8-15-2024

Cybersecurity, Image-Based Control, and Process Design and Instrumentation Selection

Dominic Messina
Department of Chemical Engineering and Materials Science, Wayne State University

Akkarakaran Francis Leonard
Department of Chemical Engineering and Materials Science, Wayne State University

Ryan Hightower
Department of Chemical Engineering and Materials Science, Wayne State University

Kip Nieman
Department of Chemical Engineering and Materials Science, Wayne State University

Renee O'Neill
Department of Chemical Engineering and Materials Science, Wayne State University

See next page for additional authors

Recommended Citation

Messina, D.; Leonard, A.F.; Hightower, R.; Nieman, K.; O'Neill, R.; Beacham, P.; Tyrrell, K.; Adnan, M.; Durand, H. Cybersecurity, Image-Based Control, and Process Design and Instrumentation Selection. Syst Control Trans 3:186-193 (2024). https://doi.org/10.69997/sct.182710

Systems & Control Transactions

Research Article
Foundations of Computer Aided Process Design (FOCAPD 2024)
Breckenridge, Colorado, USA. July 14-18, 2024
Peer Reviewed Conference Proceeding

PSE PRESS

Cybersecurity, Image-Based Control, and Process Design and Instrumentation Selection

Dominic Messina[a], Akkarakaran Francis Leonard[a], Ryan Hightower[a], Kip Nieman[a], Renee O'Neill[a], Paloma Beacham[a], Katie Tyrrell[a], Muhammad Adnan[a], and Helen Durand[a]*

[a] Wayne State University, Department of Chemical Engineering and Materials Science, Detroit, Michigan, USA
* Corresponding Author: helen.durand@wayne.edu.

ABSTRACT

Within an Industry 4.0 framework, a variety of new considerations are of increasing importance, such as securing processes against cyberattacks on the control systems or utilizing advances in image processing for image-based control. These new technologies impact relationships between process design and control. In this work, we discuss some of these potential relationships, beginning with a discussion of side channel attacks and what they suggest about ways of evaluating plant design and instrumentation selection, along with controller and security schemes, particularly as more data is collected and there is a move toward an industrial Internet of Things. Next, we highlight how the 3D computer graphics software tool set Blender can be utilized to analyze a variety of considerations related to ensuring safety of plant operation and facilitating the design of assemblies with image-based sensing.

Keywords: Industry 4.0, Dynamic Modelling, Nonlinear Model Predictive Control, Simulation, Cybersecurity, Instrumentation, Image-Based Control

INTRODUCTION

Industry 4.0 is introducing new considerations in production environments, including considerations with respect to cybersecurity, imaging, and control. While these concepts are important considerations for process operation, they also have implications for next-generation design selections (and their interactions with controllers). This work considers the implications of cybersecurity concerns and the application of image-based control on the specifications and design of modern-day processes, as well as their coupling to controllers.

CYBERSECURITY

In this section, we use a discussion of cryptography and side channel attacks to present possible future research directions related to the intersection of process design, control, and cybersecurity. Traditionally, cybersecurity has been considered to be a problem most relevant to computer scientists and information technology (IT) professionals. The details of how attacks occur can require an understanding of details of computer hardware and software that typically go beyond traditional chemical engineering fundamentals (e.g., understanding operating system fundamentals related to bootloaders, kernels, and assembly language). However, there has been a growing interest in investigating the relevance of cybersecurity to chemical engineering decisions (e.g., process control [1,2]). Cybersecurity has also begun to be discussed from a process design perspective. For example, in [3], we discussed how different designs lead to different worst-case operating conditions under an attack (similar to an inherent safety perspective). [4] refers to using a Computer Systems/Controls Hazard and Operability Analysis, highlighting interactions between the design of the computer systems and controls safeguards and the process design. This section seeks to make additional connections between process design and control system cybersecurity, with the intent to showcase potential directions in which the process design community might be able to contribute to securing systems in a manner that seeks to promote efficiency. We focus on two areas: design concepts inspired by active detection strategies, and design concepts inspired by side channel attacks.

Design Lessons from Active Detection

In the first of the two cybersecurity design perspectives, we discuss learnings from our recent work in cybersecurity of control systems. Our prior work has investigated how to use control signals to disturb the process operation in a manner that would be (ideally) difficult for an attacker to predict, such that they are unlikely to evade detection because they will create process state trajectories that are not in accordance with operating expectations [5,6]. Active detection strategies such as these that attempt to probe for attacks have an advantage over passive detection strategies that they can attempt to use clever operating policies to make it difficult for an attacker to remain undetected. However, they also disrupt operation and thus may be challenging to use in practice. However, this raises the question of whether equipment could be designed that could facilitate locally disruptive behavior but global meeting of process specifications (e.g., through designs that might promote mixing in some areas and laminar flow in others to attempt to allow for active probing with certain cleverly placed actuators and sensors within the design but in a manner that would overall have a minimal impact on actual process output/performance). This analysis indicates that one potential future direction in process design (and particularly in simultaneous design and control) is to analyze whether process and equipment designs that promote an ability to probe for cyberattacks using controllers could be developed.

Cryptography and Encryption

The second potential design direction related to cybersecurity that we discuss is inspired by side channel attacks that attempt to locate decryption keys by monitoring the power supplied to a computing system. To facilitate the discussion, we begin with a high-level discussion of encryption and then of side channel attacks, and then discuss a conceptual example indicating the potential direction in process design for cybersecurity.

An Overview of Cryptography

Cryptography has received attention in a control context, including with respect to strategies referred to as homomorphic encryption which is a method that allows for certain mathematical operations to be performed on ciphertext such that the decrypted result of an operation on two ciphertexts is equal to the result of operating on the corresponding plaintexts. This has been considered of interest for investigating the implementation of control laws on encrypted data on the Cloud to attempt to improve the privacy of information which might be sent to the Cloud for processing (e.g., [7,8]). A fundamental aspect of cryptography entails the encoding of publicly-readable ‘plaintext’ into ‘ciphertext’ (i.e., encrypted data) such that meaningful information can only be retrieved by intended parties. A popular kind of encryption is public key cryptography, which utilizes two separate keys to encode and decode information. This is done so that any party may encrypt a message using a widely available public key, but only the intended recipient has access to the secret key needed to decrypt. Public key cryptosystems have four main components: the public key, the secret key, and the encryption and decryption algorithms.

One way to promote privacy of information transferred throughout a control loop is to encrypt state measurements to be sent to a controller, where they must then be decrypted before computations can be performed. The resulting control action is then re-encrypted and returned to the actuators to be decrypted and actuated. This setup protects against so-called man-in-the-middle attacks, in which private information is intercepted in transmission. However, in general, side channel attacks can lead to information being obtained from a computing device that might reveal encryption keys. Thus, we discuss side channel attacks in the following section.

Side Channel Attacks

Side channel attacks take information from the processes that generate them [9]. This information is known as a trace. Operations in circuits follow cryptographic algorithms, and the implementation of these cryptosystems can leak data about these operations. For example, timing of the messages may reveal information. Power usage is a form of information leakage as a computer would use different amounts of power based on what it is computing. There are different types of power analysis (e.g., differential power analysis (DPA) and simple power analysis (SPA)). As a side channel attack, the focus is on data leakage from an encryption-decryption process. The cryptographic operation will require power as the device computes and this is where the data leakage occurs.

[10] details how power consumption is directly related to data transmission. Data busses, metal wires within the circuitry, function as mini capacitors by charging and discharging as they transfer data between device components. This charging and discharging consumes power. In a data bus, there is a power line, or rail, that represents the states 1 or 0, and there is a ground line. Data is transmitted as states of on, 1, or off, 0. The size of the bus determines how many bits of data can be transmitted. As data is processed and transferred, electronic switches known as FETs, or field-effect transistors, open and close depending on the state.

The state can change depending on what the bit needs to be set to in the data. To change the state, charge is applied or discharged and this requires some work to be done and power consumed. On a data bus line, the transmission follows a counter and every time a bit is set to either 0 or 1. The electronic switches control the state; if the bit is first set to 0 and then set to 1 in the next iteration, the power rail switch will close and the ground rail switch will open. When the power rail switch closes, 5 volts is now being supplied and the bit is set to 1, or “on”. The 5 volts supplied increases the power consumption, which when graphed visually could be represented by a spike in power consumption. This is important to a side channel attack because data sent through the chip will travel through these data busses, having an effect on the power consumption of the device. As there is a change in state and power is consumed, we can consider that power consumption is equivalent to the number of bits set to 1. Then, when trying to attack a system using power analysis, one can look for similarities in power consumption.

In [11], an example in which plaintext interacts with a secret key through the exclusive or (XOR) operation is performed (XOR yields a true output if only one of two conditions is true); this output is then sent to a look up table of values, which are further processed. Information is obtained after some of these operations from the circuit toward guessing keys for the encryption.

The purpose of a power analysis attack is to find patterns in the power consumption. We would expect that the number of bits set to 1 relates to power consumption, so the power consumption should be similar for outputs that share the same number of 1’s. When attacking, multiple attacks will be done to test different hypothetical keys and then an attempt will be made to determine which key is best supported by the power consumption data. Using the model of encryption and decryption with the hypothetical keys, one can obtain a hypothetical output, with its number of ones. If one of the keys chosen was right, the number of ones should relate to the power consumption, and correlations should be present in the data when evaluated for multiple rounds of the hypothetical key.

A power attack is considered a physical attack because, for example, a digital oscilloscope managed by a computer would be connected to the device under attack. While the device performs its rounds of cryptographic operations, traces of the power consumption are recorded and stored on a computer with the corresponding cryptographic data. Then, an informed guess is made for what selection function to use when partitioning the sets of traces into subsets for the averaging step used for determining if correlations exist between the partitioning strategy and the power consumption data (an example of a selection function is the predicted value of a certain bit). A piece of the hypothetical key is related to selection functions that will be used to define the subsets of traces. The averages of the subsets defined by the selection function outputs are computed for each selection function used in the previous stage. The final stage of analysis is to analyze the test results with either data visualization or data automation, like scripts, to determine which of the hypothetical keys is best supported by the data to be the unknown key. With the key, one can work backwards to the original plaintext.

Concepts for Process Design

Power analysis targets the consumption of power in a device to glean information from the possible operations underway; this raises the question of whether an industrial process leaks information that is intended to be encrypted or otherwise protected from attackers. To demonstrate one concept, consider an extreme case in which a process is designed where the process dynamics are fully known, and it is desired to keep track of the energy consumption of the process as a whole since that might be reflective of a sustainability objective. If the power requested of the actuators is exactly what is applied, and the only other sources of power usage are in executing known computations (except the encryption schemes), there may be a possibility that the data on the power usage could contain some information of value in a type of side channel attack based on the discussion above. This indicates that another potential direction for process design (and its intersection with control) with respect to cybersecurity is attempting to identify how process designs, combined with the measurements being taken in an era of Big Data and the industrial Internet of Things, may or may not cause hidden details of algorithms intended to promote security and privacy to be compromised.

IMAGE-BASED CONTROL

In this section, we move away from the discussion of cybersecurity in process design toward a discussion of the role of an 3D graphics tool set called Blender in design principles, both related to how to design/research safety monitoring strategies (with the aid of simulations that allow testing of visualization components) and in the design of advanced assemblies with image-based actuation.

Blender

Blender is a 3D graphics tool set with capabilities for modeling, animation, and image rendering. It contains a Python interface that can be used to interface codes with the animations, providing a framework for testing ideas for design and control that require an image component. Our group has recently begun to investigate the potential of the 3D graphics software Blender toward image-based control design, with an example of a render of a rod moving stochastically and under a control policy selected based on value iteration [12]. The image-based control simulation performed using the rod utilizes the coloring of the rod at both ends to help differentiate the rod from the background for the image processing algorithm. If the rod does not have these types of features, procedures such as edge detection may be required to help identify the boundaries of the rod, and the different sides of the rod may not be visually distinguishable. This example indicates that the selection of the process design (e.g., how the visuals will appear in a camera) can directly affect the available image-based control techniques and methodologies, again highlighting an intersection between design and control for next-generation manufacturing systems. The remaining examples of this section that utilize Blender (focused on object detection for safety purposes and materials design) highlight other potential uses of Blender in ensuring safe plant operation and in setting specifications of advanced assemblies as a step toward designing them.

Object Detection and Safe Processes

One of the key features of Blender that suggests its utility for researching the testing and designing of safety features at a plant based on images is that it has both visualization capabilities as well as an ability to import image processing Python packages that can then be used to analyze images generated from the software. To showcase this, Blender was used to represent hose and nut assembly shown in Fig. 1, where an object detection algorithm was created utilizing the Python API. The first objective of the code is to create an animation of the nut being loosened, recording a series of key frames. A second Python code was then created that performs an image detection algorithm. The position of the nut is determined by calculating the changes in red channel values in pixels between adjacent pixel rows and columns and subsequently using these to determine a central point as the location of the nut.

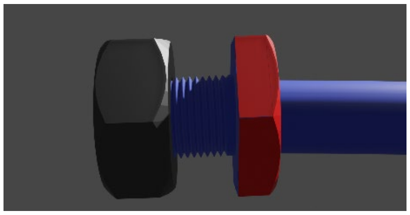

Figure 1. A render of the hose and nut assemply represented in Blender.

Another key opportunity for using Blender to aid with the design of safety enhancements at a plant is that it can be used to represent non-process components as well, such as human interactions with a process. To see this, consider the human walking in a hose room at a plant as modeled in Fig. 2. One idea for a safety algorithm would be to use images to capture the position of a human in this room and then to map those to whether the human is in a safe or an unsafe area. Without a visualization software such as Blender for testing such an algorithm, it may be harder for a process systems engineering researcher to contribute to the development of algorithms which can be used for image-based safety enhancements unless they had a physical system. Blender opens the option of being able to generate images for which tests of whether a proposed safety-enhancing algorithm is applicable can then be tested in simulation for research purposes and for better safety algorithm design. For example, using the Python programming interface in Blender, the coordinates of the human can be extracted in the image in Fig. 2 to serve as a ground truth and then compared with any coordinates obtained from an image processing algorithm to analyze how accurate the proposed image processing algorithm is. Blender thus presents a possible strategy for testing non-traditional safety monitoring components.

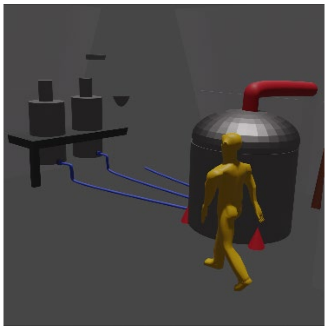

Figure 2. An image of a human walking in a hose room.

Image-Based Control in Assemblies: Blender to Aid with Specification Determination

In this section, we describe another potential use of Blender toward design, in this case focused on how it might be used in first steps toward designing complex assemblies where images are a component. In this example that showcases its potential, we focus on a stimuli-responsive material, and how to set high-level specifications for how it should respond to visual stimuli that could then be passed downstream in the design pipeline to those who design the molecular structure to see if the material can be designed to meet those specifications that were elucidated through the Blender simulations. Stimuli-responsive material assemblies which react to external signals, including optical, audio, chemical, temperature, and physical signals by means of changing configuration, from the macroscopic assembly to molecular, may have many interesting applications in the future. In this section, we explore the process of creating an initial design of an optical stimuli responsive material assembly. An important aspect of any design phase which we expect to be incorporated in the design of stimuli responsive materials is simulation, in order to understand the dynamics of the material assembly's behavior as well as controller performance under certain situations; as a motivating example, we develop a simulation within the 3D graphics software Blender to provide insights on what considerations should be made in the design of an optical stimuli responsive material assembly.

Material Assembly with Image-based Control

In this example, we explore a potential use case for a stimuli-responsive material assembly which is useful when handled properly, however potentially destructive or harmful when misused or exposed to undesired situations. The concept is that we would like to design a strategy for causing this material to "sense" that it is going to be used in the harmful way, and then to break apart when it thinks it will be used in this harmful way to prevent harm. This is a complex design concept that raises many questions, both in terms of how the material should be physically designed (e.g., which molecules may even achieve such a goal), as well as a from a control and sensing point of view. However, we argue that a first step toward attempting to develop such an assembly is to attempt to design the specifications that we want it to follow, which are not obvious. For example, one could consider many ideas for how the assembly should be set up. The material might be intended to break apart immediately when it sees some type of negative signal in image data, or might be intended to do so gradually. The type of negative signals in the images should also be defined to enable testing of whether the proposed material design would work as intended or whether there would be unexpected corner/edge cases for which it breaks in an undesired manner. We suggest that the flexibility of Blender for simulating objects and their interactions physically and through image processing makes it an interesting candidate for developing potential scenarios, evaluating different "breaking" concepts in these scenarios, and then ultimately providing a test framework to evaluate whether the developed algorithms perform as intended in new scenarios (i.e., in the presence of new image-based sensor signals). In the remainder of this section, we show with a simple case study how Blender could be used toward such pathfinding studies for setting specifications for advanced assembly designs involving image sensing, which serves to suggest Blender's utility for further use and investigation in this direction. This also is meant to motivate discussion on how new paradigms in material design and control are thought of and how they may be used to improve physical safety and provide a line of defense against physical attacks on a system.

We use Blender to create a simple macroscopic model of a non-specific material assembly composed of four blocks connected in a row down the x-axis. Attached to the first block on the long side is a camera pointed away from the assembly down the y-axis, providing optical sensing of the environment. In the camera's field of view is a block which rotates around the z-axis, where each face is a different color, representing different stimuli. These stimuli will be used to indicate whether the block should "break apart" or not. Views of the environment with the assembly and rotating block are shown in Figures 3 and 4 where a camera can be seen attached to the assembly and facing the rotating block. The camera's initial view of the rotating cube is shown in Figure 5. We assume the assembly is equipped with a controller and actuation capable of separating the end block from the rest of the assembly. The simulation begins with the camera looking at the black face of the rotating cube; when the block rotates to reveal the blue face, the controller "breaks" the cube farthest from the camera off of the assembly. As the cube rotates, each time the center pixel changes colors, another block is broken off of the assembly until only the block with the camera remains.

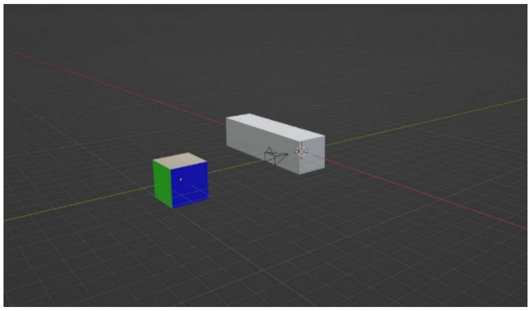

Figure 3. Initial view of assembly and rotating cube.

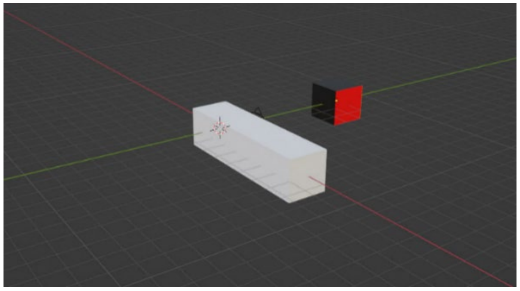

Figure 4. Alternate initial view of assembly and rotating cube.

Figure 5. Initial view of rotating cube from the camera.

More specifically, Blender's Python API is used to initialize the scene described above, where four identical, non-interacting 2x2x2 unit cubes are placed in a row down the x-axis. The first block is centered at (0,0,0), the second block at (2,0,0), and so on, so that the blocks are placed to give the appearance of an assembly. Each block is placed with a rotation of (0,0,0). The camera is placed on the block centered at (0,0,0), with a position of (0,1,0) and rotation $(\pi/2,0,0)$ The rotating block is placed down the positive y-axis at (0,8,0) with a rotation of (0,0,0). Each of the faces on this block has a different base color, four of which will be seen as the block rotates (the "bottom" and top" faces are both colored black for simplicity). The colors are set using RGBA values (red, green, blue, alpha), where blue is (0,0,1,0), green is (0,1,0,0), red is (1,0,0,0), and black is (0,0,0,0). The block rotates around the z-axis according to the dynamic equation $\frac{d\theta_z}{dt} = \frac{\pi}{2}$, numerically integrated using Euler's method with a time step of 0.001 h. At every sampling period $\Delta =$ 0.1 h, a 1920x1080 pixel image of the rotating cube is rendered to a portable network graphics (PNG) file, reflecting the taking of an image by a camera sensor as a measurement of the system. This image is processed by first opening it using the Python package Pillow and loading the image's pixel map to a matrix and checking the RGB value of the center pixel (960,540) to determine which of the four colors it corresponds to. The controller has four modes of action, one associated with each of the possible colors the center pixel can hold in this simulation. Specifically, when the center pixel is black, no action is taken. When it is blue, the first cube is moved away from the assembly. When it is green, the first and second cube are moved away from the assembly, and when it is red, all three cubes are moved away from the last cube holding the camera. When signaled, each cube moves down the x-axis according to the dynamic equation $\frac{dx}{dt} = 2$, again numerically integrated using Euler's method and the same time step as before. The simulation is run for 2 h (equating to one full rotation of the rotating cube so that each control action is performed).

In this simulation, control actions are applied at the beginning of each sampling period based on a signal received from the image. Figure 6 demonstrates the control action applied to the first block. Specifically, at time t = 0.2 h, no control action has been applied as the black face still occupies the center pixel. Between t = 0.2 h and t = 0.3 h, the blue face crosses over the center pixel, however the control action is not applied until t = 0.3 h when the first block begins to break off from the assembly.

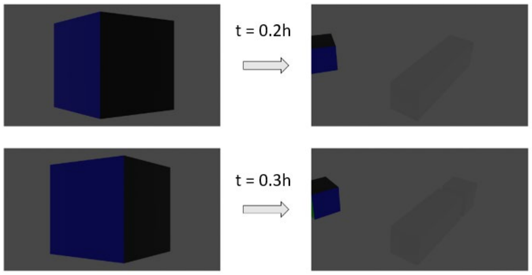

Figure 6. View the assembly and camera view of the first control action taken at t = 0.3 h (bottom left; the effect of the action at 0.3 h is shown at 0.4 h on the bottom right) compared to the system at t = 0.2 h (top left; the effect of the action at 0.2 h is shown at 0.3 h on the top right).

Remark 1

One important step in verifying the performance of the controller was determining how to use pixel data to set the behavior of the controller. In this simple case, this was "calibrated" by determining the RGB value returned by the loaded image for each color in the set of colors the controller is to see, where black corresponded to a value of (9,9,9), blue to (9,9,73), green to (9,73,9), and red to (73,9,9). When the image processing algorithm returned one of these values, a control action associated with the value is applied. This however is highly idealized; many aspects which require consideration in real processes could be analyzed using this testbed, including the effects of material properties, lighting properties, and sensor measurement noise. For example, one could imagine that instead of one discrete pixel value being used to represent a color, a range of similar values may be needed to account for variations caused by lighting, or perhaps similarly a number of pixels may need to be analyzed so that pixels affected by intense lighting variations such as glare do not negatively impact the controller.

Remark 2

Colors were set using filter intensities between 0 and 1, however .PNG files store the values between 0 and 255. It is noted that the value of the pixels read back may not correspond to what is expected analytically; for example, setting the color blue as (0,0,1,0), one may expect a read back of a blue pixel to be (0,0,255) (where the alpha filter is not considered), however, a value of (9,9,73) was found. This sheds light on how the complexities of using a simulated environment for setting colors as well as capturing and processing images need to be carefully considered in the design of a controller which utilizes image data.

Remark 3

The assumptions that the assembly is equipped with a controller and actuation is non-trivial. With regard to a controller, depending on the size of the assembly, it may be difficult to integrate the proper hardware with the assembly. Similar problems arise with actuation, however this is further complicated by considerations of the dynamics of the assembly which are desired under a stimulus. For example, the controlled material assembly in this simulation can be thought of to be progressively "breaking" as it is exposed to certain optical stimuli; depending on the design and material of the device, it may be difficult to not only actually provide actuation which breaks the device, but is also able to perform the action to receive a deterministic result.

Remark 4

The idea of progressively breaking the material assembly reflects the desire to make material changes in a reversible or continuous manner. The reason for this is that, especially when dealing with intention, uncertainty may arise where it may be desirable from a safety perspective to begin to take actions to disable the device pre-emptively before any harm can be done, but the function of the assembly may also be lost when actions are taken to disable the device in the case harm is present (i.e. the device breaks before harm can be done). This motivates the use of a simulation test bed to fully characterize the control behavior under a wide variety of possible conditions.

Remark 5

The choice of having the controller only move one block at some times and one or more at other times was arbitrary and made so that the blocks do not collide after "breaking" off of the assembly. Many different assembly and actuation models of varying complexity could have been considered here depending on the intended function of the material assembly. Instead, this simulation is intended to demonstrate the potential for Blender to be used as part of a testbed framework for developing optical stimuli responsive materials, including those equipped with intent recognition.

Material Assembly with Image Prediction-Based Control

Utilizing the same simulation, we now demonstrate the integration of image predictions in the control law. Specifically, at each sampling time, the controller receives an image of the current system (i.e. an image of the rotating cube from the camera attached to the material assembly). By integrating the dynamics of the rotating cube forward in time, predictions of future images captured by the assembly camera can be generated by Blender and used to preemptively signal control actions to be applied. In this simulation, the dynamics of the system are integrated forward in time to produce image predictions at 0.1, 0.2, and 0.3 h into the future at every sampling time. Using the same algorithm to determine control actions (i.e. analyzing the color of the center pixel of each image), each predicted image is processed. In the current algorithm, the control action signaled by the prediction from 0.3 h in the future is applied at the beginning of the sampling period (this is demonstrated in Figure 7 where the image prediction for t = 0.3 h signals the first block to begin to break off at the beginning of the first sampling period at t = 0 h, where the effect is shown at time t = 0.1 h in Figure 8).

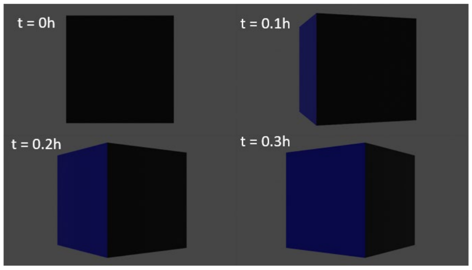

Figure 7. At the beginning of the first sampling period at t = 0 h, the controller receives the top left image. The controller integrates the dynamics of the rotating cube forward in time to produce predictions of the image it will see at t = 0.1 h, t = 0.2 h, and t = 0.3 h in the future.

The ability of the controller in this simulation to pre-emptively act based on predicted images demonstrates how the behavior of image responsive systems (in this case, an image responsive material assembly) can be compared with and without image predictions to design a desired response. Further testing may be conducted to tune the desired controller response; for example, consider that the response of the predictive controller in the example above is considered too aggressive in the sense that control actions are being applied based on predictions of images which are too far in the future (i.e. irreversible control actions are being applied based on predictions which we are less confident in). It may be desired to change how the control signals are used, for example using the prediction from 0.1 h in the future (instead of 0.3 h) to signal the controller, or changing how the controller responds to signals (such as breaking each cube off of the assembly at a slower rate) to achieve a desired response. This indicates that Blender may be used as a simulation testbed to design controlled material assemblies and tune aspects of their behavior, including control design and the integration of image predictions, as well as image processing algorithms. These simulations more broadly showcase the ability of Blender to be used to develop simulations which facilitate the testing of integrated image-based and image prediction-based control strategies and image processing algorithms.

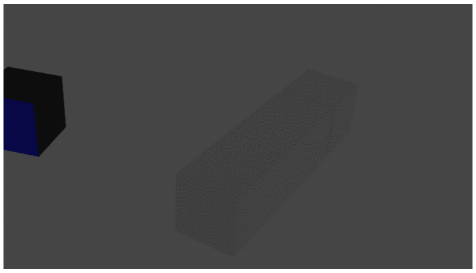

Figure 8. View of the assembly at t = 0.1 h after the predictive controller signaled a control action at t = 0 h to

break the first cube off the assembly.

Conclusions

This work provided a perspective on two areas in which process design (and its integration with control) could be impacted, and new avenues opened, by Industry 4.0 considerations related to control system cybersecurity and the use of image-based control and safety systems. We began with a discussion of two ideas of potential avenues for cybersecurity in process design, one which was inspired by the impacts of active attack detection mechanisms on process objectives (i.e., that designs be developed which can facilitate probing for attacks during operation but without impacting overall profits) and one which was inspired by the ability of power supply attacks to use physical measurements on a computing device to backtrack encryption information (i.e., that designs and instrumentation/information availability strategies be analyzed for whether they have any ability to leak information that could reduce security/privacy). We then discussed the potential utility of Blender for testing various considerations related to images in next-generation manufacturing systems design, including in the design of safety monitoring schemes, as well as for advanced assemblies (e.g., stimuli-responsive materials that should respond to certain image data).

ACKNOWLEDGEMENTS

Financial support from the National Science Foundation CBET-1839675, CNS-1932026, and CBET-2143469, Air Force Office of Scientific Research FA9550-19-1-0059, the National Aeronautics and Space Administration (NASA) under award number 90NSSC30M0124, Michigan Space Grant Consortium (MSGC) and Wayne State University is gratefully acknowledged. We would like to thank Nicholas Deeb for his work on investigating operating system fundamentals and communicating those principles to us.

REFERENCES

1. Parker S, Wu Z, and Christofides PD. Cybersecurity in process control, operations, and supply chain. *Comput. Chem. Eng.* 108169 (2023).
2. Narasimhan S, El-Farra NH, Ellis MJ. A control-switching approach for cyberattack detection in process systems with minimal false alarms. *AIChE J.* 68:e17875 (2022).
3. Durand H, Wegener M. Mitigating safety concerns and profit/production losses for chemical process control systems under cyberattacks via design/control methods. *Mathematics* 8:499 (2020).
4. Cormier A, Ng C. Integrating cybersecurity in hazard and risk analyses. *Journal of Loss Prevention in the Process Industries* 6: 104044 (2020).
5. Oyama H, Durand H. Integrated cyberattack detection and resilient control strategies using Lyapunov-based economic model predictive control. *AIChE J.* 66:e17084 (2020).
6. Oyama H, Messina D, Rangan KK, Leonard AF, Nieman K, Durand H, Tyrrell K, Hinzman K, Williamson M. Development of directed randomization for discussing a minimal security architecture. *Digital Chemical Engineering* 6:100065 (2023).
7. F. Farokhi, I. Shames, and N. Batterham, “Secure and private control using semi-homomorphic encryption,” Control Engineering Practice, vol. 67, pp. 13–20, Oct. 2017.
8. A. B. Alexandru, M. Morari, and G. J. Pappas, “Cloud-Based MPC with Encrypted Data,” in 2018 IEEE Conference on Decision and Control (CDC). Miami Beach, FL: IEEE, 2018, pp. 5014–5019
9. MIT OpenCourseWare. 16. Side-Channel Attacks. https://youtu.be/3v5Von-oNUg?si=b5XuqBQ8dzSUTAjn
10. Flynn C. Introduction to Side-Channel Power Analysis (SCA, DPA). https://youtu.be/OlX-p4AGhWs?si=yleaesMyXWP7j4Cb
11. Kocher, Paul, et al. "Introduction to differential power analysis." *Journal of Cryptographic Engineering* 1 (2011): 5-27.
12. Akkarakaran Francis Leonard, Gjonaj G, Rahman M, and Durand H. Virtual Test Beds for Image-Based Control Simulations Using Blender. *Processes* 12 (2024): 279.