White Paper

Agilent
Trusted Answers

Agilent InfinityLab Assist Hub: Representing Advancements in Cybersecurity

Abstract

Ensuring the security of connected infrastructure and devices in an ever-evolving threat landscape has become increasingly challenging. As stated in the European Commission's proposal for the second version of the directive on the security of network and information systems (NIS2):

"The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges... any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market."

Various countries and organizations have provided conflicting recommendations, making it difficult for users to implement a coherent law-abiding approach. Efforts that are successful in the long term must consider possible threats, applicable laws and standards, the manufacturer's approach to information security, and device behavior regarding cybersecurity. These efforts must also be accounted for when implementing one's own information security approach. The Agilent InfinityLab Assist Hub has been developed to directly target cybersecurity improvements in the laboratory environment.

The laboratory as an operational technology (OT) environment: bridging the gap between OT and IT

Compared to connected industrial production environments, the connected laboratory environment closely aligns with an operational technology (OT) environment. OT is defined as "the practice of using hardware and software to control industrial equipment, and it primarily interacts with the physical world" (RedHAT, 2024).

In the classical Purdue reference model, established in the early 1990s to protect identities, information, and assets, the OT environment is clearly separated and secured from the information technology (IT)/enterprise environment.

The model only allows direct communication between adjacent levels.

OT environments (lab environments) are necessary due to the long life cycles of the systems typically exposed to cybersecurity threats, with the mitigations listed in Table 1.

Addressing cybersecurity challenges in OT environments requires customized security strategies that incorporate both traditional IT security principles and specific measures for the physical operations they control.

Unlike some IT system components and devices where complete infrastructure replacement is common, lab devices are typically replaced gradually over years, sometimes even over decades.

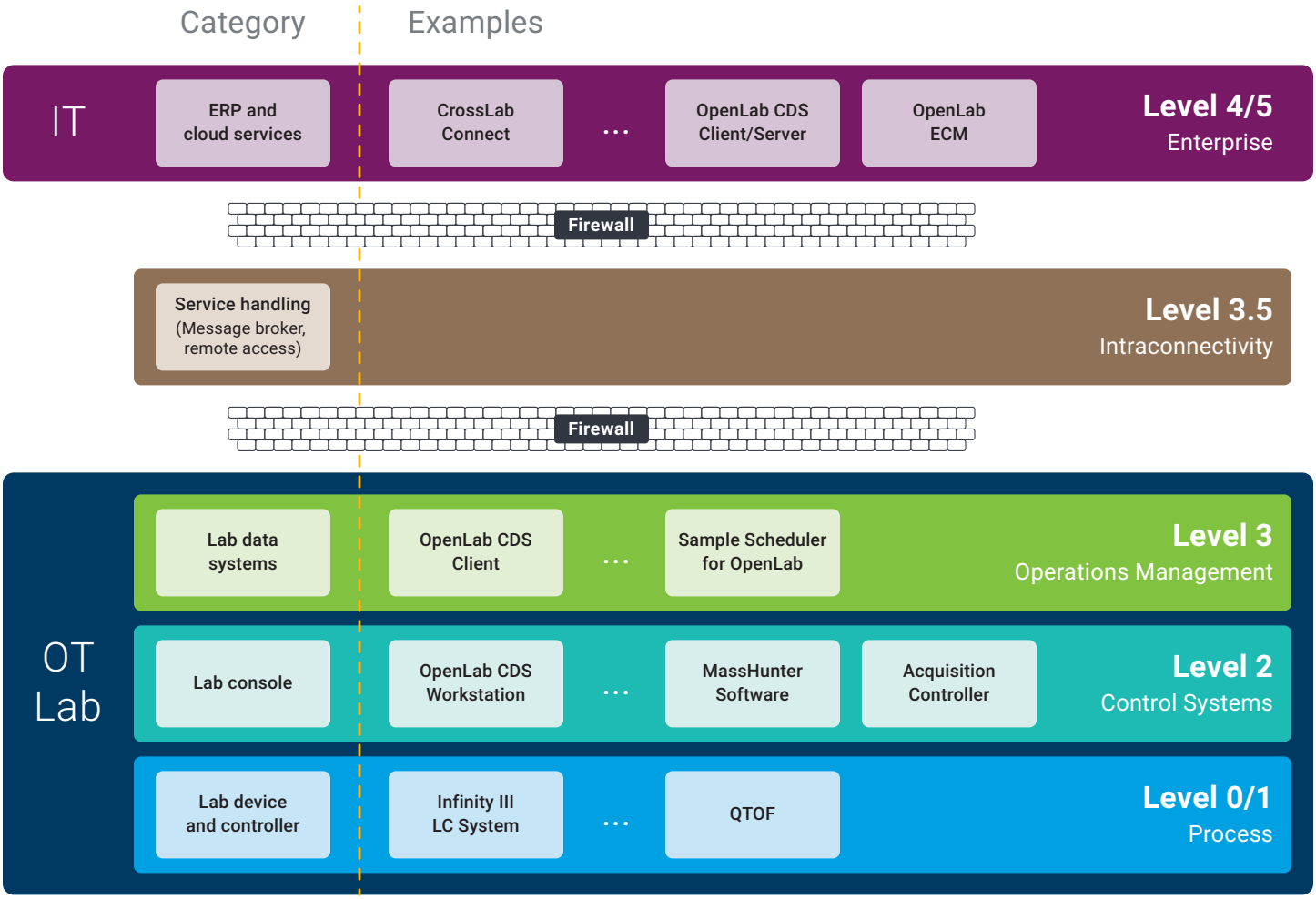

Figure 1. Classical Purdue reference model mapped to a laboratory focus (Microsoft, 2024).

Table 1. Cybersecurity threats in OT environments.

Cybersecurity Issue	Risk	Consequences	Mitigation
Legacy Systems with Weak Security	Outdated systems with vulnerabilities	Unauthorized access, data theft, system manipulation	Incremental modernization, patch management, compensating controls
Lack of Segmentation Between IT and OT Networks	Interconnected IT and OT networks	Compromise of critical infrastructure, process disruption	Network segmentation, firewalls, VLANs, secure gateways
Inadequate Patch Management	Difficulty in patching due to uptime requirements	Exploitation of unpatched vulnerabilities	Robust patch management, planned downtime, virtual patching
Lack of Security Monitoring	Absence of real-time security tools	Undetected breaches, malware, operational disruptions	OT-specific Intrusion Detection System (IDS), Security Information and Event Management (SIEM) tools, continuous monitoring
Weak Authentication and Access Controls	Weak or default credentials, lack of Role-Based Access Control (RBAC)	Unauthorized access, system tampering, process changes	Strong RBAC, multifactor authentication (MFA), password policies
Insider Threats	Employees or contractors misusing access	Data theft, sabotage, safety risks	Strict access controls, user monitoring, background checks
Remote Access Vulnerabilities	Poorly secured remote access	Unauthorized control or data exposure	VPNs, MFA, encrypted remote communication
Insecure Communication Protocols	Use of legacy protocols with noencryption	Eavesdropping, tampering, man-in-the-middle attacks	Use encrypted protocols, secure communication, protocol monitoring
Ransomware and Malware	Ransomware or malware targeting OT systems	Downtime, production loss, compromised safety	Regular backups, network segmentation, antivirus solutions
Third-Party and Supply Chain Risks	Vendors and third-party systems introducing vulnerabilities	Indirect compromise, backdoors, insecure software	Vendor risk assessments, secure vendor management, regular audits
Physical Security Weaknesses	Physical access to OT systems	Sabotage, disruptions, unauthorized data collection	Surveillance, locked cabinets, physical access controls
Denial of Service (DoS) Attacks	DoS or DDoS attacks overwhelming OT systems	Downtime, failure of safety-critical systems, production delays	Traffic filtering, redundancy, network segmentation
Insecure Configuration of Devices	Poor configuration of OT devices (e.g., PLCs, sensors)	Unauthorized access, faulty operations, loss of control	Security hardening, regular configuration reviews

The clear separation between OT and IT is becoming increasingly blurred due to new connectivity requirements, cloud functionality, and Industrial Internet of Things integration. This process, known as IT/OT convergence, is essential for achieving the next level of automation, such as Industry 4.0/5.0 or its counterparts, such as Pharma 4.0.

The effectiveness of any new development will be evaluated based on how well it addresses cybersecurity within a converging IT/OT environment.

Industry 4.0	Also known as the fourth industrial revolution, refers to the integration of digital, physical, and biological systems to create smart factories and advanced manufacturing processes. This era is characterized by the use of technologies such as the Internet of Things, artificial intelligence, machine learning, and cloud computing to enhance productivity, flexibility, and efficiency in production. Industry 4.0 aims to revolutionize how companies manufacture, improve, and distribute their products by enabling real-time decision making and automation (IBM).
Pharma 4.0	Refers to the application of Industry 4.0 principles and technologies to the pharmaceutical industry. It aims to enhance drug development and manufacturing by integrating advanced technologies. This approach streamlines processes, reduces errors, lowers costs, and accelerates the development of therapies. Pharma 4.0 also focuses on improving product quality, patient safety, operational efficiency, and regulatory compliance (ISPE, 2017).

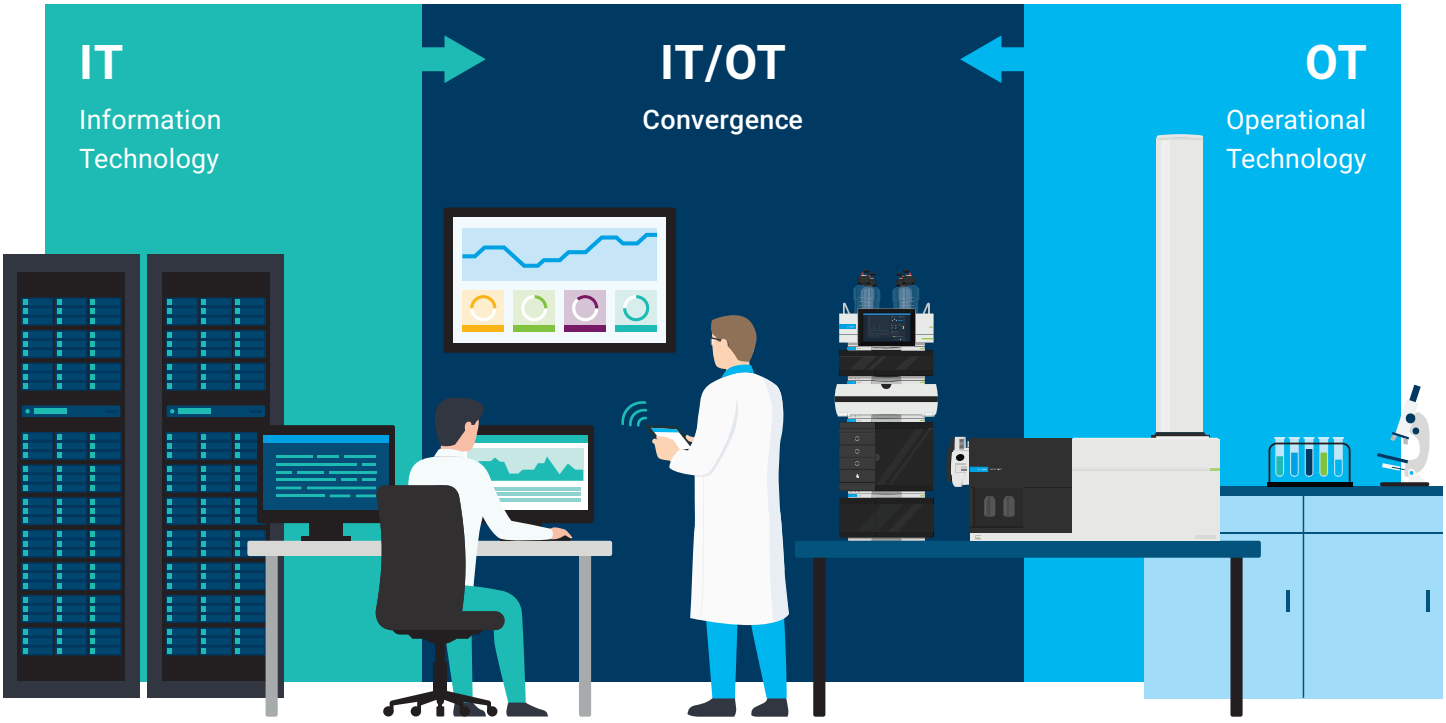

Figure 2. IT/OT convergence (Claroty, 2024).

Standards and organizations

The diverse standards and organizations can be exemplified by the approaches taken in the U.S., Europe, and China. This summary aims to showcase the complexity of regulatory environments, and is not comprehensive. For specific situations, consulting with dedicated field experts is crucial.

United States

In the U.S., cybersecurity standards are primarily guided by government agencies and industry organizations, often focusing on risk management, data protection, and critical infrastructure.

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** Developed by NIST, the voluntary CSF is widely used in the private and public sectors. It provides guidelines for managing cybersecurity risks based on five core functions: Identify, Protect, Detect, Respond, and Recover.
- **Cybersecurity Maturity Model Certification (CMMC):** Introduced by the U.S. Department of Defense, CMMC is a mandatory standard for contractors, emphasizing cybersecurity practices to safeguard sensitive data within the defense industrial base.
- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA sets security standards for protecting sensitive health information, ensuring confidentiality, integrity, and availability of medical data.
- **Federal Information Security Management Act (FISMA):** FISMA mandates that federal agencies develop, document, and implement a cybersecurity program to protect government information and operations.

Europe

European cybersecurity regulations prioritize privacy and data protection, with an emphasis on harmonizing standards across member states.

- **General Data Protection Regulation (GDPR):** GDPR is the cornerstone of data protection in the European Union (EU). It sets strict rules on handling personal data, including requirements for data breach notifications, data minimization, and individual rights over personal data. Noncompliance can result in severe fines.
- **Network and Information Security Directive (NIS Directive):** Adopted in 2016, the NIS Directive focuses on the cybersecurity of essential services (such as energy, transportation, and finance) and digital service providers. It requires member states to strengthen their national cybersecurity capabilities and cooperation.
- **European Union Agency for Cybersecurity (ENISA):** ENISA is the EU's dedicated cybersecurity agency, helping to develop and promote cybersecurity standards across Europe, including guidelines for incident reporting and cybersecurity certifications.
- **ISO/IEC 27001:** While ISO/IEC 27001 is a global standard for information security management systems, it is heavily adopted in Europe. This standard outlines processes for systematically managing sensitive company information, ensuring its security.
- **Cybersecurity Act (EU):** The Cybersecurity Act establishes a framework for cybersecurity certification for products, services, and processes, ensuring they meet recognized EU-wide standards.

China

China's cybersecurity regulations are heavily influenced by state control and national security priorities, emphasizing data localization, state monitoring, and the protection of critical infrastructure.

- **China Cybersecurity Law (CSL):** Enacted in 2017, the CSL is the cornerstone of China's cybersecurity framework. It mandates that companies store data within China, and grants government authorities broad access to these data. The law focuses on securing critical information infrastructure and protecting personal data.
- **Multilevel Protection Scheme (MLPS):** MLPS (2.0) is a classification system for protecting information systems based on their potential harm if compromised, ranging from 1 (low risk) to 5 (high risk, affecting national security). The updated MLPS 2.0 imposes stricter controls on sensitive systems and technologies.
- **Personal Information Protection Law (PIPL):** Effective in 2021, PIPL is China's equivalent to GDPR, focusing on personal data protection. It sets stringent requirements for data processing, storage, and transfer, particularly for cross-border data flows.
- **Data Security Law (DSL):** Enacted in 2021, the DSL governs the handling of "important data" and regulates data exports. It requires organizations to categorize data, conduct risk assessments, and comply with national security rules.
- **Technical Committee 260 (TC260) Standards:** China's TC260 develops standards for cybersecurity, covering areas such as data protection, network security, and encryption. These are mandatory for many companies operating in China.

Agilent's information security approach

Understanding the manufacturer's security approach gives customers confidence and trust that devices are developed to the highest standards and align well with their own information and cybersecurity strategies.

Agilent's security program is built on industry standards, including ISO 27002 Code of Practice (ISO), NIST (NIST, 2018), and the COBIT 5 Framework (ISACA, 2012). Our policies, standards, and operating procedures provide a comprehensive approach to maintaining the confidentiality, integrity, and availability of the data and systems within our environment. Security is a companywide priority, and we continuously invest in our people, processes, and tools to strengthen our security posture to protect both Agilent's and our customer's data.

Agilent focuses on:

- Policy, standards, and operating procedures
- IT compliance
- Security operations
- Risk management
- Threat and vulnerability management
- Security awareness

Our overall security approach focuses on these five key areas:

Identify	Identify systems, data, data flows, and regulatory requirements, and determine an appropriate risk management approach.
Protect	Implement measures to protect the environment.
Detect	Monitor the environment and alert appropriately.
Respond	Put processes and people in place to address issues and incidents.
Recover	Enact plans and systems to recover from events.

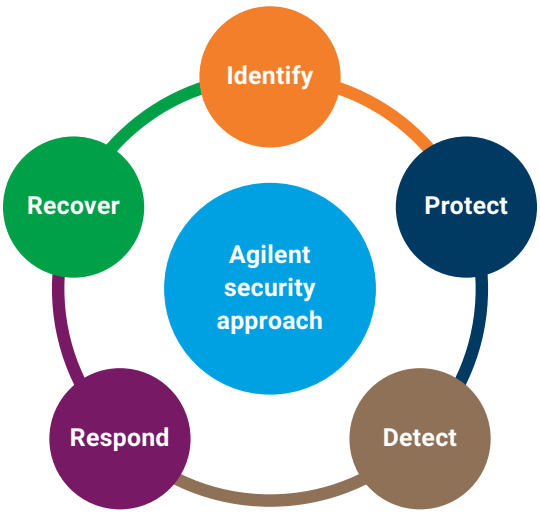

Figure 3. Agilent's information security approach (Agilent, 2024).

Identify

Understanding our environment, the applicable regulatory requirements, and industry and customer expectations is crucial for managing associated risks effectively. We employ the following processes and tools to comprehend Agilent's risk profile and define our ongoing security posture and road map:

- **Threat management process:** We monitor new and evolving threats, collaborating with third parties and using threat information from government agencies.
- **Customer expectations:** Input and requirements from our customers are integrated into our overall security program and, where applicable, delivered as standard controls and solutions.
- **Risk assessment process:** All new systems and changes are reviewed to understand and classify their risk. This assessment covers data, privacy, applications, and server, network, cloud, logical, and physical security.
- **Third-party risk assessment process:** Agilent evaluates third parties to ensure that they comply with our security policies and standards using both internal teams and third-party risk assessment providers.
- **Asset register:** Agilent maintains a configuration management database detailing devices, risk ratings, configurations, and classifications.
- **Regulatory requirements assessment:** With a global presence, and comprehensive product and solution portfolio, Agilent adopts an integrated approach to deploy security standards and controls that address regulatory requirements. Current regulatory requirements include:
  - SOX
  - PCI
  - GDPR
  - HIPAA
  - NIST SP 800-171

Detect

Agilent employs a variety of measures to safeguard the quality, reliability, and accessibility of our environment and data against potential attacks. These measures encompass physical, logical, procedural, and technical aspects in a layered security approach based on risk.

- **Environment controls:** Our facilities, data centers, and server rooms are secured by highly trained security officers and IT professionals.
- **Network protection:** We use firewalls, intrusion detection and prevention systems, email protection, and web content filtering.
- **Mobile device management:** We control the configuration and encryption of all mobile devices accessing Agilent systems or data.
- **Encryption:** We use encryption for data at rest, and in transit where required.
- **Vulnerability management:** We continuously address identified vulnerabilities using appropriate tools, services, and external third parties for assessments.
- **Patch management:** We proactively maintain a process to patch our environment.
- **Security awareness program:** We conduct ongoing training programs for our global workforce on security, compliance, and privacy, including function-specific training and regular phishing simulations.
- **Application security assessments:** A dedicated team assesses developed software before deployment into production.
- **Endpoint protection:** We deploy the latest antivirus and advanced malware detection tools, and use standard build configurations to ensure appropriate security controls.
- **Identity and access management:** We have robust provisioning and deprovisioning processes, least privilege access, privileged account management, third-party access controls, and multifactor authentication.
- **Information rights management:** We use tools to limit access and distribution of data.
- **High availability and backups and disaster recovery:** Our environment is designed to maintain and protect systems and data based on their use and data type.

Protect

As threats continue to evolve, relying solely on protection controls is insufficient. It is crucial to detect and alert to potential risks to the confidentiality, integrity, and availability of our data.

Agilent employs the following measures to monitor and detect potential events in our environment:

- **Security Operations Center (SOC):** Individuals monitor for potential IT security events 24/7.
- **IT operations:** Around-the-clock IT support operations monitor the health of the environment.
- **Antivirus and advanced malware detection:** Network and endpoint tools alert to potential malware detected in the environment.
- **Real-time network monitoring:** Tools using machine learning alert to internal network activity.
- **Event correlation and anomaly reporting:** Big Data solutions correlate operational and security logs to identify and report anomalies.
- **Change management process:** Changes in the environment are monitored to identify potential issues.
- **Database activity monitoring:** Monitoring and reporting on database activity.
- **Threat monitoring and hunting:** Threat-hunting based on industry information and active exploits.

Respond

Taking prompt action in response to potential attacks, breaches, or disruptions is crucial to minimize their impact on the confidentiality, integrity, and availability of our environment. Agilent emphasizes the importance of people and processes in ensuring an appropriate response.

- **Incident response plan:** Agilent has documented security incident response plans that define roles and responsibilities. These plans include regular exercises to test against evolving threats and focus on continuous improvement.
- **Incident response team:** This dedicated team leads investigations into security-relevant events identified by the SOC, using detection tools or individuals.
- **IT incident and problem management:** IT support teams handle nonsecurity-related incidents and events to ensure a robust environment, maintaining availability and integrity of the systems and data.

- **Reporting security issues or concerns:** If you are concerned about security, or have identified an issue related to Agilent, our services, products, or websites, please contact our Corporate IT Security Incident Response Team (CITSIRT) – CITSIRT@agilent.com. The team will review your submission and respond to you appropriately. When contacting the team, please provide the following information to support the investigation:
  - Product, service, or website name
  - Description of the issue
  - Impact of the issue

Recover

Our approach to responding to security events emphasizes assessing and mitigating the impact of incidents. We have established plans and processes to restore affected environments to a known, reliable state. Agilent prioritizes recovery processes, supported by dedicated tools and teams, to restore environments following an attack, data loss, or integrity impact event.

- **Disaster recovery planning:** We maintain documented and tested disaster recovery plans based on system ratings.
- **Communications:** We have a notification process to inform impacted parties during and after an event.
- **Continuous improvement:** We integrate operational, test, and theoretical findings into continuous improvement of our programs and roadmaps.

InfinityLab Assist Hub cybersecurity capabilities

The InfinityLab Assist Control Software runs on the InfinityLab Assist Hub and is displayed on the InfinityLab Assist Interface for local control of the instrument. The user interface is designed to be intuitive and to support the laboratory user as an assistant with everyday work. The software running on the Assist Hub can also be accessed remotely through most browsers. The InfinityLab Assist Hub, as well as the InfinityLab Assist Control Software, have been developed to directly target cybersecurity improvements in the laboratory environment. CDS-related features require LC drivers, version 3.8 onward.

InfinityLab Assist Hub—providing a physically separated module network

The Assist Hub offers a dedicated LAN port, as well as four Ethernet ports, forming a physically separated network for connecting modules. Module access is only possible through the Assist Hub. Modules cannot accidentally be exposed to the corporate network. On the software side, a secure encrypted connection to the driver can be used. This approach also allows an Agilent OpenLab CDS Client-Server system to have the Agilent Instrument Controller (AIC) as well as the LC through the Assist Hub securely on the same network, which facilitates a virtualization approach for the AIC.

InfinityLab Assist Control Software

Role-based access control (user authentication): The system implements five user roles, described in Table 2. Each role is protected by an individual four-plus digit pin. It is recommended to raise the number of digits to at least six when protecting the administrator account.

Table 2. Overview of roles.

User Role	Description
Administrator	The user has full access to the Assist Control Software.
Lab Analyst	The user can view all screens of the Assist Control Software, and is allowed to: – abort tasks or maintenance procedures – start quick actions from the status screen – run tasks interactively – edit role-specific notification settings – edit role-specific home screen layout
Maintenance Technician	The user has full access to the Assist Control Software, except for editing security settings and editing the ambient screen.
Agilent Service Technician	The user has full access to the Assist Control Software, except for editing security settings and editing the ambient screen.
Viewer	The user can view all the screens in the Assist Control Software but is not able to execute tasks, perform maintenance, or access troubleshooting guides.

Access token: If the "Access Token Required" feature is enabled (default), only LC drivers that have been previously identified by confirming the first connection on the Assist Hub can connect to the instrument. When an LC driver tries to connect for the first time, the connection needs to be confirmed or rejected by the administrator within the InfinityLab Assist Control software. Existing tokens can be invalidated by the administrator. Only a confirmed connection establishes the communication between a chromatographic data system using the LC driver and Assist Hub.

CDS-required toggle for guaranteed data logging: This feature was designed to provide additional benefits for compliant environments. When activated with the latest LC drivers installed, users will have view-only access to InfinityLab Assist unless a data system is connected. Troubleshooting functionality will be available. For informatics environments using existing drivers, CDS required should be disabled. The CDS log notes that the InfinityLab Assist is connected as an "unknown/unconfigured module" and instrument actions are still recorded.

Easy update deployment: An update of the InfinityLab Assist Control software can be deployed through a USB drive or through https://update.pl29.agilent.com/infinitylabassist/ using any modern web browser. Updates require administrator access.

Built-in backup and restore features: With an integrated backup and restore functionality that uses encryption, unaltered recovery is guaranteed, as well as safe storage of backup files.

Encrypted communication with LC drivers: When a TLS certificate is installed, communication between the LC drivers and an Agilent CDS is encrypted*.

HTTPS/TLS browser access: After installing a certificate from the customer's IT department, the software uses only secure browser connections (HTTPS/TLS).

Logging: The system offers an internal log, as well as logging in the various CDS logs.

Addressed cybersecurity threats

Table 3. Addressed cybersecurity threats.

Cybersecurity Issue	Agilent InfinityLab Assist Hub/ InfinityLab Assist Control Software Feature
Legacy Systems with Weak Security	Easy deployment of updates through a USB drive at the machine or through a connected browser
Lack of Segmentation Between IT and OT Networks	Facilitating better segmentation by moving modules as early as possible to a physically separated network
Inadequate Patch Management	Continuous software improvements and a rigorous QA together with easy deployment allow for up-to-date machines
Lack of Security Monitoring	Logging provided for environments requiring compliance allows tracing of violations
Weak Authentication and Access Controls	Role-based access offering five predefined roles including a view-only role, CDS-access token
Insider Threats	Role-based access, log-based monitoring, encrypted driver connection
Remote Access Vulnerabilities	Role-based access over an encrypted HTTPS connection
Insecure Communication Protocols	Secure encrypted driver communication, secure browser connection, access token
Ransomware and Malware	Closed system with manufacturer-certified software only
Third-Party and Supply Chain Risks	Addressed by Agilent's QA policy as well as our approach to information security
Physical Security Weaknesses	N/A: Customer's physical access control, locked cabinets
Denial of Service (DoS) Attacks	N/A: Customer's OT security policy, traffic filtering, network segmentation
Insecure Configuration of Devices	N/A: Customer's OT security policy

N/A = Not applicable

Additionally, customers of an Agilent Infinity II system can easily integrate the InfinityLab Assist Hub into their existing setup and take advantage of its cybersecurity features.

Conclusion

With the initial release of the InfinityLab Assist Control Software, the InfinityLab Assist Hub offers plenty of cybersecurity features that can be leveraged for a secure lab network environment founded on a customer-specific OT/IT security strategy.

* Consult your local representative on discrepant behavior of your CDS installation/setup.

Index of abbreviations

References

1. InfinityLab Assist User Manual. *Agilent Technologies user manual*, document number D0113047 Rev. A, **2024**.
2. Agilent Technologies Information Security Web Page. https://www.agilent.com/about/workingwa/information-security/ (accessed 2024-11-18).
3. Claroty IT vs OT Security: Key Differences In Cybersecurity Web Page. https://claroty.com/blog/it-and-ot-cybersecurity-key-differences/ (accessed 2024-11-14).
4. Proposal for Directive on Measures for High Common Level of Cybersecurity Across the Union. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (accessed 2024-10-12).
5. What is Industry 4.0? IBM Web Page. https://www.ibm.com/topics/industry-4-0 (accessed 2024-11-15).
6. COBIT 5 Framework ISACA Web Page. https://www.isaca.org/resources/cobit/cobit-5 (accesssed 2024-10-12).
7. ISO Web Page. https://www.iso.org/standard/75652.html (accessed 2024-10-12).
8. Pharma 4.0. ISPE Web Page. https://ispe.org/initiatives/pharma-4.0 (accessed 2024-11-15).
9. Extending Operational Technology to Azure Web Page. https://techcommunity.microsoft.com/blog/azureinfrastructureblog/extending-operational-technology-to-azure/3265466 (accessed 2024-11-12).
10. Cybersecurity Framework V1.1. NIST Web Page. https://www.nist.gov/cyberframework/csf-11-archive (accessed 2024-10-12).
11. What is operational technology (OT)? RedHAT Web Page. https://www.redhat.com/en/topics/edge-computing/what-is-ot. (accessed 2024-11-12).

www.agilent.com/lc/infinity-iii-upgrades

DE-006950

Printed in the USA, May 20, 2025
5994-8261EN

Agilent
Trusted Answers