator and stirred for 5 min. The output is dry mixed for a few minutes, and then the binder is added and blended for 2 to 3 min. In the next process, steam is used to dry the wet granules for about 10 min. A loss-on-drying (LOD) test is conducted with moisture balancing at 105° C to ascertain that the LOD is within a limit of not more than 2–2.5%. The dried granules are passed through a sifter-cum-multimill using a sieve and 2-mm screen and collected in double-lined poly bags. This is followed by adding sifted lubricants obtained from earlier steps and blending for 10 min. Lubricants are added in the cage blender, and the mix is further stirred for 5 min. The granules are unloaded into double-polythene-lined drums or intermediate process containers and labeled. The next step is compression and packing using aluminum and polyvinyl chloride (PVC) sheets. Every stage of the process has quality requirements as well as fault handling and estimated energy consumption metrics that are not present in Figure 2. A summary of the manufacturing processes is in Table 1.

Here are details of four subworkflows of the processes in Figures 2 and 3. The process of creating the binder is provided in Figure 3, which is the main subworkflow of the paracetamol production pipeline. It starts by heating demineralized water to 80º F to mix starch2, then sent to a container for stirring. Separately, heated demineralized water is used to make a combination of methylparaben sodium, polyvinyl chloride K-30, and propylparaben sodium. This product is sent to the container with starch2 and made into a slurry, cooked for 5 min, and cooled to create the binder that is fed into the wet mixing process of the main workflow.

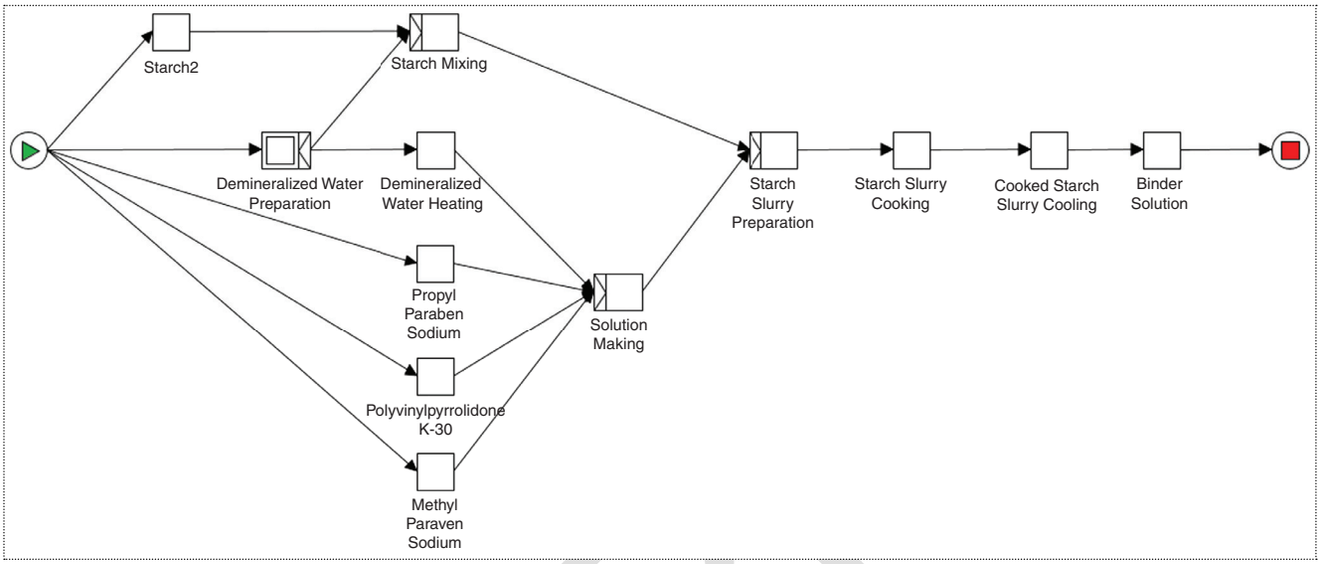

Figure 3. The paracetamol binder production workflow.

Table 1. The paracetamol production steps and quantities.

Name	Material	Amount	Condition	Process
Powder mixture preparation	Paracetamol powder and Avecell, Emcompress or pregelatanized starch	Batches of 60-g paracetamol to others	Ratio of 1:1.5	Mix excipients Store in airtight containers
Dry mixing	500-mg paracetamol powder, lactose 10%, and starch 5%	100 g each	5 min in a mixer	Dry mix
Wet mixing	Dry-mixed binder solution	As needed	A 4% concentration	Moisten
Sieving	Wet masses		1,400-μM mesh Sieve 18 h at 60 C°	Pass through dry sieve in hot-air oven for 18 h at 60 C°
Resieving	Dried mass from sieve		1,000-μM mesh	Granulate finer
Tablet preparation	Output from dry sieving		500–1,000-μM granule size	Output granules
Compressing powder	Powder from dry sieve		Lubricate with 10% dispersion of magnesium stearate in acetone Compress for 30 s	Flat-face punch to 10.5 mm and compress for 30 s, in loads of 0.25, 0.5, 0.75, 1, and 1.25 metric tons
Storing tablets	Eject after compression		Stored over silica gel for 24 h	Allow for hardening and elastic recovery

The auxiliary workflows of producing soft water and demineralized water are in Figure 4(a) and (b). Figure 4(c) and (d) illustrate the steam generation process and final blister packing process. Blister processing is done using one compression tablet-making machine that is supplied with compressed paracetamol, aluminum foil, and PVC sheets. The machine compresses the tablets by using two plates: the top one compresses the material into the shape of a tablet, and the bottom one pushes the tablets into a container/bottle.

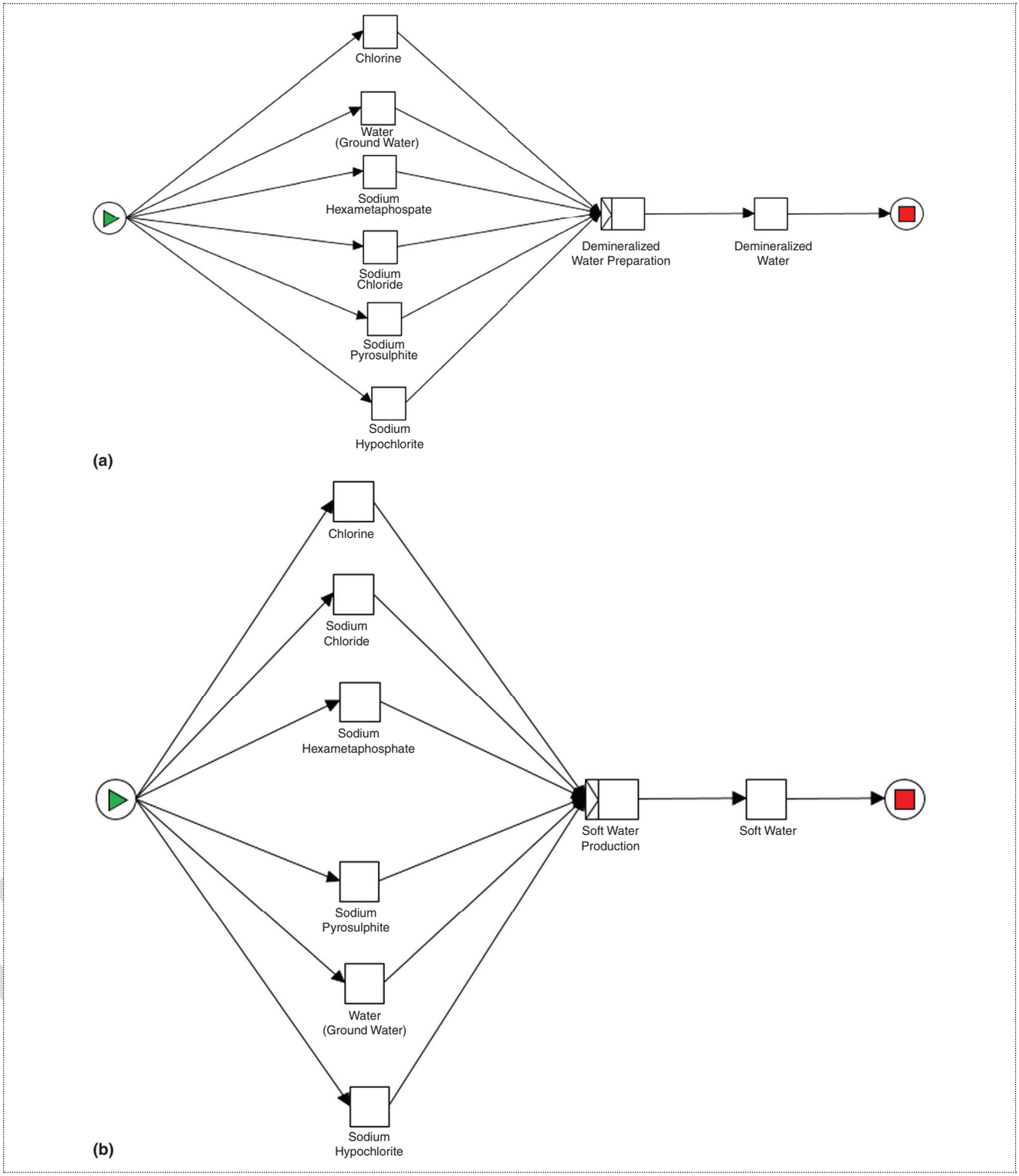

Figure 4. The auxiliary workflows: (a) demineralized water production, (b) soft water production, (continued).

Many quality metrics must be batch checked after every process, such as the size, solubility, and hardness of the tablets. If the samples chosen from a batch do not satisfy the quality check, the whole lot is discarded. Furthermore, if any handler is found to violate hygiene requirements, the whole batch (including the binders) is discarded. Some of the quality attributes are listed in the following:[4]

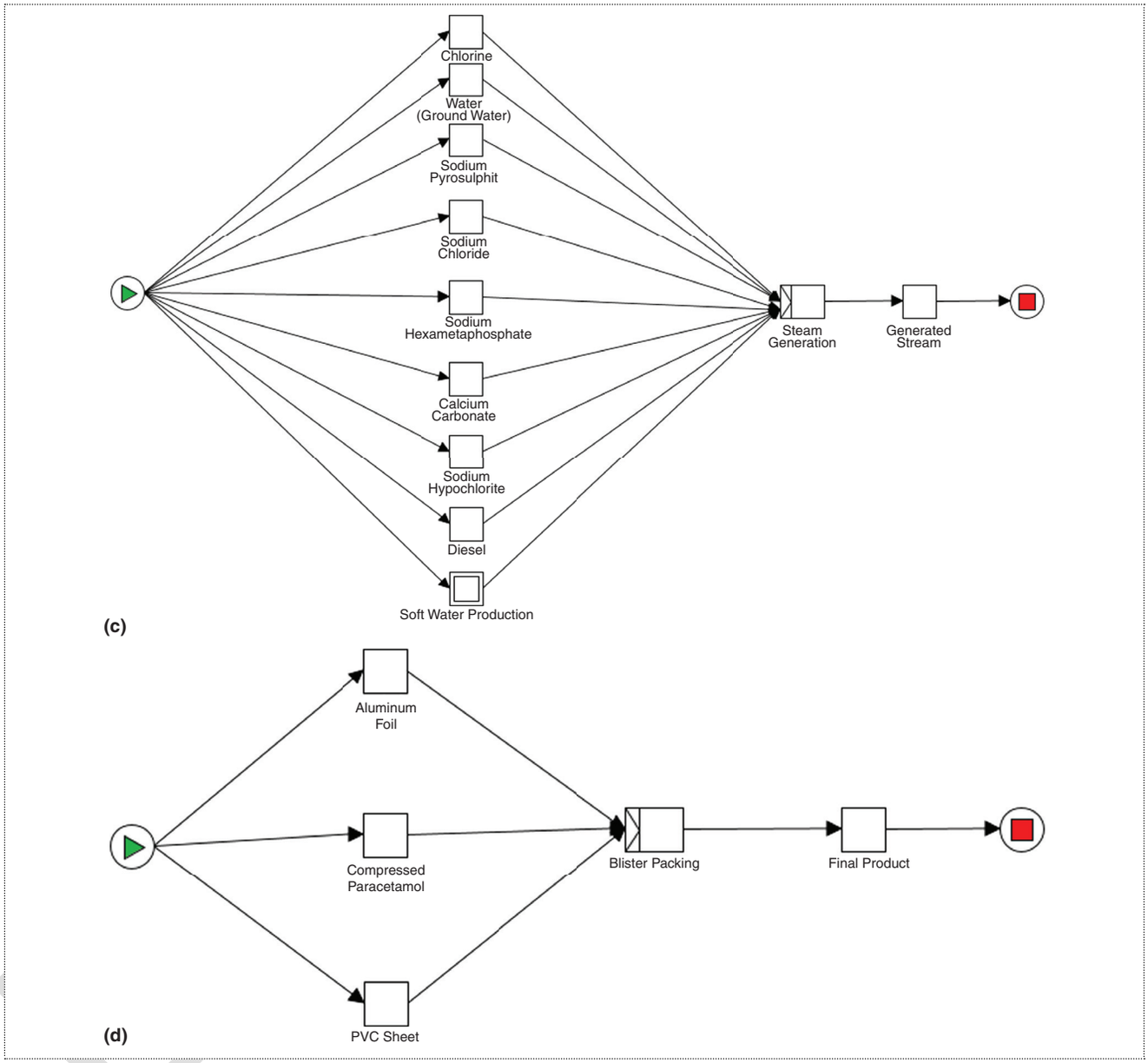

Figure 4. (continued) (c) steam generation, and (d) blister packing.

- *Compressional/granule properties*:
  - *Density tests*: Evaluation of paracetamol: 1) pour 30-g granules through a short-stemmed glass funnel into a 100-ml graduated cylinder, and 2) read the volume occupied by the granules and compute the bulk density (Bt) in grams per milliliter. To evaluate paracetamol granules and paracetamol powder tapped densities, tap the cylinder containing the granules two times from a height of 2 cm and compute the density in grams per milliliter.
  - *Angle of repose*: Take 20 g of granules made using different excipients, and flow them through a funnel from a particular height to form a conical heap on a horizontal surface. As the heap is formed, the particles slip and roll over one another until the mutual friction among them just balances the gravitational force. The angle of the heap against the horizontal surface is the angle of repose, and it is determined by the formula $\tan\theta = h/r$.
  - *Carr's index*: The percentage compressibility is calculated from the difference between the tapped density (Dt) and Bt divided by the Dt; the ratio is expressed as a percentage.
  - *Hausner's index*: Hausner's ratio (HR) is compares the Dt and Bt: HR = Dt/Bt.

- *Mechanical properties of tablets*:
  - *Crushing strength*: The load required to diametrically break every tablet should be determined at room temperature and using a tablet hardness tester.
  - *Friability*: The friability of the tablets should be determined using a friabilator operated at 25 r/min for 4 min. These two parameters should be used to find the crushing-strength-to-friability ratio.
- *Drug release properties*:
  - *Disintegration time*: The disintegration time of the tablets should be determined, and the percentage of paracetamol released at each time needs to be calculated.

Safety and Security Concerns

The paracetamol case study shows numerous aspects of safety and cybersecurity issues. The first is that any exploitable vulnerabilities and faults in the production equipment (i.e., the tablet production machine) can result in pills that do not satisfy compressibility, friability, and disintegration times and thereby have a different Carr's or Hausner's index. During the testing phase, a prechosen number of samples that fail the test results in the rejection of an entire batch, and if a predetermined number of successive batches fail, the quality tests require production to stop. Rejected samples should be safely destroyed, as they should not enter the marketplace through illicit means; the use of defective product can result in adverse medical conditions. Similarly, any attack and fault in the demineralized water production workflow will cause lower-quality results, which may be even more difficult to detect through friability and compressibility tests and may lead to recalls of large numbers of products.

Many aspects of our paracetamol analysis can be applied to other biopharma product lines and especially at the interface of IT and OT systems. Although essential, this interface tends to create attack pathways from one side to the other. Since most IT systems are exploited for profit, using these pathways can lead to inferior, ineffective, and harmful pharmaceutical products going to market despite strict quality control. In addition, many manufacturers ship partially constructed products among facilities, under strict environmental conditions. For example, for vaccine manufacturing, some components are frozen and shipped from one plant to another. Any interference with the logistics may cause a freezer temperature to exceed its threshold. Furthermore, some vaccines need to be used within a limited time after production; altering the production time stamp can make these ineffective, according to strict guidelines.

The formalized workflow is common among the paracetamol production descriptions we could find. Hence, the workflow is portable among the medication's manufacturing lines. Thus, at the process level, failures and cascading failures are the same, but at the workflow engine implementation level, they could depend on software, hardware, an underlying operating system, and networks with different vulnerabilities and failures. The implementation of the workflow management process and the equipment used to execute each step could be different. For example, factories could use various brands of centrifuges and water purification systems with changing vulnerabilities and failures that could arise from individual machines. The value of this kind of analysis is that it shows process-level dependencies. Therefore, if additional failures and faults arise from an individual machine or implementation platform, one could use the process flow dependencies to ascertain their cascading effects and boundaries.

Verification and Validation

One of the solutions we are advancing in our work is to formally model federal regulations and drug-specific recommendations as logical statements and verify that the formally modeled workflow and tests ensure that the guidelines are satisfied. One of the important aspects we focus on, but is missing in previous work, such as Hazzazi et al.[11] and Mirasol,[13] is the dependency on sampling-based acceptance criteria for production batches. Validation requires carefully contrasting a model against actual production lines to capture the workflow accurately. This will lead to security guarantees for production lines, and combined with digitally integrated inventory, it will provide an ability to verify the end-to-end manufacturing process in a PURE architecture.

This article raised awareness of the need to (re) build secure biopharma supply chains that are pandemic adaptive and enable advanced and rapid biopharmaceutical manufacturing. Establishing PURE biomanufacturing requires a coordinated approach that includes universities, national laboratories, private companies, entities such as the National Center for Manufacturing Sciences, and manufacturing innovation institutes. A federally orchestrated response is immediately needed to strengthen U.S. biomanufacturers. ■

Acknowledgments

This material is based on work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy, under Advanced Manufacturing Office award DE-EE0009046.The views expressed herein do not necessarily represent the views of the U.S. Department of Energy and the U.S. government.

References

1. "Hackers from potential 'nation-state' target COVID-19 vaccine supply chain, IBM warns: Cybersecurity experts warned of a phishing scheme spanning six countries." ABC News. https://abcnews.go.com/Technology/hackers-potential-nation-state-target-covid-19-vaccine/story?id=74518869 (Accessed: Mar. 14, 2022).
2. "Supply-chain obstacles led to last month's cut to Pfizer's COVID-19 vaccine-rollout target: Pharma giant found raw materials in early production didn't meet its standards." The Wall Street Journal. https://www.wsj.com/articles/pfizer-slashed-its-covid-19-vaccine-rollout-target-after-facing-supply-chain-obstacles-11607027787 (Accessed: Mar. 14, 2022).
3. "Hackers break into 'biochemical systems' at Oxford university lab studying COVID-19." Forbes. https://www.forbes.com/sites/thomasbrewster/2021/02/25/exclusive-hackers-break-into-biochemical-systems-at-oxford-uni-lab-studying-covid-19/?sh=217ba0ab2a39 (Accessed: Mar. 14, 2022).
4. T. O. Ajala, O. I. Aremu, P. A. Segun, and J. O. Ayorinde, "The effect of formulation methods on the mechanical and release properties of paracetamol tablets," *J. Pharmaceutical Allied Sci.*, vol. 8, no. 2, pp. 1327–1342, 2011.
5. E. Braw. "Blindsided on the supply side." Foreign Policy. http://www.foreignpolicy.com/2020/03/04/blindsided-on-the-supply-side (Accessed: Mar. 14, 2022).
6. "21 CFR part 211 - Current good manufacturing practice for finished pharmaceuticals." Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-C/part-211 (Accessed: Mar. 14, 2022).
7. "Analgesic combination, acetaminophen/salicylate (oral route)." Mayo Foundation for Medical Education and Research. https://www.mayoclinic.org/drugs-supplements/analgesic-combination-acetaminophen-salicylate-oral-route/proper-use/drg-20069948 (Accessed: Mar. 14, 2022).
8. *Yet Another Workflow Language (Yawl)*. (1998). YAWL. [Online]. Available: http://www.yawlfoundation.org
9. R. Gibson. "ChinaRx: Exposing the risks of America's dependence on China for medicine," China Rx. https://www.chinarxbook.com (Accessed: Mar. 14, 2022).
10. D. Guttieres, S. Stewart, J. Wolfrum, and S. Springs, "Cyberbiosecurity in advanced manufacturing models," *Frontiers Bioeng. Biotechnol.*, vol. 7, p. 210, Sep. 2019, doi: 10.3389/fbioe.2019.00210.
11. N. Hazzazi, J. Albasri, B. Yu, D. Wijesekera, and P. Costa, "Using temporal logic to verify the blood supply chain safety," in *Emerging Trends in Applications and Infrastructures for Computational Biology, Bioinformatics, and Systems Biology*, Q. N. Tran and H. R. Arabnia, Eds. New York, NY, USA: Elsevier, 2016, pp. 267–292.
12. J. John, M. Mylrea, M. Nielsen, and M. Abbaszadeh, "AI driven cyber physical industrial immune system for critical infrastructures," in *Systems Engineering and Artificial Intelligence*, W. F. Lawless, D. A. Sofge, and R. Mittu, Eds. Cham: Springer Nature Switzerland AG, 2021, pp. 1–22.
13. F. Mirasol, "Automating the biomanufacturing process," *BioPharm Int.*, vol. 32, no. 3, pp. 26–30, 2019.
14. "What you need to know about acetaminophen (Tylenol)." Association of Medical Ethics. http://www.ethicaldoctor.org/medical-ethics/articles/americas-most-popular-drugs/tylenol/ (Accessed: Mar. 14, 2022).
15. R. K. Sharma, P. Sarkar, and H. Singh, "Assessing the sustainability of a manufacturing process using life cycle assessment technique—a case of an Indian pharmaceutical company," *Clean Technol. Environ. Policy*, vol. 22, no. 6, pp. 1269–1284, 2020, doi: 10.1007/s10098-020-01865-4.

Howard D. Grimes is the organizer and director of the Cybersecurity Manufacturing Innovation Institute, University of Texas at San Antonio, San Antonio, Texas, 78249, USA. His research interests include plant genomics, proteomics, metabolomics, and phenomics; renewable energy research into aviation biofuels; synthetic biology for sensor design; and the global facilitation of intellectual property for pharmaceuticals and plant biotechnology. Grimes received a Ph.D. in biophysics and physical biochemistry from North Carolina State University. He is an elected fellow of the American Association for the Advancement of Science, the author of 65 peer-reviewed publications and multiple op-ed pieces, and the holder of two patents. Contact him at howard.grimes@utsa.edu.

Gabriela F. Ciocarlie is an associate professor in the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, Texas, 78249, USA, where she is also a vice president for securing manufacturing and secure manufacturing architecture at the Cybersecurity Manufacturing Innovation Institute. Her research interests include anomaly detection, application-level security, and cyberphysical and distributed system security. Ciocarlie received a Ph.D. from Columbia University. She is an associate editor of *IEEE Security & Privacy* and a Member of IEEE. Contact her at gabriela.ciocarlie@utsa.edu.

Bo Yu is a research assistant professor at the Command, Control, Communications, Computing, Intelligence, and Cyber Center, George Mason University, Fairfax, Virginia, 22030, USA. Her research interests include cybersecurity, policies, systems, semantic technologies and probabilistic reasoning, and applications of 5G. Yu received a Ph.D. in information technology from George Mason University. Contact her at byu3@gmu.edu.

Duminda Wijesekera is the acting chair of the Department of Cyber Security Engineering and a professor in the Department of Computer Science, George Mason University, Fairfax, Virginia, 22030, USA, and a visiting research scientist at the National Institute of Standards and Technology. His research interests include the safety and security of networked control systems in general (and intelligent transportation systems and industrial automation systems in particular) and Next G-based edge services. Wijesekera received a Ph.D. in mathematics from Cornell University. He is a Senior Member of IEEE. Contact him at dwijesek@gmu.edu.

Greg Shannon is a computer scientist at the Idaho National Laboratory, Idaho Falls, Idaho, 83415, USA and the Cybersecurity Manufacturing Innovation Institute, University of Texas at San Antonio. His research interests include science, technology, and policy for cybersecurity. Shannon received a Ph.D. in computer sciences at Purdue University, with a fellowship from the Packard Foundation. He served as the first chair of the IEEE Cybersecurity Initiative and general chair for the 2015 IEEE Symposium on Security & Privacy. Contact him at gregory.shannon@inl.gov.

Wayne Austad leads the Secure & Resilient Cyber Physical Systems Initiative at the Idaho National Laboratory, Idaho Falls, Idaho, 83415, USA, and is the chief research and development officer at the Cybersecurity Manufacturing Innovation Institute, University of Texas at San Antonio. His research interests include building impactful national security research programs. Austad received an M.S. in electrical engineering from the University of Wyoming, with an emphasis on digital signal processing and embedded systems. He is a Senior Member of IEEE. Contact him at wayne.austad@inl.gov.

Charles Fracchia is the founder of BioBright, Boston, Massachusetts, 02116, USA, and the cofounder of the Bioeconomy Information Sharing and Analysis Center. His research interests include threats to the bioeconomy and enabling coordination among stakeholders to facilitate robust and secure industry. Fracchia received an M.S. in media arts and sciences (Media Lab) from the Massachusetts Institute of Technology (MIT) Media Lab and Harvard Medical School. He has received a number of awards, including recognition among the *MIT Technology Review* 35 Innovators Under 35, IBM Ph.D. fellowships, and the Extraordinary Minds fellowship. He is a member of the DARPA Information Science and Technology Study Group. Contact him at charlesfracchia@gmail.com.

Dongyan Xu is a Samuel Conte Professor of Computer Science and the director of the Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana, 47907, USA. His research interests include computer system security and cyberphysical system security. Xu received a Ph.D. in computer science from the University of Illinois Urbana–Champaign. He is a member of the Association for Computing Machinery and American Association for the Advancement of Science. Contact him at dxu@purdue.edu.

Thomas R. Kurfess is the HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control and a professor of mechanical engineering at Georgia Tech, Atlanta, Georgia, 30332, USA. His research interests include the design and development of advanced manufacturing systems targeting secure digital manufacturing, additive and subtractive processes, and large-scale production enterprises. Kurfess received a Ph.D. in mechanical engineering from the Massachusetts Institute of Technology. He is a member of the National Academy of Engineering and a fellow of American Society of Mechanical Engineers, American Association for the Advancement of Science, and Society of Manufacturing Engineers. Contact him at kurfess@gatech.edu.

Lisa Strama is president and chief executive officer of the National Center for Manufacturing Sciences, Ann Arbor, Michigan, 48108, USA. Her research interests include large-scale manufacturing, product delivery, sales, infrastructure improvements, and supply chain optimization to fill technology gaps. Strama received an M.B.A. in management information systems from DePaul University. She is the 2022 recipient of the Society of Mechanical Engineers International Manufacturing Management Award. Contact her at lisa.strama@ncms.org.

Michael Mylrea is a senior distinguished engineer at National Resilience, La Jolla, California, 92037, USA. His research interests include secure, innovative manufacturing. Mylrea received a Ph.D. in cybersecurity resilience for operational technology from George Washington University. He is an adjunct professor of computer science and distinguished fellow at the University of Miami Data Science Institute, cochair of the IEEE Blockchain Standards Group, and a participant in the Association for the Advancement of Artificial Intelligence, Cybersecurity Manufacturing Innovation Institute, and Center for Accelerated Real Time Analytics. Contact him at michael.mylrea@resilience.com.

Bill Reid is the chief information security officer and vice president of security and privacy at National Resilience, La Jolla, California, 92037, USA. His research interests include privacy-preserving computing and privacy by design. Reid received an M.S. from Tufts University. Contact him at bill.reid@resilience.com.

“Biopharmaceutical production systems and processes, in particular, have proved to be vulnerable to cyberattacks from sophisticated adversaries.”

“Risks across all critical infrastructure sectors are growing at a staggering pace, and biomanufacturing has critical consequences for economies and national security impacts.”

“The need to safeguard human lives requires us to protect and retain the integrity of our processing machines, production, and distribution workflows.”

“Exacerbating the challenge is that the industry and its production systems are often vulnerable by design and operation, lacking security, auditability, and verifiability.”

Today's reality is that the industry cannot track, trace, and validate the integrity of the production life cycle with an acceptable level of assurance.

The average time to detect an adversary in IT systems with monitoring is about 280 days, which is 280 days too long.