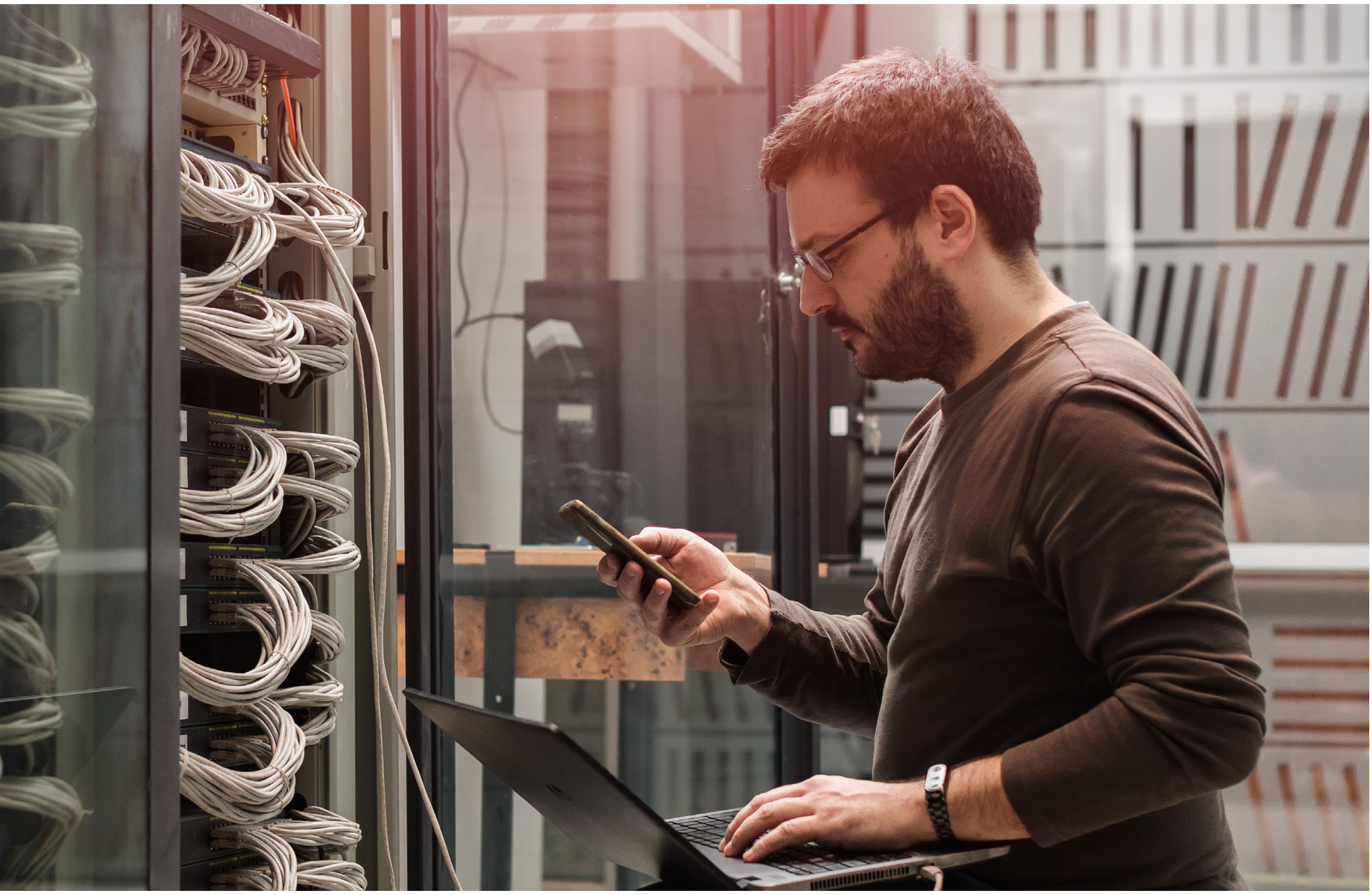
DEFENSE IN DEPTH

# ABB Process Automation's Layered Cyber Security Strategy



Today’s threat landscapes are ever evolving and becoming more and more impactful, making it increasingly difficult to determine the right approach to remain proactive. There is a wide array of standards, local regulations, new technologies and a constant flow of conflicting recommendations from various organizations and government bodies that can be overwhelming and confusing.

**Luckily, some of the most effective strategies are not new, but tried and true foundations that can be universally applied. One such strategy is the Defense in Depth strategy.**

# Table of contents

# Defense in Depth

What is a Defense in Depth strategy and how do we run a Defense in Depth program? The Computer Security Resource Center (CSRC) suggests the following definition for Defense in Depth[1]:

**"The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another."**

Simply put, no single cyber security control can completely protect your systems. Instead, we must apply layers of individual cyber security controls that complement each other and fill the gaps.

From a simple control such as a Group Policy Object to a comprehensive Business Continuity Plan, a successful Defense in Depth program should be modelled to overlap to protect or mitigate the most common and likely attack vectors.

Our overall strategy is to reduce the amount of risk, a function of likelihood and consequence, down to an acceptable level. Using a Defense in Depth approach can help achieve this goal. The National Institute of Technology (NIST)[2] recommends using a defense in depth program from the very start to design security and privacy architectures and the International Society of Automation (ISA)[3] refers to defense in depth as a superior approach to achieving security objectives.

A common way we like to conceptualize Defense in Depth is by comparing it to Swiss cheese. If we compare a single piece of cheese to a single security control, we find that although there is a lot of coverage, there are also a lot of holes. Add a second piece of cheese and we can cover up some of the holes, but some may continue to overlap. As we continue to add more and more layers of cheese, we slowly cover up more and more of the holes, although we may never cover them up completely, we should be able to get a significant amount of coverage after just a few layers.

ABB Process Automation has adopted a Defense in Depth strategy both internally to become a secure and reliable supplier to our customers, as well as externally in our cyber security services portfolio to enhance our customers cyber security programs.

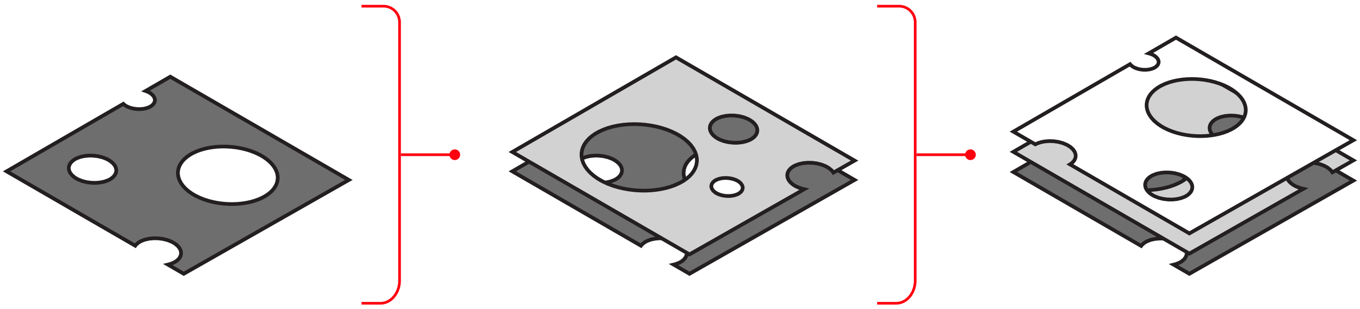


**Figure 1**: Defense in Depth visualized as stacking slices of Swiss cheese to close gaps.

# Surface Area of Vulnerability

When beginning the discussion about Defense in Depth, we often bring up the phrase, Surface Area of Vulnerability. Reducing the Surface area of Vulnerability is our primary aspiration when implementing a Defense in Depth program. The phrase is essentially a way of mentally visualizing how we are reducing our risk.

Let's visualize, we have a dartboard which represents all the openings an attacker can use to access a machine or system. Each dart we throw and land on the dartboard is a successful attack. The larger the dartboard, or the more surface area it has, the higher the frequency that a thrown dart will stick to the board. However, what if we can shrink the dartboard smaller and smaller or reduce the Surface Area. This will make it much more difficult to land a dart on the board successfully.

We hope to achieve this with our Defense in Depth program. We want to keep that dartboard as small as we can, so it is very difficult for a bad actor to successfully land an attack, thus effectively reducing the Surface Area of Vulnerability. Often, we think of surface area of vulnerability through a small window, individual vulnerabilities in a single machine, such as a missing patch, an open firewall port or an unsecure application. However, we must also consider it on a larger scale as well, with each machine, device, network, etc. bringing its own set of attack vectors that must be considered and hardened against.

In a practical sense, every policy or firewall restriction or new security control can help to reduce this surface area of vulnerability. On the other hand, each new piece of software, communication port, service, new server, a new piece of equipment, or network segment will add additional attack vectors thus increasing the surface area of vulnerability.

Successfully implementing a defense in depth program will result in balancing these opposing pressures to keep the surface area of vulnerability as small as possible throughout the life of the industrial control system.

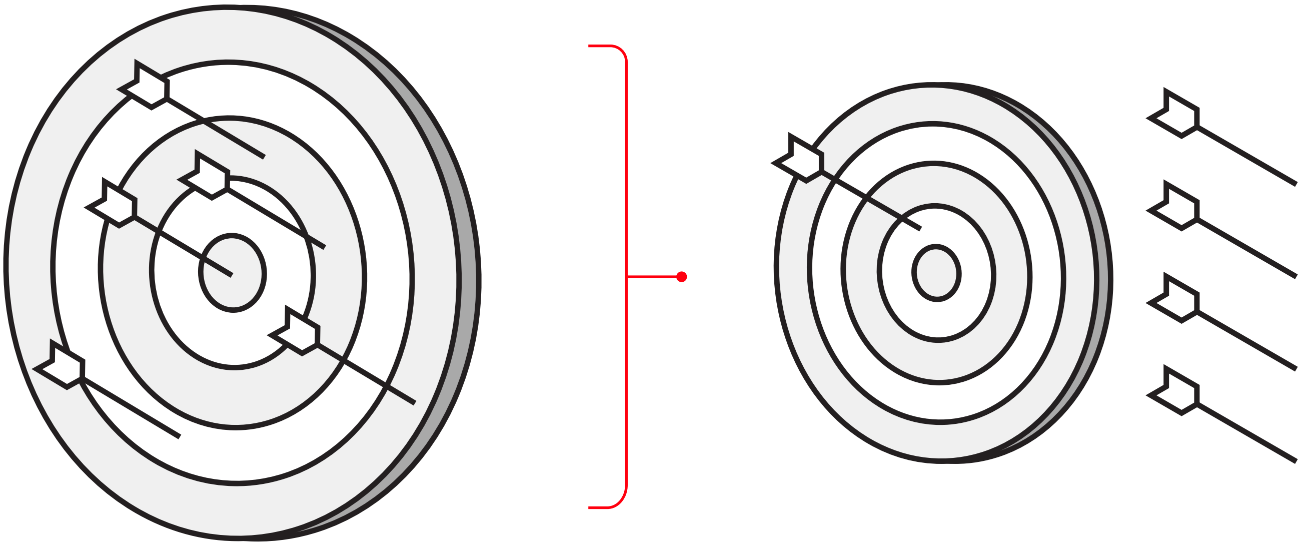


**Figure 2**: Surface Area of Vulnerability visualized as a shrinking dart board. The smaller the target the harder it is to hit.

# Candy Shell Security

Another idea we must consider in our defense in depth program is what we like to call candy shell security. Candy shell security is the concept of creating a hard outer shell to protect a fragile and soft center much like a piece of hard candy with a caramel center. From a cyber security perspective, this means we've created a thoroughly secure outer perimeter and if an attacker breaks through or circumvents this outer layer there are no further protections and the attacker would have full command and control over the entire inner system. For example, you can have the most sophisticated corporate barrier, but if a persistent attacker finds a way to bypass and get into the OT system, where administrative credentials are cached or stored in plain text, the attacker now has full command and control in the OT environment, as opposed to being frustrated with yet another layer of defense.

While we want to avoid this approach as much as possible, this is an example of where IT and OT systems significantly diverge. Due to the extended life cycle of OT environments, we will often face very old technology with little to no embedded security features which could cause significant deviations from corporate IT security standards or policy.

Sometimes we may find it easier to not adjust the corporate security standards and policies to the OT systems but to simply build protections around the system. Thus, we fall into the Candy Shell Security trap.

In this case, we reinforce the importance of successfully layering security controls in our Defense in Depth program.

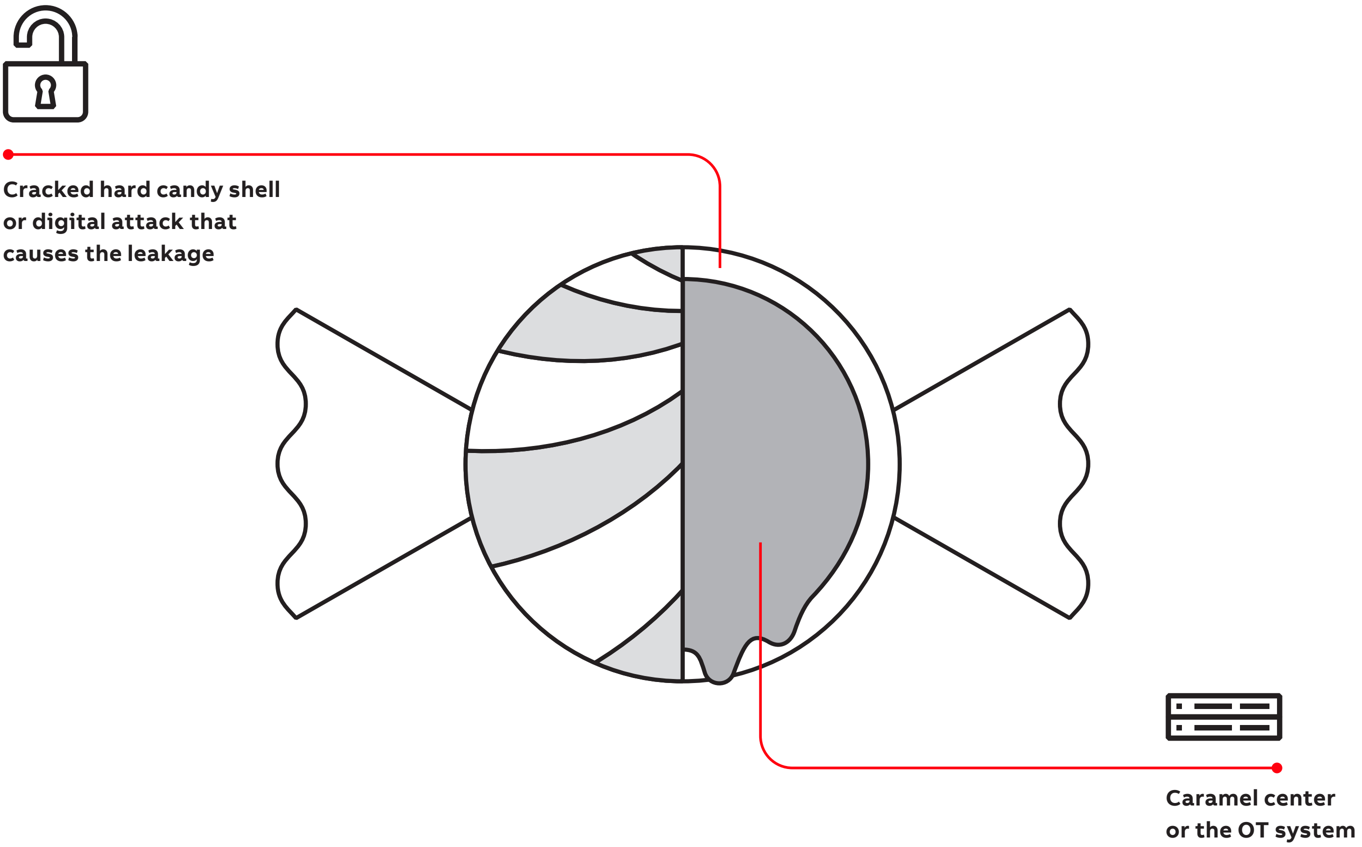

Cracked hard candy shell or digital attack that causes the leakage
Caramel center or the OT system

**Figure 3**: Candy Shell Security, a hardened exterior with a soft interior.

# Risk Reduction Roadmap

A Defense in Depth strategy covers a broad spectrum of vulnerabilities including personnel, procedures, system configurations, and physical security. the ABB Process Automation's Defense in Depth strategy is applicable to the areas of the delivery of a distributed control system. The items outside the prerogative of the ABB Process Automation's control as a supplier include items such as personnel, training, procedures, and physical security.

One of the ways in which the ABB Process Automation describes its defense in depth approach is through our Risk Reduction Roadmap. This roadmap shows the various major controls in the ABB Process Automation cyber security portfolio to provide our customers with a recommended approach to implementing security controls.

At the beginning of the journey, we start to assess what we have and plan our implementation strategy. While there is no reduction in overall risk, these are important milestones in the Risk Reduction journey including customizing the most appropriate implementation order and priorities that fit our customers' needs.

As we begin to layer the security controls on top of each other in the implementation phase, we can see the risk begin to decline. The Center for Internet Security states that implementation of basic cyber security controls could reduce your risk by up to 85%[4].

As we get more towards the Maintain and Detect phases, the Risk Reduction begins to level off, as now we are trying to protect against more sophisticated and targeted attacks such as organized crime and advanced persistent threats. As mentioned earlier, you can never fully remove all your risk in your systems, and as we get later into the roadmap, we require considerably more investment to reduce the risk.

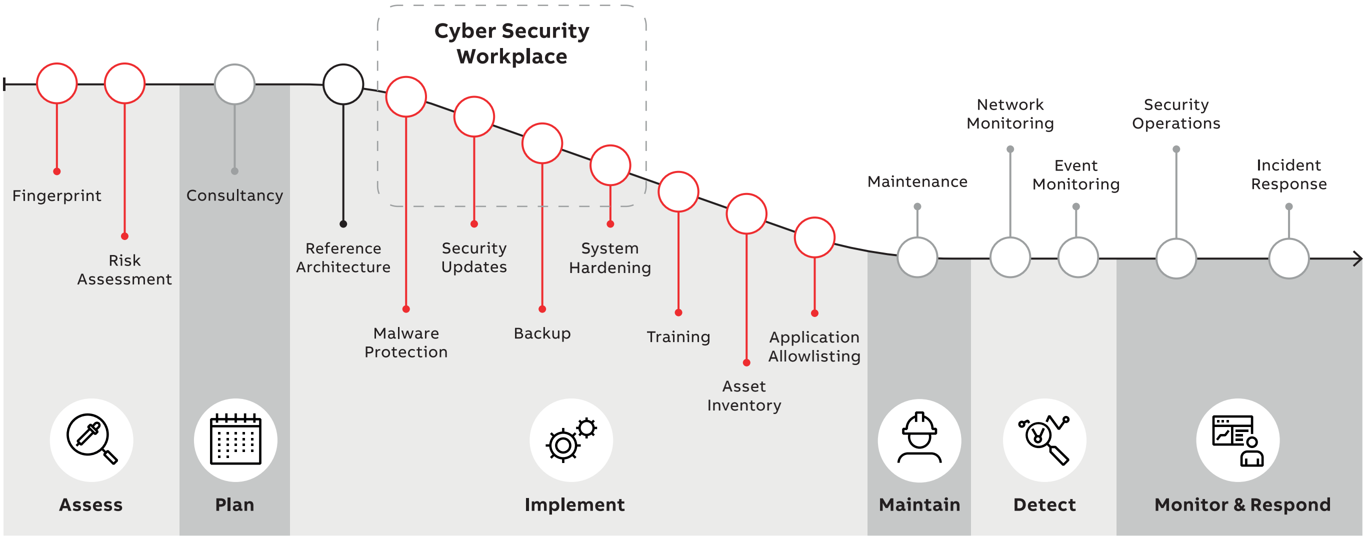


**Figure 4**: ABB Process Automation's Risk Reduction Roadmap, a series of controls applied to reduces overall risk.

# ABB Process Automation's Internal Defense in Depth program

As a supplier, how does ABB Process Automation go about Defense in Depth in the internal processes? In addition to running our own internal Defense in Depth program on our information systems, ABB Process Automation has additional layers of processes and policies to ensure that we are a secure and trustworthy supplier to our customers. A few highlights include Minimum Cyber Security Requirements, Security Development Life Cycle, Vulnerability Handling and Supply Chain Security.

**Minimum Cyber Security Requirements (MCSR).**
ABB has what is known as Minimum Cyber Security Requirements (MCSR)[5]. This is the starting baseline of requirements ABB imposes upon its organization to not only protect our organization and brand but our customers. There are five categories of MCRSs:

1 **Products:** The requirements for developing, testing, and managing product life cycles. This includes topics such as establishing a Device Security Assurance Center for testing, ensuring requirements for acceptable cryptography, supporting vulnerability handling processes, security assessment procedures, and building a security development life cycle.

2 **Project Deployment:** The requirements that must be fulfilled by all ABB Process Automation deployment projects. This includes such topics as training requirements, malware prevention, security patch management, and secure system handover.

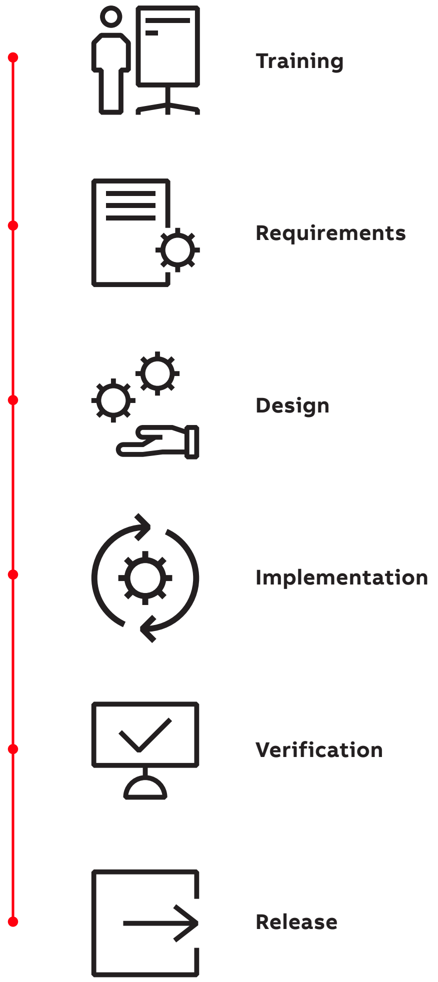
3 **Service:** The requirements for that must be fulfilled by all ABB service offerings and service work. This encompasses training requirements, handling customer user accounts, malware prevention, changing customer systems and data protection.

4 **Internet-facing Solutions:** Additional requirements on top of Products and Services that address additional concerns for cloud-connected solutions. This includes such topics as secure communication, access controls and authorization, logging and monitoring, data protection, and vulnerability monitoring.

5 **Product Procurement:** The requirements for procuring third-party software, hardware and services. ABB is only as strong as its weakest link, therefore we have specific requirements that must flow down to any supplier to ABB to ensure we protect our customer’s entire supply chain.

**Security Development Life Cycle (SDLC)**
As defined in the Minimum Cyber Security Requirements for Products, ABB Process Automation has established a rigorous Security Development Life Cycle with the intent to introduce cyber security in all phases of the product and solution development life cycle[6]. ABB Process Automation's SDLC was originally modelled after the Microsoft Security Development Life Cycle and continues to evolve to better fit ABB Process Automation's products and processes[7].

Today the model consists of seven phases: Training, Requirements, Design, Implementation, Verification, and Release.



Training Phase: ABB aims to provide comprehensive training requirements and courses available to all developers such as writing secure code, threat modelling and OWASP Top 10.

Requirements Phase: Details exactly security requirements must be addressed, such as services that must pass inspection, architectural requirements like robustness and minimum performance and scalability, and activities to assure outcome is not subject to vulnerabilities like data classification, coding guidelines, and test methodologies.

Design Phase: Designing the product's security architecture while considering compliance standards, industry best practices, market and customer needs, and security upgrade and patching processes.

Implementation Phase: Executing with secure development, implementation, and coding practices by recommendations found in OWASP, CWE/SANS Top 25, CERT Coding, DISA standards and reviewing with static code analysis.

Verification Phase: Another specific requirement in the Minimum Cyber Security Requirements for Product, ABB's Device Security Assurance Center (DSAC)[8] shall conduct comprehensive verification of the products including robustness testing, vulnerability assessments, device profiling, denial of service testing, protocol fuzz tests, and any applicable government or industrial regulatory testing.

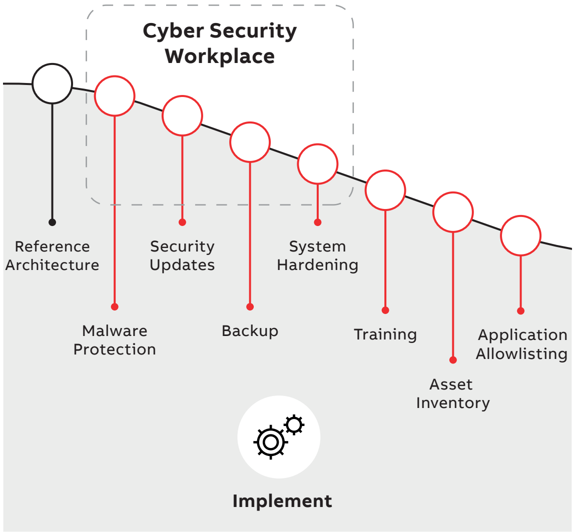
Release Phase: Managing the release and post-release life cycle including code-signing, end-user documentation, deployment guidelines, patch management, vulnerability handling and continuous improvement development.

**Vulnerability Handling**
Finally, ABB has a comprehensive Vulnerability Handling process for our customers to securely report, identify, report, and fix security vulnerabilities found in our products[9]. ABB has a public Alerts and Notifications portal through which customers subscribe directly and report vulnerabilities. ABB also participates with the major industrial notification bodies to ensure reported vulnerabilities are widely published, such as ICS-CERT, CISA Top-Level Root CVE Numbering Authorities (CNA), and NIST National Vulnerability Database (NVD).

ABB's Vulnerability Handling process consists of five phases: First Response, Initial Triage, Investigation, Remediation and Notification. In the First Response phase, ABB formally acknowledges the issue, usually within two business days, with written notification to the reporter and assignment of an ABB lead investigator. The next stage, Initial Triage, verifies the vulnerability, severity and impact according to Common Vulnerability Scoring System (CVSS) and involved any government organizations or other third parties as necessary. During Investigation, ABB documents the vulnerability and identifies all affected products in collaboration with reporting entities. In the Remediation phase, ABB develops and validates software remediations and/or mitigation procedures to reduce the risk or impact of the vulnerability. Finally, in the Notification phase, ABB publicly discloses the vulnerability through a security advisory through all official channels.

# ABB Process Automation's External Defense in Depth program

ABB Process Automation's Risk Reduction Roadmap describes the comprehensive Defense in Depth steps that are recommended to ABB Process Automation's customers. Let’s explore our most popular segment of the roadmap which we refer to as the foundational security controls and how we approach them in the ABB Process Automation Defense in Depth program.



**Implementation Phase**
Once you have completed your Assessment and Planning phases in your Risk Reduction Roadmap, the implementation of the defense in depth program begins. Below we have outlined the typical approach to layering our foundational security controls in our defense in depth program assuming they have not been modified by the results of the assessment and planning phases.

**Reference Architecture**
ABB Process Automation first approaches the system through its architecture. We have built a comprehensive Industrial Control System Cyber Security Reference Architecture which provides specific and detailed recommendations for planning and architecting the system with high-security practices in mind according to IEC 62443-3-3.

By implementing a secure architecture with proper separation of functions, zoning, and electronic security perimeters you can reduce the overall system’s surface area of vulnerability by limited unnecessary exposure and access.

**Foundational Controls**
Next, ABB Process Automation approaches what we call the Foundational Controls, or the basic security controls that maintain the security level and reliability of the system. These include Malware Protection, Security Patch Management, and Backup and Recovery.

**Malware Protection**
First, we approach Malware Protection. Often taken for granted, basic malware protection can provide some of the most comprehensive protection available. AV-Test is now reporting over 450,000 new malicious programs every day. While it is not often an Industrial Controls System[10] is exposed or targeted by the vast majority of these, there is comparably little investment required to deploy comprehensive malware protection with daily signature updates across the system to ensure that it is not compromised by known malicious software.

**Security Patch Management**
Second, we address Security Patch Management. There is an average of at least three new Microsoft security vulnerabilities found each day[11]. Security patches could potentially be the most important and most feared cyber security control. Unfortunately, we live in the age of Ransomware.

Ransomware continues to be the most common attack type year over year totaling nearly 25% of all reported attacks over the past two years[12] and costing an average of $4.62M USD[13].

Many of the most prominent Ransomware attacks relied on vulnerabilities which were already closed by Microsoft Security Updates months or even years earlier.

Why do we not patch? It is simple, we worry about a machine going down and not coming back up and it seems everyone has a story about a patch that broke their entire system. At ABB Process Automation, we promote that monthly patching can increase your reliability, specifically rebooting machines in the system to exercise your reliability in a controlled and expected activity. Looking at it from a risk perspective, if shutting down a machine in a controlled, scheduled manner, with maintenance personnel actively overseeing the tasks, results in a minor interruption, think of the much larger impact it could have if the machine went offline on its own due to failure, malware, or accident.

**Backup and Recovery**
Next, we insist on Backup and Recovery as the next layer in the program. While our previous controls focused on reducing risk by lowering likelihood, we now look to alleviating the consequences by implementing controls to reduce your recovery time objective (RTO). As a data point, in 2021 the average recovery outage due to restoring from a cyber incident was approximately 22 days. ABB Process Automation's DCS lines includ embedded backup and recovery capabilities, but by adding a comprehensive image recovery solution you can significantly reduce the impact of a cyber security outage, as well as retain images for forensic uses.

**System Hardening**
Next, we look to System Hardening, which not only includes individual firewall, service, and application hardening on each machine, but also system-wide security policies, event and log auditing, and role-based access controls. About our defense in depth program, we refer to monitoring the System Hardening to ensure policies remain unchanged as System Hardening is an embedded security feature of ABB Process Automation's Control System lines. This further ensures that we do not fall into the Candy Shell Security trap. Nevertheless, monitoring is extremely important as over the life cycle of a control system's life, changes are inevitable. Sometime during the implementation of these changes, individuals will intentionally or unintentionally disable security policies, install new software or open firewall rules, thus increasing the surface area of vulnerability. By monitoring the baseline and capturing the hardening posture we can ensure the mitigation or restriction of a growing surface area of vulnerability.

**Cyber Security Workplace**
Lastly, for our example, ABB Process Automation would recommend its Cyber Security Workplace package. One of the pitfalls of a defense in depth program is that in layering many security controls, they often come with their software package, procedures, reporting mechanisms and performance indicators. This means that you must have a resource or resources who are experts in each of the controls to view and understand the siloed data and verify that each security control is functioning as intended.

Currently, there is a growing workforce shortage in the field of cyber security with 3.5 million unfilled cyber security jobs globally[14].

Deploying resources familiar with routine checks across disparate security controls means an excess of man-hours required from a scarce resource.

ABB Process Automation's solution to this is Cyber Security Workplace. By pulling the key performance data from each of the various cyber security controls and harmonizing them into an easy-to-read dashboard, with detailed supporting information on each KPI in the event of a warning or error, any user now can monitor the security state of the industrial control systems. This reduces the total amount of man-hours required for routine maintenance and checks and frees your cyber security experts to focus their limited time on more important tasks.

# Summary

In summary, ABB Process Automation has found success in both leveraging Defense in Depth internally and providing a roadmap to our customers to reduce their cyber security risk. By mapping a clear Defense in Depth strategy and avoiding some of the pitfalls, such as Candy Shell security, you can successfully reduce your surface area of vulnerability.

# Reference

1. **“The Computer Security Resource Center (CSRC) suggests the following definition for Defense in Depth”** https://csrc.nist.gov/glossary/term/defense_in_depth

2. **“The National Institute of Technology (NIST) recommends using a defense in depth program from the very start to design security and privacy architectures”** NIST Special Publication 800-53 Revision 5, PL-8 Security and Privacy Architectures, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

3. **“and the International Society of Automation (ISA) refers to defense in depth as a superior approach to achieving security objectives.”** ISA/IEC 62443-1-1 Section 5.4, https://www.isa.org/products/isa-62443-1-1-2007-security-for-industrial-automat

4. **“The Center for Internet Security states thatimplementation of basic cyber security controls could reduce your risk by up to 85%.”** https://www.cisecurity.org/about-us/media/media-mention/implementing-the-cis-20-critical-security-controls-slash-risk-of-cyber-attacks-by-85

5. **“ABB Process Automation has what is known as Minimum Cyber Security Requirements (MCSR).”** As defined in ABB Process Automation's internal minimum cyber security requirements reference guide

6. **“As defined in the Minimum Cyber Security Requirements for Products, ABB Process Automation has established a rigorous Security Development Life Cycle with the intent to introduce cyber security in all phases of the product and solution development life cycle.”** As outlined in ABB Process Automation's internal Security Development Life Cycle Guide

7. **“ABB Process Automation's SDLC was originally modelled after the Microsoft Security Development Life Cycle and continues to evolve to better fit ABB Process Automation's products and processes.”** As defined in ABB Process Automation's internal Security Development Life Cycle Guide

8. **"Verification Phase: Another specific requirement in the Minimum Cyber Security Requirements for Product, ABB Device Security Assurance Center (DSAC)"** For more information on DSAC: https://library.e.abb.com/public/03f77d8934134c72865f88cc61b59798/ABB_Device_Security_Assurance_Center(DSAC)_9AKK107680A9866.pdf

9. **“Finally, ABB Process Automation has a comprehensive Vulnerability Handling process for our customers to securely report, identify, report, and fix security vulnerabilities found in our products.”** https://search.abb.com/library/Download.aspx?DocumentID =9ADB 005059&LanguageCode=en&DocumentPartId=& Action=Launch

10. **“AV-Test is now reporting over 450,000 new malicious programs every day.”** https://www.av-test.org/en/statistics/malware/

11. **“There is an average of at least three new Microsoft security vulnerabilities found each day.”** https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

12. **“Ransomware continues to be the most common attack type year over year totaling nearly 25% of all reported attacks”** IBM Security X-Force Threat Intelligence Index 2022, https://www.ibm.com/security/threat-intelligence

13. **“Ransomware continues to be the most common attack type year over year totaling nearly 25% of all reported attacks over the past two years and costing an average of $4.62M USD.”** IBM Security Cost of Data Breach Report 2021, https://www.ibm.com/security/data-breach

14. **“Currently, there is a growing workforce shortage in the field of cyber security with 3.5million unfilled cyber security jobs globally.”** https://cybersecurityventures.com/jobs/#:~:text=%E2%80% 9CThere%20are%203.5%20million%20unfilled, world%20that%20we%20live%20in.%E2%80%9D

—

**ABB**
Operating in more than 100 countries

**Joseph Catanese**
Cyber Security Practice Lead Americas
ABB Energy Industries

**abb.com/cybersecurity/service**