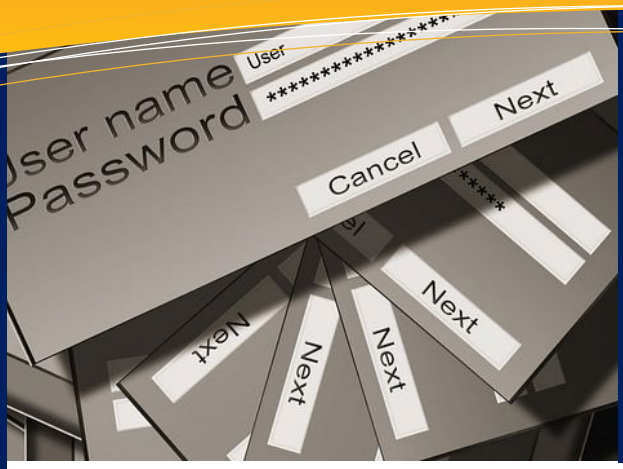
TAI ENGINEERS • MANAGERS • TECHNICAL SERVICES

QUARTERLY JOURNAL

OPERATIONAL TECHNOLOGY IMPLEMENTATION

ISSUE 02

December 2023



this issue

NIST Updated Password Guidelines P.1

Access Control Systems P.2

Badge Readers or Dongles for HMI P.3

The Evolution of AI P.4

Making a Strong Password

Maximum Length

New guidelines prioritize password length - above all. Longer passwords, including, passphrases, are considered crucial for increased security. Organizations should restrict the minimum length of passwords to 8 characters.

Prioritize Memorability

Using memorable words or passphrases can aid users in remembering a longer, more secure password. Password memorability is essential for security, as immemorable passwords are often recorded physically or digitally in unsecured locations.

Ignore Complexity

Rather than improving security, password complexity requirements have been shown to result in predictable, easily guessed passwords. They can also become an obstacle to making a long, memorable password.

NIST Updated Password Guidelines

Introduction to NIST's Evolving Password Guidelines

In the ever-evolving landscape of cybersecurity, NIST password guidelines have undergone a significant transformation in recent years. Historically, password policies emphasized complexity—requiring a mix of character types like uppercase letters, numbers, and symbols. However, the latest NIST guidelines break from this precedent. Instead, they prioritize the length of passwords, recognizing that longer passphrases offer better security without sacrificing user experience.

Understanding Human Behavior in Password Creation

The Predictability of User-Generated Passwords One of the primary drivers for this change lies in understanding human behavior. Users tend to respond predictably to complexity requirements, often resorting to easily guessable patterns when forced to create complex passwords. Research highlighted in the updated guidelines shows that users who might have chosen a simple password like "password" are likely to modify it to meet complexity rules (e.g., "Password1" or "Password1!"), doing little to improve security.

Implementing Blocklists to Enhance Security

The updated guidelines also recommend the use of blocklists to reduce password predictability. These blocklists should consist of commonly used passwords, dictionary words, and passwords from previous breaches. By comparing user-chosen passwords against these blocklists, services can mitigate the use of highly guessable passwords, enhancing overall security.

Prioritizing User Experience and Memorability

The Drawbacks of Highly Complex Passwords

Moreover, the emphasis on user experience and memorability is another significant aspect of the updated guidelines. Highly complex passwords, while theoretically secure, pose challenges for users in remembering them. This often leads to unsafe practices such as writing passwords down or storing them electronically in insecure ways. Therefore, the guidelines discourage overly complex passwords, recognizing that they might inadvertently compromise security.

Differentiating Password Requirements: Centrally Verified vs. Local Verification in Multi-Factor Authentication

The distinction between centrally verified passwords and those used for local verification in multi-factor authentication is another noteworthy addition. This differentiation acknowledges different threat models and adjusts password requirements, accordingly, offering a tailored approach to security based on the verification method.

Conclusion: A Shift Towards User-Friendly and Secure Password Policies

In conclusion, the evolution of NIST password guidelines signifies a departure from stringent complexity requirements toward a more nuanced, user-friendly, and security-aware approach. By prioritizing length, considering user behavior, implementing blocklists, and acknowledging diverse verification methods, these guidelines pave the way for stronger and more user-conscious password security in the digital age.

Access Control Systems: What OT Managers Really Need to Know

Enhancing Security with Badge Readers, Dongles, and Biometric Scanners.

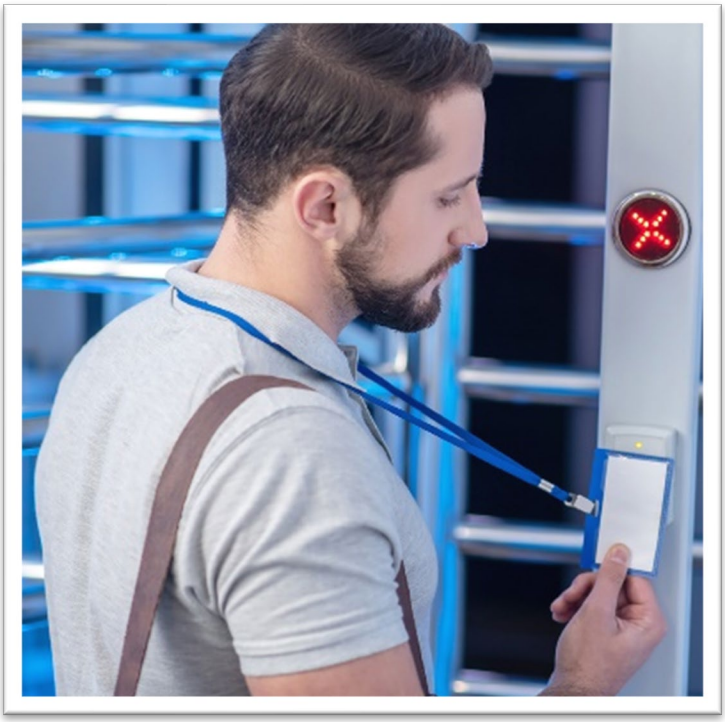
Access control systems are security mechanisms designed to regulate and manage entry to physical or digital spaces. These systems ensure that only authorized personnel or entities gain access to specific areas, resources, or information within an organization or facility. They encompass a range of technologies and protocols that authenticate, authorize, and monitor individuals' or devices' access rights based on predefined permissions or credentials.

The primary functions of access control systems include:

1. **Authentication:** Verifying the identity of individuals or entities seeking access. This can involve various methods such as passwords, biometric scans (fingerprint, iris, facial recognition), smart cards, or cryptographic keys.
2. **Authorization:** Granting or denying access based on validated credentials. This process determines what level of access an authenticated user or device is permitted, often defined by roles, permissions, or access rights associated with the user's profile.
3. **Accountability and Auditing:** Logging and recording access attempts, successful or failed, to create audit trails. These logs aid in monitoring activities, investigating security incidents, and ensuring compliance with regulations.

Safeguarding critical assets against unauthorized access is a top priority for any Operational Technology network. Access control systems stand as the vanguards, fortifying the security perimeter of industrial facilities, securing Human-Machine Interface (HMI) access, and ensuring operational continuity.

Within this realm, peripheral devices such as biometric scanners, dongles and badge readers emerge as integral components, offering robust layers of defense against potential threats.



As the linchpin of OT security, Access Control Systems are designed to regulate entry to physical or digital spaces within industrial environments. These systems authenticate and authorize individuals, granting them specific levels of access based on their credentials.

While dongles and badge readers represent common effective and low-cost solutions, biometric scanners can also be used to bolster OT security. These systems validate identity using unique biological traits like fingerprints, retina scans, or facial recognition. Biometrics offer heightened accuracy and mitigate risks associated with lost or stolen credentials.

Access control systems can be implemented in both physical and digital environments. In physical security, these systems regulate entry to buildings, rooms, or specific areas within a facility using mechanisms like badge readers, turnstiles, or barriers. In digital contexts, they manage access to networks, databases, software applications, or sensitive information through authentication protocols, firewalls, encryption, and other cybersecurity measures. Overall, access control systems are fundamental components of security strategies, safeguarding assets, data, and critical infrastructure by controlling and managing who can access what, when, and under what circumstances.

HMI Access Security: Dongles or Badge

Safeguarding HMIs stands as a critical imperative for OT security. When it comes to fortifying HMI access, two prominent solutions take center stage: dongles and badge readers. Each offers unique advantages and drawbacks, catering to specific security needs within industrial environments.

Dongles fortify digital defenses by serving as physical tokens, requiring their presence for access. This physical aspect fortifies security, reducing the risk of remote breaches or unauthorized access. They also allow authorized users to move between terminals while carrying their authentication key. This flexibility is advantageous in dynamic industrial settings. Furthermore, dongles often employ robust encryption and digital signatures, adding layers of protection to the authentication process, making them harder to duplicate or replicate.

However, the reliance on physical dongles can become a limitation, especially in scenarios where the dongle is misplaced, damaged, or stolen, as these situations can cause access disruptions. Additionally, procuring and maintaining dongles for all authorized users can incur additional costs and logistical challenges, especially in large-scale deployments.

On the other hand, badge readers enable fine-grained access control, restricting entry to specific areas and systems based on credentials encoded in badges or cards. This granularity enhances security within industrial facilities. Badge readers maintain comprehensive logs of entries and exits, facilitating audits, compliance checks, and aiding investigations in case of security incidents. Badge reader systems can also be scaled effectively to accommodate varying access requirements within an organization, offering flexibility as operations expand.

It is important to note that lost or stolen badges pose a significant risk as unauthorized individuals might gain access by using someone else's credentials, potentially compromising security. Implementing badge reader systems requires integration with existing infrastructure, potentially demanding significant effort, time, and resources.

The selection between dongles and badge readers hinges on the specific security needs, operational requirements, and risk tolerance within an industrial setting. For Enhanced Digital Security, dongles offer robust encryption and physical authentication, ideal for scenarios prioritizing digital defense against remote breaches. For Granular Physical Access Control, badge readers excel in regulating physical entry to restricted areas, facilitating detailed access logs and control over on-site movement. Ultimately, a comprehensive security strategy might incorporate elements from both solutions to create a resilient and multi-layered defense against evolving threats in industrial settings. Security can be even further enhanced for HMIs by including standard username and password login systems with dongles and/or badge readers.

Dongles

Dongles, small USB-based devices, are used to authenticate users before granting entry to HMIs, often utilizing encryption and unique digital signatures to verify authenticity. Dongles act as physical keys, enhancing security by requiring their presence for system access.

Dongles act as tangible barriers, ensuring that only authorized personnel with the physical dongle can access the HMI, reducing the risk of remote breaches.

They also offer a portable solution for HMI access, allowing authorized users to move between terminals without compromising security.

Badge Readers

A cornerstone of physical access control, badge readers authenticate individuals based on their credentials encoded in badges or cards. These readers grant or deny access to restricted areas within industrial facilities.

By restricting physical access to critical areas, badge readers create an additional layer of defense, complementing digital security measures.

TAI Engineering
600 Red Brook Blvd
Suite 300
Owings Mills, MD 21117
844-261-1080
ben.amoss@taiengineering.com

THE EVOLUTION OF AI IN ENGINEERING AND MANUFACTURING

Introduction

As leaders in the engineering and construction industry, TAI is always at the forefront of technological advancements. We are keenly monitoring the rapid development of Artificial Intelligence (AI) to determine how and when it can be utilized for the benefit of our clients. The integration of AI in engineering and manufacturing is evolving at a remarkable pace. These advancements are intriguing, yet the full potential of AI in these fields is still emerging, primarily behind the scenes. Notably, large companies seem to be developing AI systems in-house, indicating a lack of widespread commercial solutions applicable across various industries.

Key Areas of AI Application in Manufacturing

1. Digital Twins

AI is revolutionizing manufacturing with the creation of digital twins. These virtual models of physical systems enable real-time monitoring and predictive maintenance. A prime example is Siemens, which utilizes digital twins in its manufacturing processes for operational optimization and maintenance forecasting.[1]

2. Predictive Maintenance

Major corporations like Pepsi and Colgate are leveraging AI technology from startups such as Augury. This technology is crucial in predicting and preventing equipment failures, thus reducing downtime and maintenance costs.[2]

3. Lights-Out Factories

The concept of lights-out factories is becoming a reality, as seen with the FANUC factory in Japan. This factory operates autonomously, without human intervention, for extended periods. Similarly, Philips runs a near-autonomous factory in the Netherlands for electric razor production.[3]

4. Enhanced Inventory Management

AI systems are increasingly used for efficient inventory management. These systems are adept at predicting supply needs and identifying potential supply chain bottlenecks.

5. Automated Visual Inspection

In the automotive industry, companies like BMW and Ford are employing cobots equipped with computer vision. These robots are integral in performing tasks such as quality control inspections.[4]

6. Analyzing Large Datasets

AI plays a critical role in analyzing extensive datasets to discern trends and predict manufacturing outcomes. This capability is essential for strategic decision-making and planning.

The Future of AI in Manufacturing

Despite these promising applications, AI in manufacturing is still in a developmental phase. Its current usage is somewhat limited and not robust enough for broad application across different industries, especially for companies not as large as BMW or Siemens. However, the future of AI in engineering and manufacturing holds immense promise. Staying at the forefront of this evolution is vital for maintaining a competitive edge and fostering innovation.

References

[1]Siemens. "Digital Twins in Manufacturing." Siemens Digital Industries Software.

[2]Augury. "Predictive Maintenance Solutions." Augury Systems.

[3]FANUC. "The Lights-Out Factory." FANUC Robotics.

[4]BMW Group. "BMW Group Uses AI for Quality Control." BMW Group Press.