Google Cloud

Office of the CISO

Manufacturing & Industries

Security Guidance for Cloud-Enabled Hybrid Operational Technology Networks

July 2025

Contributors

Vinod D'Souza,
Office of the CISO

Sri Gourisetti,
Office of the CISO

Nick Panos,
Office of the CISO

Jon Watson,
Office of the CISO

Paul Shaver,
Mandiant

Chris Sistrunk,
Mandiant

Lukas Grimfors,
Office of the CISO

Camille Felx Leduc,
Mandiant

Rohan Kanungo,
Office of the CISO

Jose Giron,
Mandiant

Table of contents

1. Introduction

The adoption of cloud services within the manufacturing and industrial (M&I) and energy sectors[1] is a significant opportunity for both operational and security enhancements. Cloud platforms accelerate data-driven optimization of both business operations and engineering processes while providing the foundation for AI-powered digital immune systems with integrated security. This technological leap enables secure hybrid manufacturing networks with information technology (IT) and operational technology (OT) systems.

Cloud services allow chief manufacturing officers (CMOs) and chief digital/technology officers (CD/TOs) to securely digitize operations, drive down costs, and generate revenue streams. Cloud migrations also empower chief information security officers (CISOs)/chief security officers (CSOs) to protect these business operations while maintaining process safety. For a CMO and CISO to achieve their occasionally competing goals, a strong strategic alignment between business and cybersecurity operations is necessary. A blueprint for this alignment can be found in the blog series on security-inclusive site management.

In this report, we focus on actionable and tactical security guidance for manufacturing OT systems with an emphasis on safe and secure hybrid OT networks, regardless of which cloud provider you are using.

A recap of the manufacturing threat landscape

The rapidly evolving manufacturing and industry threat landscape further exacerbates the complexity of manufacturing security and necessitates a holistic approach to security that addresses IT, OT, product engineering, and supply chain security. A broad spectrum of bad actors, ranging from state-sponsored advanced persistent threats (APTs) to hacktivists to financially motivated ransomware groups, target this space. And recent data suggests that the manufacturing sector is one of the most targeted global sectors.

In the context of manufacturing processes, vulnerability exploitation is a top vector, followed by others such as insecure and inadvertent exposure to the internet, weak identity and access management (IAM), and lack of segmentation. Multiple recent incidents indicate that the impact on the manufacturing process can be direct or indirect. A direct impact would be due to a targeted attack on the manufacturing processes, operations, and systems – IT or OT. An indirect impact would be due to an attack on enterprise IT systems, including enterprise resource planning (ERP) and manufacturing execution system (MES), that may force the organization to shut down the manufacturing processes/operations. Irrespective of the nature of the incident, any direct, indirect, or perceived threats to the production systems could have direct safety, security, productivity, availability, and reliability implications on the manufacturing processes and the overall business operations. The increase in Software as a Service (SaaS) offerings from OT application vendors and the opportunity to use secure cloud infrastructure offers a significant opportunity. This paper provides manufacturing and security leaders, engineers, integrators, architects, and security analysts with an actionable blueprint that doesn't expand the attack surface or expose critical systems to threats.

[1] The Google Cloud categorization of the manufacturing and industrial (M&I) sectors includes (but is not limited to) organizations from the following sectors and subsectors: industrial manufacturing and assembly, automotive, process manufacturing, electronics and semiconductor, power and energy, construction, consumer packaged goods, logistics and transportation, and aerospace and defense.

2. Evolution of hybrid OT networks

A standard industrial OT architecture, if represented using the Purdue Enterprise Reference Architecture (PERA[2]) model with a demilitarized zone (DMZ) can be visualized as shown in Figure 1. In a security-centric, traditional OT architecture, there are physical and logical security controls between each level and between systems within the levels of industrial or manufacturing zones. Adhering to the IEC 62443 standard and NIST 800-82 guidance, the secure means of facilitating the communications across the OT architecture is by using zones and conduits. Could something like the following work here?

To significantly bolster security-inclusive OT operations, it's crucial to implement security-focused leading practices. These include deploying dedicated network services, separate from enterprise networks, with OT-specific IAM and dedicated OT network services. This should be combined with monitoring, segmentation, role-based access controls (RBAC), granular firewall rules, and a secure and encrypted unidirectional connection from the OT to the virtual private cloud (VPC).

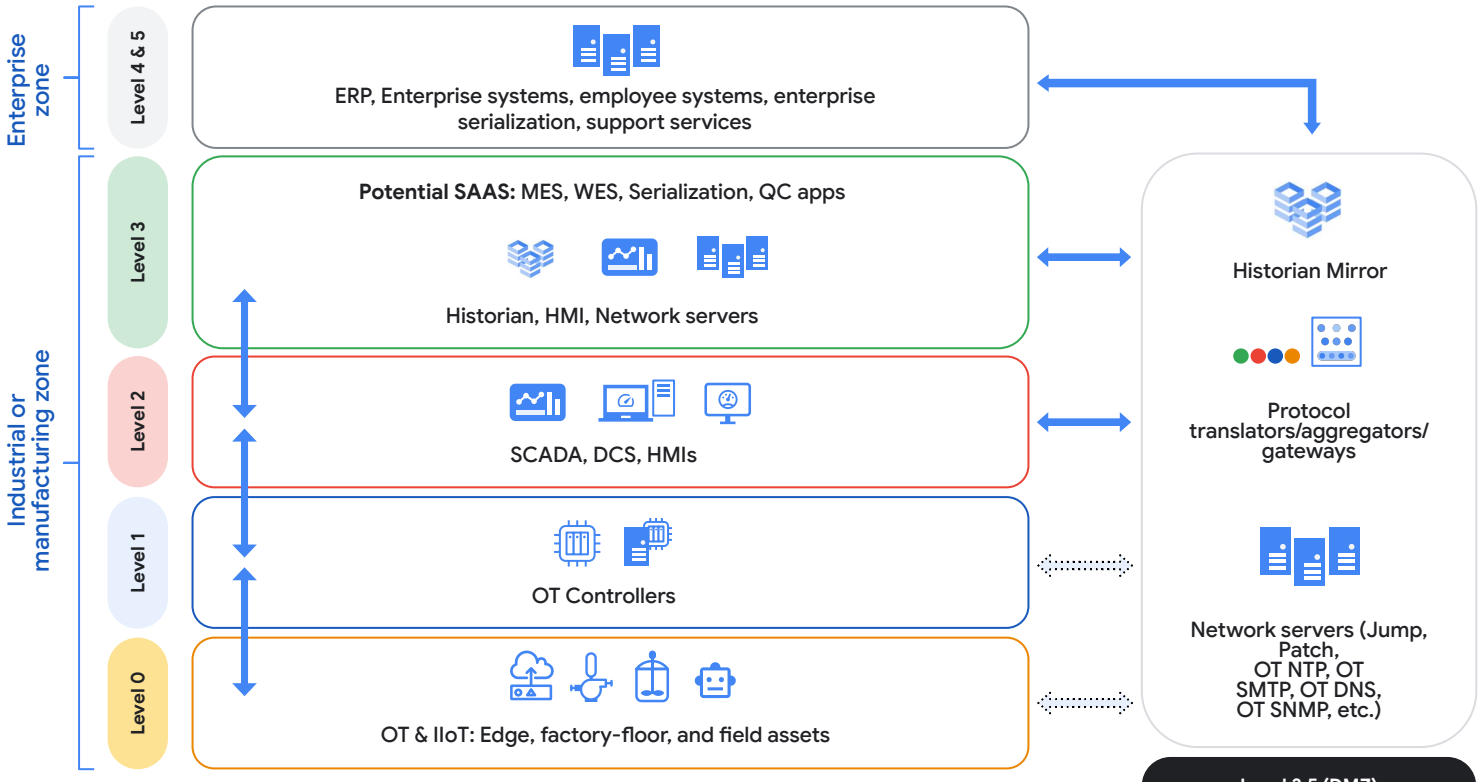

Figure 1. Illustration of an OT architecture using the PERA model[3] with DMZ[4]

[2] PERA provides a good discussion mechanism. The intent is not to project PERA as a network or security architecture; instead, the goal is to use it to present the OT security concepts. Therefore, consider the diagrams in this document as adoptions of the original PERA, NIST 800-82 architectures, and diagrammatic representations from other similar sources. Organizations should design their own network and security architectures that meet their business needs. Apply the 80–20 rule when using the guidance from this document, as some of the recommendations may not be agreeable to all experts in the OT security space. Google Cloud Security is open to feedback and recommendations for future iterations.

[3] Broadly, the manufacturing network can be visualized as three zones: (1) enterprise zone, (2) demilitarized zone(s) or DMZ, and (3) industrial or manufacturing zone. These zones may have multiple subzones. Multiple network segments and VLANs exist across and within these subzones and zones. This zone-based visualization can be combined with PERA as follows: (1) Levels 4 and 5 are under the enterprise zone, (2) Level 3.5 is the DMZ, and (3) Levels 0–3 are under the industrial or manufacturing zone.

[4] The solid double-headed arrows from PERA levels 2, 3, 4, and 5 to 3.5 are the network connections that most likely exist. The dotted double-headed arrows from PERA levels 0 and 1 to 3.5 indicate either non-existent direct connections (i.e., connection through a parent level 2 or 3 system) or niche IIoT devices with functionality that spans across PERA levels 0–2 and may use network services from 3 or 3.5.

Traditional OT networks have been constantly evolving, driven by the integration of SaaS-applications, built-in digital artifacts and controls, Industrial Internet of Things (IIoT) for granular sensing, and remote monitoring. These evolutions have opened doors to newer and more sophisticated solutions using cloud systems – a family of security-centric infrastructure and services that can be leveraged for rapid design and development in IT and OT environments. By combining Google Cloud security capabilities with partner security solutions, OT process owners can use Google Cloud to address the goals of secure infrastructure architectures, comprehensive on-premises and cloud monitoring, and rapid incident response and recovery.

A modern cloud or cloud-embracing environment as shown in Figure 2 simply builds upon the traditional on-premises architecture that is shown in Figure 1. This presents an opportunity for OT process owners and pertinent business owners to migrate on-premises computing and data management infrastructure to Google Cloud without impacting local controls. At the start of any transformation or change, the business and engineering teams should evaluate the direct impacts and value to the business objectives. Cloud services can simplify efforts and streamline processes across manufacturing optimization, business intelligence, cybersecurity, and other business avenues. Using cloud services does not change the fundamental security principle of ensuring secure, safe, reliable, and resilient operations with high availability.

The best practices pertinent to securing hybrid OT networks with SaaS and cloud-connected services are grouped under the following thematic areas:

- Secure strategic cloud transformation
- Security-by-design, security-by-default, security-in-deployment
- Asset management program
- Cyber-physical modularity
- Attack surface and internet exposure
- Manual operations and safety
- Software and hardware process reproducibility
- Preventive maintenance and security testing
- Supply chain transparency
- Incident response and disaster recovery
- Google Cloud tools and services for secure OT connectivity

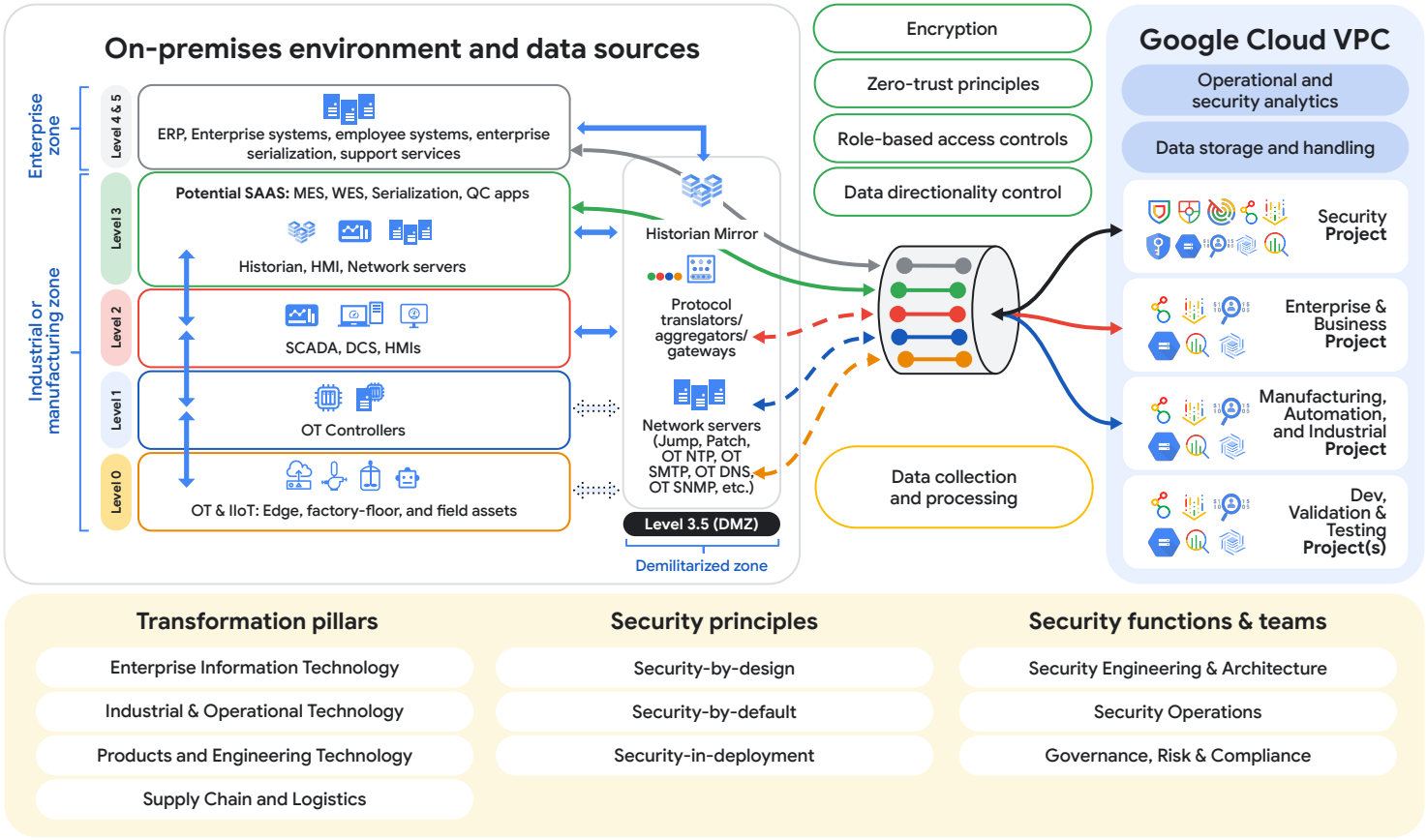

Figure 2. Illustration of a hybrid OT architecture with Google Cloud using the PERA model[5]

[5] The double-headed arrows between on-premises and the virtual private cloud (VPC) are not intended to indicate bidirectional communications. Depending on the risk assessment, as well as business and engineering goals, the communications are to be architecturally determined as unidirectional or bidirectional. Specific best practices around directionality are discussed in the later sections of this document.

3. Strategic, operational, and tactical security checklists

Operational and tactical approaches to secure OT networks rely on various security processes, controls, hardening, and strategic placement of tools and services across the network and systems. To achieve a scalable defense-in-depth approach, fundamental enforcers – such as up-to-date planning and operational network architectures, information flow discoveries and definitions, systems interconnections coupled with the physical inventory – are needed for an operational-level understanding of the system-to-system operational and data dependencies.

The engineering teams should continue on this journey to enumerate industrial control system ICS/OT protocols used, direction of read/write tags across their supervisory control and data acquisition (SCADA), distributed control system (DCS), historian, and open platform communications (OPC) servers; expected controller commands; function codes between components and applications; and other PERA levels 0-2 components within their network. Then systems and their communication paths should be overlayed with assigned protection levels for each system or subsystem during inventory activities to help determine the security controls needed to protect and defend the systems without compromising or degrading their performance. The checklists presented in this section leverage best practices from zero-trust principles, NIST 800-82, and IEC 62443, and they are intended to serve as guidance for on-premises and hybrid (cloud-connected) OT environments. A reference architecture that adheres to Google Cloud's security philosophy is shown in Figure 3.

Organizations should approach hybrid architecture security from two fronts: (1) on-premises OT security and (2) secure cloud operationalization for OT. The following checklists provide operational and tactical security considerations for security and engineering teams across those two fronts. The security and engineering teams can tactically use the architectural guidance in this document to achieve secure on-premises architectures and leverage Google Cloud products and services, including the built-in/integrated security suite, for a holistic hybrid network security.

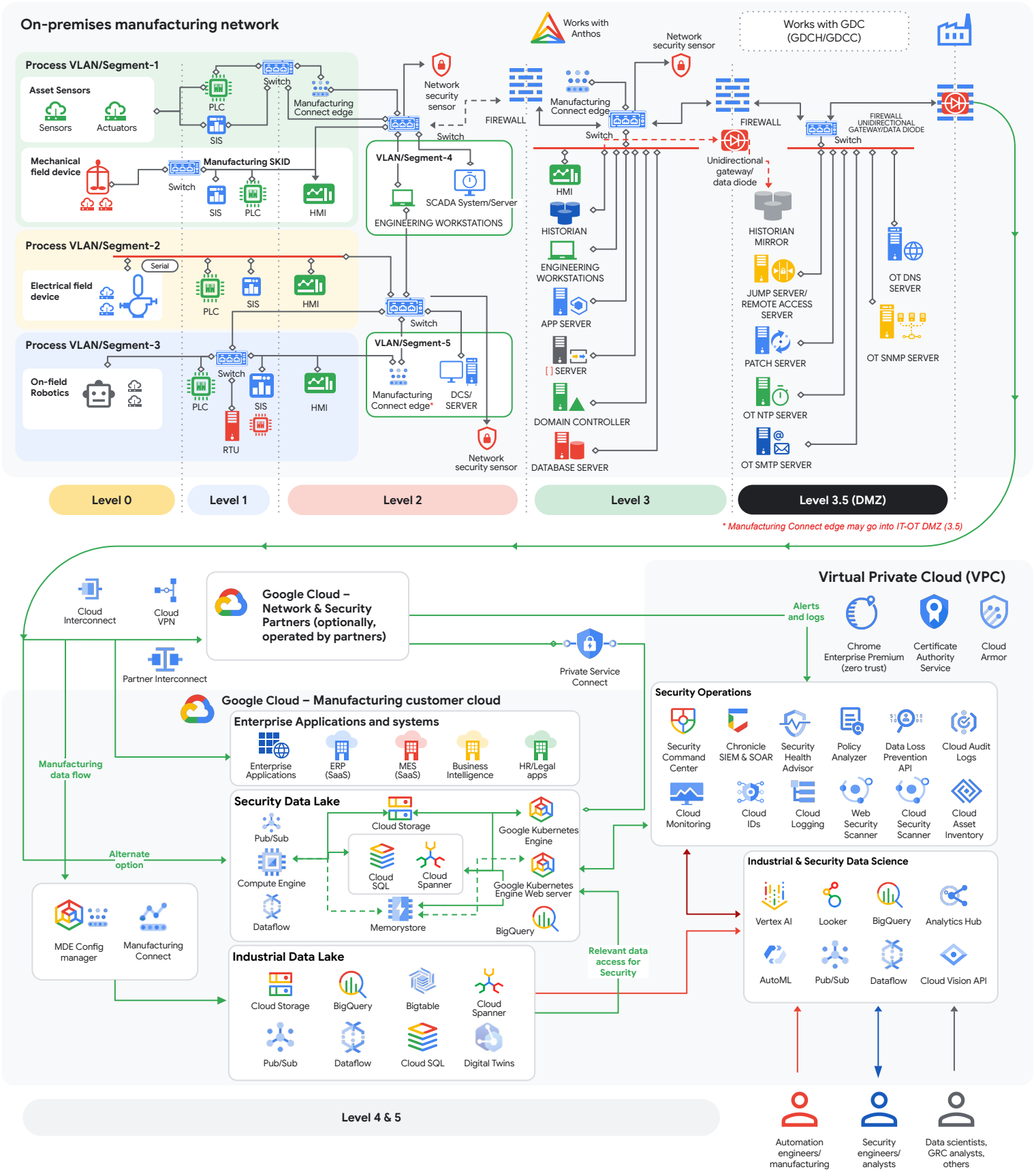

Figure 3. Illustrative Operational and tactical OT architecture with Google Cloud using the PERA model[6]

[6] Clarification on the placement of "Anthos" and "Google Distributed Cloud (GDC)" boxes on the on-premises overlay rectangle: This is to indicate the ability to run OT applications on systems such as GDC, which is Google's on-premises solution for air-gapped and on-premises use cases. GDC can run containers and common operating systems seen in most OT networks.

3.1. Secure strategic cloud transformation

- ❏ Ensure that the security engineering, security operations, governance risk and compliance (GRC), and functional manufacturing and automation teams are equipped with OT security, cloud security, and cloud engineering expertise.
- ❏ Identify and **migrate enterprise IT** assets that are expected to interact with the OT zones.[7]

  Note: It is common to see SaaS or self-hosted applications such as the ERP, configuration management database (CMDB), and similar. These use either a cloud service provider or on-premises hypervisors. Migrating these systems to Google Cloud would not be detrimental to their interaction with OT applications such as the MES, warehouse execution system (WES), and others.
- ❏ Identify and consider **migration of the industrial OT** systems/applications that can be migrated to Google Cloud.[8]

  Note: Examples include historian replicas, one-way SCADA replicas for centralized monitoring (no controls to be issued from the cloud application to on-premises OT systems), serialization, quality-control systems such as quality management system (QMS), data science systems such as manufacturing science and technology (MSAT), and execution systems such as the MES and WES. Most of these systems are already offered as SaaS/self-hosting deployments.
- ❏ Identify and **migrate product and engineering** technology systems, including custom software applications.
- ❏ Identify and **migrate supply chain/track-and-trace systems**, including third-party risk management, security rating services, demand forecasting systems, software bill of materials (SBOM), hardware bill of materials (HBOM), and transportation management systems such as asset-in-transit tracking systems.
- ❏ Use Google Cloud's security and resilience framework as a guiding resource to structure your IT and OT cybersecurity program.
  - ❏ Identify measurable cyber-physical resilience opportunities and leading indicators to determine the resilience posture of the OT networks.
  - ❏ If AI is involved/used in procured or in-house applications, leverage secure deployment of AI best practices.
- ❏ Make threat intelligence-informed risk-based decisions. Use Google Threat Intelligence and M-Trends to gain sector/industry-specific cyber threat intelligence to inform your decisions. Make security decisions within OT environments that are driven by data, evidence, and threat information.
- ❏ Integrate threat modeling principles and philosophy across all phases of engineering and security processes. Threat modeling should be at the core of all strategic, operational, and tactical decisions that impact any business and engineering functions. This allows organizations to augment a compliance-based approach with a threat-centric approach to security.
- ❏ Take advantage of Google Cloud's shared fate model and leverage Google's expertise in architecting your OT security policies, procedures, policy-as-code templates, standards, and guidance. Professional services through the Office of the CISO (OCISO), Google Cloud Consulting, and Mandiant Consulting are positioned to advise customers in designing their security foundation, strategy, and optimal methods of operational and tactical enforcement of a CISO's vision.

---

[7] It is imperative to perform a risk assessment on the migration of enterprise IT assets that interact with OT zones in the cloud before they are migrated. If the enterprise IT asset cannot communicate with OT zones, organizations should evaluate what impact that has to OT/operations. For additional information on this process, use guidance from sources such as NCSC's guidance on OT and SCADA in the cloud, and NERC (energy sector).

[8] This should be determined based on a risk assessment. For instance, if the OT systems require high-speed controls and low latency, then they should not be migrated to the cloud if such migration results in additional latency or loss of needed availability. There are valid use cases for some SCADA/ICS/OT to issue controls to on-premises, but only for OT that doesn't require high speed and low latency, or if the on-premises systems cannot operate independently due to telecommunication outages to the cloud.

3.2. Security-by-design, security-by-default, security-in-deployment

- ❏ Use a **defense-in-depth architecture** instead of relying on a single security control, as failure of a single control could have catastrophic consequences
  - ❏ Map security objectives and security controls in place. Leverage frameworks and standards such as the NIST CSF, NIST 800-82, and NIST 800-53, in addition to the guidance from IEC 62443. Identify control gaps and requirements for additional layers of security.
- ❏ Adopt **security-by-design and security-in-deployment principles** and enforce effective system and network segmentation, and boundary protection.

  Note: Security should be treated as a contributor with the same level of importance as other business and engineering entities. Ensure that security requirements are included in the standard operating procedures (SOPs) and company-wide policies, and ensure that security is included in the site acceptance tests/factory acceptance tests (SATs/FATs).
- ❏ Physically segment the on-premises IT and OT networks using a hardened demilitarized zone (DMZ). Perform physical segmentation within the on-premises OT networks between process-based zones. If physical segmentation within OT is not feasible, at least perform logical segmentation using virtual local area networks (VLANs) and subnets. Physical segmentation may involve using dedicated physical firewalls, unidirectional gateways, secure aggregators or gateways, and unshared hardware.
- ❏ For user access, use strong, unique, unshared passwords combined with multi-factor authentication (MFA) for all access. Exceptions must be reviewed and approved on a case-by-case basis. All privileged/admin access and users must be mandated to use MFA under all circumstances. Privileged/admin accounts should not be used for business as usual (BAU) activities.
- ❏ Use long passwords with 120-day rotations for service accounts. Where possible, use certificates or short-lived certificates combined with machine-identity solutions for secure machine-to-machine communications.
- ❏ For all computing systems within OT, harden them using Center for Internet Security (CIS) Benchmarks or a security technical implementation guide (STIG). Ensure principles of least functionality are enforced and only necessary services, ports, and protocols are in place. Everything else is disabled. Take a similar approach to harden all OT-connected cloud systems leveraging Google Cloud Policy Controller bundles, infrastructure configuration recommendations, and CIS compliance-based configurations. Use Google Cloud's Compliance Manager, Control Navigator, and Audit Manager (through Security Command Center) to automate and scale security controls enablement and hardening efforts.
- ❏ Ensure encryption in place (when feasible for OT and always for cloud connections) and role-based access controls (RBAC) associated with all network segments.
- ❏ If needed and feasible, organizations can consider the option of allowing programmable logic controllers (PLCs) and lower-level controllers to send logs to the security information and event management (SIEM) or network security monitoring (NSM) in a unidirectional manner.[9]
- ❏ Implement the Top 20 PLC controls to harden PLCs and lower-level controllers.
- ❏ Ensure allowlists and denylists pertinent to OT system access require connections to be initiated from the approved OT zones. Do not allow external connection initiations, unless necessary on a case-by-case basis. Such requests should come with business justification and should be reviewed after the business justification has expired.

[9] Windows and Linux in OT logs should be collected. PLC logs, where possible, should be collected on a risk-based approach. Also, some PLC manufacturers collect logs with their own software, such as Rockwell Automation FactoryTalk AssetCentre.

- For shared services between IT and OT networks, pass the connections and traffic through IT-OT DMZ (PERA level 3.5).[10]
- Use DMZ for secure cloud/virtual private cloud (VPC) connectivity. Google Cloud's secure hybrid connectivity solution, Manufacturing Data Engine (MDE) (see Figure 4), can be leveraged for such use cases. MDE relies on Manufacturing Connect edge (MCe) that is deployed in the IT-OT DMZ and establishes an encrypted, configurable unidirectional data flow connection from OT to the VPC. Use DMZ as a termination and reinitiation (with reauthentication and reauthorization) for traffic between OT and IT networks. This approach can contribute to reducing potential lateral movement risks from IT to OT.
- Ensure a combination of endpoint monitoring (for example, endpoint detection and response [EDR] where possible or necessary[11]), network monitoring through NSM (where needed in OT), intrusion detection system (IDS)[12], and SIEM (including IT and OT visibility) for logging, alerting, continuous monitoring, and intrusion detection are in place.
- Use continuous detection and continuous response (CD/CR) to adopt security operations practices of continuous integration and continuous deployment (CI/CD) for SIEM and security orchestration, automation, and response (SOAR) management.
- If possible, allow PLC software suites, PLCs, and lower-level controllers to send logs to the SIEM or NSM software in a unidirectional manner.
- Run EDR in passive mode (alert only, deny/drop nothing[13]) on supporting OT-related computing systems and servers[14]. Rely on NSM and nonintrusive scanning to monitor lower-level controllers.
- Implement restrictive allowlist-based firewall policies (deny all, permit by exception). Firewall rules should specify IP addresses, specific transmission control protocol (TCP)/user datagram protocol (UDP) ports (avoiding broad port ranges), and stateful inspection. IP addresses should be constrained to /28 at the minimum.[15] Similarly, all outbound traffic from the OT network to the enterprise IT network (and VPC) must be restricted by both source and destination IP address, plus service and port. In critical networks and as needed by regulations, unidirectional gateways can enhance boundary protection and enforce logical tamper-resistance.
- Use proxies to access OT and any mission-critical systems. Deny all direct access to such systems. For the OT-connected systems hosted on Google Cloud VPC, use Identity-Aware Proxy (IAP). Complementary forms of secure connection OT-related systems on Google Cloud VPC include using a bastion host, Cloud VPN, or Cloud Interconnect.
- Configure security domains[16] with separate network addresses (disjoint subnets).
- Common PERA level 3 systems, such as master servers and historians, are accessed by non-OT business processes only through replicated instances. Ensure that network services such as lightweight directory access protocol (LDAP), Active Directory (AD), domain name system (DNS), network time protocol (NTP) patch servers, and so on are dedicated to the OT networks and not shared with enterprise IT. If that's not possible, then an AD assessment should be conducted to ensure that all AD attack vectors are accounted for in the risk register and are mitigated/controlled with continuous assessments.
- Identify the network hotspots (network areas of high activity) and ingress/egress points. Align ingress/egress points and hotspots to prioritize network traffic collection and monitoring. This activity includes identifying north-south and east-west traffic/connections and ensuring the connections are authorized.

---

[10] A DMZ offers an extra security layer for shared services by preventing persistent traversal between trust zones. The decision to use a DMZ should stem from a risk assessment and compliance needs. Alternatively, some customers are exploring secure architectures that replace DMZs (which are essentially firewall zones) with options like unidirectional gateways, dedicated/partner interconnects, well-managed firewall rules (though these require careful upkeep to avoid staleness and increased attack surface), or cloud VPNs with strong IAM and MFA.

[11] This is operating system (OS) dependent. For instance, Chromebooks would not need an additional EDR due to built-in endpoint security features.

[12] Intrusion prevention systems (IPSs) have the potential to introduce latency/jitter, and in some cases, they could drop packets. Because of the potential safety and productivity reasons, IPSs are often avoided in the OT environments. Organizations should conduct a risk assessment, determine their risk appetite and risk tolerance and decide if they should use an IPS or IDS.

[13] This has to be determined based on the risk assessment and profile. If a production interruption is typically acceptable while production malfunction is unacceptable, perhaps denial may be an option as long as there are no safety risks.

[14] Some operating systems may not need to use EDR (for example, ChromeOS). Businesses should evaluate their inventory and act accordingly.

[15] This recommendation is based on the most typical OT networks, which are segmented at a process level and broken into multiple private subnets. In cases where the company has matured, microsegmented architecture (segmentation at an IP or a system level), consider using granular firewall rules to restrict down to individual IPs.

[16] Security domains refer to a logical or physical grouping of resources (such as servers, applications, data, and users) that share a common security policy, trust level, and set of security controls. Essentially, it's an area within a network infrastructure where a consistent level of security is applied and enforced. Separating these domains with disjoint subnets helps to isolate them, limiting the impact of a security breach in one domain on another.

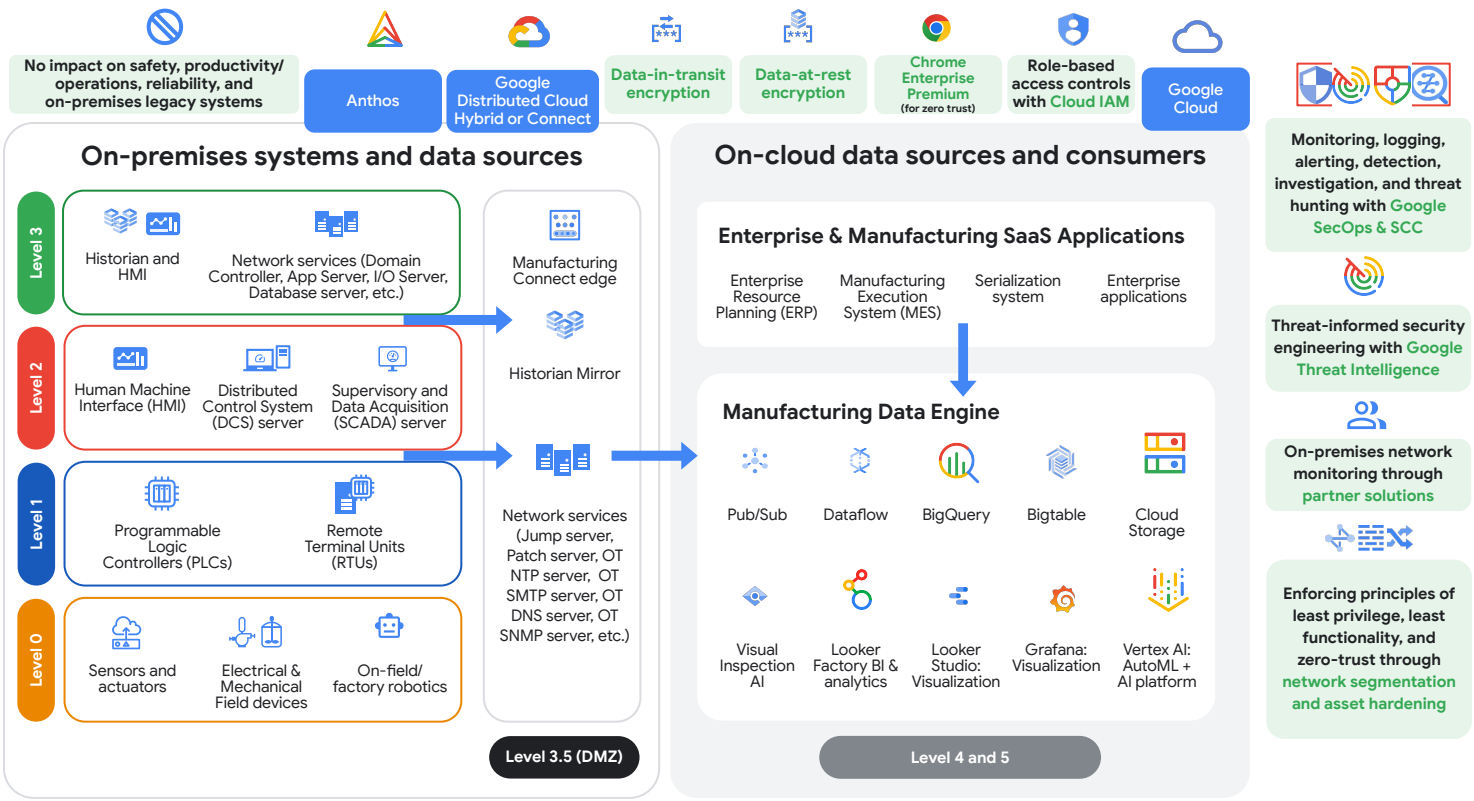

Figure 4. MDE as a secure on-premises gateway to Google Cloud VPC

3.3. Asset management program

- Establish a robust **asset management program**. Maintain **up-to-date inventory** of all OT assets and their connections, including to the IT and cloud systems. Change management, clear and up-to-date documentation, and critical spare equipment are also important to include in the asset management program.
  - Maintain up-to-date network diagrams that are evaluated at least quarterly or as per the organization's policy.[17]
  - Maintain regular backups, online and offline, of all OT systems. Ensure that backups are included in change management standard operating procedures. Test backups at least yearly.
  - Trace and track all cloud connections and data flows from and to the OT networks.
  - Perform continuous periodic review of firewall rules to ensure that the rules are still applicable at the time of inspection. If feasible to use next-generation firewalls, consider performing a near-real-time review of firewall rules. This step should be part of the change management process. Also, perform near-real-time monitoring and review of firewall logs.

    Note: It is fairly common to see a firewall with temporary rules that have effectively become permanent and haven't been used in years due to lack of firewall governance processes. This presents a possible vector for adversaries to gain access to the OT environment.
  - Maintain a list of approved and/or denied OT hardware and software vendors and products for consistent procurement practices across the organization.

    Note: The goal is not to discourage heterogeneity in product procurement. For a product type/class, the security team can identify multiple approved vendors. The goal is to ensure a form of governance in the procurement process.
  - Leverage a combination of on-premises and on-cloud active scanning and passive monitoring tools to automate asset discovery and inventory management.
  - Perform correlation between assets, vulnerabilities, threats, and impact for an accurate depiction of the overall risk posture. Leverage automation and AI to optimize the efforts with human oversight, confirmation, and to take actions.
  - Maintain comprehensive and up-to-date documentation for all critical ICS/OT systems, including network architecture diagrams, device configurations (including human-machine interface [HMI] dashboards, and PLC programs/program files and configurations), software versions, firmware revisions, and data backup/recovery procedures. This documentation must be stored securely and be readily accessible in case of a cyber incident impacting the ICS/OT environment.

[17] Change management is a critical component. Diagram and document updates should be a regular part of the change management process, which is a subset of asset management.

3.4. Cyber-physical modularity

- ❑ Reduce cascading failures by ensuring **high cyber-physical modularity** through segmentation and segregation.
  - ❑ Identify essential services that require precedence and high levels of sustainability to achieve minimum viable operational delivery objectives in the event of disruptions. Leverage asset inventory and dependencies to perform per-asset failure and impact analysis. Identify redundancy and modularity needs and bottlenecks.
  - ❑ Architect the OT systems and networks with well-defined security zones. Isolate critical processes and minimize interdependencies to limit the impact of security breaches.
  - ❑ Implement protective devices and redundant systems (for example, network segmentation, backup power supplies, or fail-safe valves) to prevent cascading failures and ensure operational continuity in the event of an incident. Leverage cloud systems to achieve seamless data and application redundancies.
  - ❑ Ensure segmentation and microsegmentation (when feasible) strategies are implemented as opposed to a flat network. This allows you to minimize blast radius and overall damage in case of a cyber event or incident.
    - Identify all industrial processes. Implement process-level segmentation. Physically (or at least logically) segment these zones and subzones, including termination of all process-to-process communications if not needed. Use network access control (NAC), dynamic VLANs, and private VLANs to microsegment the OT networks.
    - Segment all OT-connected cloud systems following the Google Cloud resource hierarchy recommendations (illustrated in Figure 2 under *Google Cloud VPC* and in Figure 3 under *Google Cloud – Manufacturing customer cloud*).

3.5. Attack surface and internet exposure

- ❑ Eliminate all unintended and unnecessary OT exposures to the internet.
- ❑ Leverage Manufacturing Data Engine (MDE) or similar solutions for secure connection from OT to cloud and IT networks.
- ❑ Leverage air-gapped solutions such as Google Distributed Cloud (GDC) or similar for OT applications that are required to be on premises while having the advantages of a cloud-like environment.
- ❑ Identify critical OT processes and systems that require external network connectivity. This includes third-party/vendor monitoring of the building management system or facility utilities. Prioritize these for enhanced security and resilience measures. Perform a thorough external exposure analysis and risk assessment.
- ❑ Establish redundant communication channels for critical OT systems (such as dedicated fiber lines, cellular, or satellite) if possible to ensure continuous operation in case of primary network failure or compromise.
- ❑ Conduct regular drills simulating communication failures to validate backup communication systems and personnel training to ensure operational continuity during cyberattacks or disruptions.
- ❑ Help ensure that the endpoints (on-premises OT and OT-connected systems on VPC) are not exposed or directly accessible from the public internet. Perform attack surface management and external exposure analysis. Mitigate any exposures and vulnerabilities.

3.6. Manual operations and safety

- ❑ **Ensure manual operations** as a backup method of operation when automation fails. Ensure **isolation of safety systems** even in a fully automated environment.
  - ❑ Maintain an adequate degree of manual and local control of OT systems. Use manual operations in case of automation failures or compromises.
  - ❑ Help ensure business continuity by running at least critical operations in a degraded mode during failures. Leverage asset inventory, dependencies, and crown jewel analysis to proactively establish security and resilience controls to achieve this.
    - If possible, maintain analog control planes/analog backups as a last resort in the event both primary and digital backup systems fail. Note that this may not be feasible for lower-level OT systems. In such cases, use manual operations and isolated local controls (for example, manual controls through a PLC to the field devices while the HMI is disconnected).
    - For critical IT to OT data flows (such as in ERP or MES), have a backup or manual "paper-based" process to ensure systems can still operate.
  - ❑ Do not expose safety systems. Avoid remote connectivity for safety systems, unless absolutely necessary on a rare case-by-case basis.

3.7. Software and hardware process reproducibility

- Help ensure **software and hardware process reproducibility** using development environments and digital twins.
  - Leverage third-party risk assessment and vendor/product security assessments where applicable to evaluate the product's use and compliance with NIST SSDF and SLSA.
  - Select cloud-based patch management solutions where available. For on-premises OT assets and situations, cloud-integrated automation might introduce complexities that require manual patch processes. Facilitate OT patch management when patches are available, but only upon testing. Embrace automation where feasible and upon rigorous testing and rapid failback mechanisms. Use manual patching processes when automation might have safety implications.
  - Leverage infrastructure as code (IaC) or similar to automate patch testing and deployment processes. This streamlines software updates for critical systems, decreasing operational downtime and the risk of disruptions.
  - Use production-analogous development environments and digital twins (where possible) within Google Cloud for application replication and patch testing for all OT applications.
  - Help ensure security controls are in place to revert to a known good state in case of unexpected failures after patching. Always securely maintain a golden image to use as needed.
  - Use augmented continuous integration and delivery (CI/CD) principles (see Figure 5) for rapid testing and deployment through incremental upgrades with security-integral testing – this ensures process repeatability and reliability.
  - Produce bills of materials (BOMs) independent of those provided by vendors when possible. Analyze vendor/product BOMs for software, firmware, and hardware when they're available to detect vulnerabilities and backdoors, and to perform risk evaluation from deployment.
  - Implement version control for all OT applications, custom applications, and code. This includes HMI dashboards, PLC programs, and custom automation scripts, among others.
  - Stress test patches, software, and hardware for potential compatibility issues with upstream and downstream systems, including legacy systems.
  - Establish digital supply chain integrity mechanisms to facilitate safe downloading of OT software and firmware updates for critical systems. Often, industries rely on support websites that may not have security features like file hashes or signatures. Proactively coordinate with the vendor (during procurement) to have patch integrity checks in place.

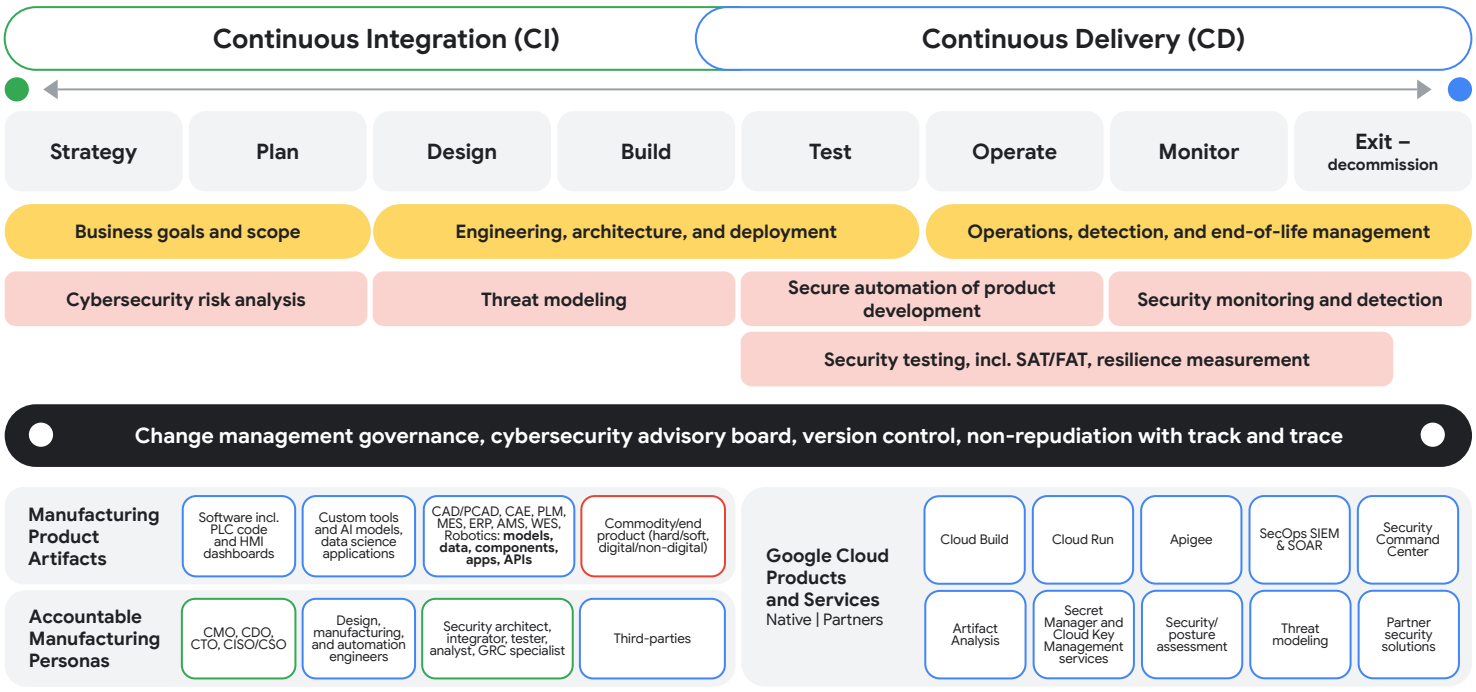

Figure 5. Adoption of augmented CI/CD principles for manufacturing product engineering

3.8. Preventive maintenance and security testing

- ❏ Perform **preventative maintenance and testing** on the OT systems.
  - ❏ Leverage signal-based monitoring (vibration monitoring, thermal monitoring, and so on) with AI to predict system degradation and failure.
  - ❏ Leverage development environments and cloud-based digital twins for more aggressive stress testing, including adoption of chaos engineering-like methods. Perform scheduled preventative maintenance and testing on production systems during non-production hours. Note that direct use of penetration testing and chaos engineering on production-live OT systems may have safety implications, and is therefore not recommended.[18]
- ❏ Establish **safety and security testing**[19] across the entire OT asset and process life cycle.
  - ❏ Have security site acceptance testing (SAT) and factory acceptance testing (FAT) in place. Ensure the following processes are part of security SAT and FAT:
    - Collect static information such as asset information (for example, make, model, version), asset documentation (such as process flow diagrams, or PFDs; piping and instrumentation diagrams, or P&IDs; requirements; and specifications), asset IP addresses, VLAN IDs, and media access control (MAC) addresses.
    - Identify asset connectivity capabilities (serial, Ethernet, Wi-Fi, Bluetooth, and so on). Enable or disable them in compliance with business and engineering requirements.
    - Identify asset owners, automation engineers, and third-party integrators.
    - Identify required ports, protocols, and services. Disable everything unnecessary to the engineering function that meets a business need.
    - Review firewall rules, access control lists (ACLs), and router and switch configurations. Export and save them as baselines.
    - Perform a physical inspection and maintain photographic records of the panels, tags, asset information labels, and so on. For all digital OT assets, capture baseline configurations in machine-readable format.
    - Create backups of all OT configurations, including PLC programs, variable frequency drive (VFD) profiles, HMI dashboards, and similar. Check the list of host processes and services, registries, installed software, OS version, certificates, BIOS, network information, SBOM, and similar network and system information for anomalies. Mitigate all insecure configurations that do not conflict with the engineering process. Implement compensating controls as needed.
    - Use hardening guides such as CIS Benchmarks,[20] STIGs, or even the Top 20 PLC secure coding practices[21] for secure configuration.
    - Use Cloud Storage and Google Cloud's backup and disaster recovery solutions.
  - ❏ Perform periodic red teaming to determine the effectiveness of security controls.
  - ❏ Perform a purple team assessment to determine the effectiveness of SIEM logging and NSM, threat hunting, and other defenses.
  - ❏ Leverage chaos engineering in the development and digital twin environments. Leverage a safer subset of those tests for production environments to ensure personnel safety is not compromised.
  - ❏ Leverage penetration testing where feasible or adapt periodic vulnerability assessments/tests where the exploitation demonstrability is not needed.

---

[18] Mandiant's OT team published a blog post on our OT red team philosophy, including in live OT environments. We ensure safety and operations/production impacts are not affected due to agreed upon rules of engagement and regular involvement of client subject-matter experts (SMEs) during the test.

[19] Refer to the standard IEC 62443 and NIST SP800-82.

[20] Refer to https://www.cisecurity.org/cis-benchmarks.

[21] Refer to https://plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf.

3.9. Supply chain transparency

- ❑ Gain **transparency into the overall supply chain** and dependencies (see Figure 6 for a supply chain process flow reference).
  - ❑ Identify third-party dependencies, including managed service provider (MSP)/managed security service provider (MSSP) and vendor services dependencies. Evaluate the impact of those dependencies, if they were compromised, on your business processes.
  - ❑ Develop and test mitigation strategies. Embed this process during the procurement and contractual engagements.
  - ❑ Know your place and role in the overall supply chain (dependencies and dependents). Ensure necessary security controls are in place to meet expectations/requirements.
  - ❑ Establish security processes across the asset procurement life cycle (for example, third-party risk management and security rating services). Ensure supplier SLAs define vulnerability management, secure product design and engineering, incident response support, and disclosure transparency. Ensure supplier redundancy is in place.
  - ❑ Establish security-in-deployment for on-premises OT systems (see checklists from the previous sections pertaining to hardening and system and network security) and leverage Google Cloud's security-in-deployment guidance for OT SaaS and self-hosted applications.
  - ❑ Ensure the assets are produced in security- and safety-inclusive environments.
  - ❑ Ensure customer, regulatory, and organizational requirements around data security, privacy, personnel safety, and end-to-end security testing are maintained.

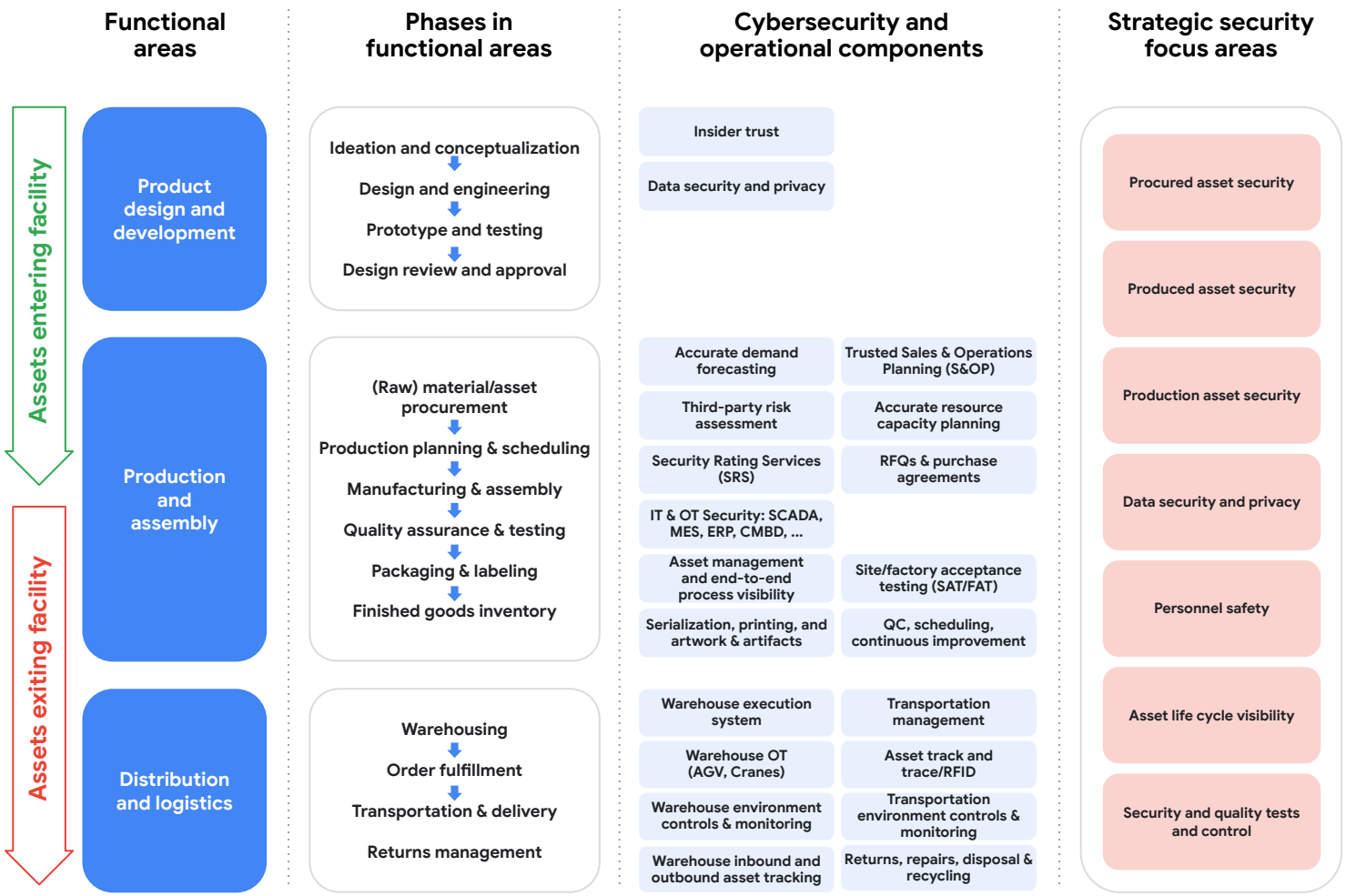

Figure 6. Supply chain management, life cycle, phases, and security focus areas

3.10. Incident response and disaster recovery

- ❏ Establish an incident response and business continuity/disaster recovery program that is relevant for IT and OT.
  - ❏ Establish **incident response and recovery** policies, procedures, standards,[22] and playbooks that are compatible with the OT environments. Conduct periodic testing through table-top exercises, attack simulation tests, and vulnerability assessment.
  - ❏ Ensure that the incident response (IR) and disaster recovery processes are tailored for the OT environments and thoroughly tested.[23] Use Google Cloud's ThreatSpace, table-top exercises, and Google Threat Intelligence to tailor proactive security testing. Leverage Mandiant Incident Response Services to ensure rapid response to cyber incidents across the holistic IT, OT, and cloud environments.
  - ❏ As part of the IR preparation phase, follow the digital forensics and incident response (DFIR) for OT framework by collecting all the tools for ICS/OT, troubleshooting, root-cause analysis, vendor support, and data identification and collection.
  - ❏ Establish a **hard-restart recovery** time to proactively prepare for catastrophic failures where typical backup and restore measures are insufficient[24].
  - ❏ Maintain documentation for OT system configuration, software installations (including HMI dashboards and PLC programs and configurations), and data restoration procedures. Ensure that the detailed documentation does not rely on the system in question for access and that it is kept current.
  - ❏ Implement secure, out-of-band communication and collaboration tools for incident response teams involved in system recovery. These tools should remain operational, independent of the impacted ICS network. Develop detailed recovery procedures with a clear, sequential order of operations to ensure safe and reliable restoration of critical processes.
  - ❏ Perform an analysis of ICS/OT system dependencies, including interdependencies with IT and cloud systems, to identify and eliminate circular dependencies. Use this to inform a prioritized recovery sequence that ensures safe and predictable restoration of critical functions and data flows, minimizing the risk of cascading failures during recovery.
  - ❏ Implement an offline/air-gapped backup strategy for critical ICS/OT systems. These backups should be stored securely, with strict access controls/RBACs, to prevent unauthorized modification or deletion. Validate backup integrity periodically to ensure recoverability.
  - ❏ Conduct periodic testing of recovery procedures by simulating attack scenarios and system failures. Testing should include both "live" disruptive tests in controlled/development environments and ongoing, zero-disruptive tests to validate specific recovery steps in the production environment. Use actual operational tools and processes for testing to ensure realism and prevent reliance on test-specific tools that may become outdated. Use the findings and lessons to improve security processes.

3.11. Google Cloud tools and services for secure OT connectivity

- ❏ Leverage Google Cloud's segmented architecture. Establish projects in accordance with business and engineering needs. Examples include a security folder; an enterprise and business folder; and a manufacturing, automation, and industrial folder. Each of these folders may have their own folders and projects – for example, a security folder may have a security engineering folder, a security operations folder, and so on. Similarly, manufacturing, automation, and industrial folders may have respective projects such as development, validation, and production. Provision compute and storage resources within these projects.
- ❏ Use RBAC to ensure granular access controls are in place. For instance, the security data lake and NSM application within the security operations project may have IT and OT security and inventory data. The security operations engineers may have read and write access to this project and pertinent folders. An automation engineer may only need read access to the NSM asset inventory data. Leverage groups and roles in Google Cloud's IAM to manage access.

---

[22] Refer to "Develop an Incident Response Capability" NIST 800-82.

[23] Refer to "Develop a Recovery and Restoration Capability" NIST 800-82.

[24] From our experience engaging with security leaders while conducting security assessments and incident response activities, we've found that executives often underestimate the time required for system recovery from backups, anticipating days rather than weeks or more, depending on the nature of the attack.

- ❏ For air-gapped, on-premises OT applications that don't have or cannot have cloud connectivity, leverage Google Distributed Cloud (GDC)[25] to host Google Cloud infrastructure, resources, and applications in your own data centers/facilities.[26] Gain cloud-like experience and benefits without over-the-internet cloud connectivity.
- ❏ For OT-to-VPC for data flow, storage, and analytics, leverage Manufacturing Data Engine (MDE), which serves as a secure, encrypted gateway between on-premises and cloud systems. Deploy MCe/gateway in the OT DMZ (or IT-OT DMZ).
  - ❏ Define data directionality (such as data flows between on-premises OT-to-VPC, VPC-to-OT on-premises) based on the organization's policies, risk assessments, regulations, and engineering and business needs.
  - ❏ Define control directionality[27] (such as control flows between on-premises OT-to-VPC, VPC-to-OT on-premises) based on the organization's policies, risk assessments, regulations, and engineering and business needs.
  - ❏ Use Identity Aware Proxy (IAP) for secure access to the MDE configuration platform on Google Cloud.
  - ❏ Route security events to Google Security Operations (SecOps) for alerting on anomalous activity.
  - ❏ Perform key management and certificate management within the (separate) security project handled by the security operations team if the manufacturing team is not expected to handle key and certificate life cycle management.
- ❏ Gain visibility into your networks and perform dynamic/automated asset inventory using a combination of Cloud Asset Inventory (cloud infrastructure) and partner solutions (on-premises IT and OT infrastructure).
- ❏ Perform recurring and periodic security and posture assessments, including but not limited to software and application security and vendor, procurement, and product security.
- ❏ Automate (almost) everything in security (monitoring, detection, alerting, triaging, and so on). Automate what you can in the OT operations without impacting safety, productivity, and reliability, providing a demonstrable tangible business value.
- ❏ Deploy on-premises network monitoring through Google Cloud partner solutions.
- ❏ Leverage modern cloud OT solutions for secure centralization, where needed, using Google Cloud solutions such as MDE and partner solutions.[28]
- ❏ Design, deploy, and test your hybrid network following Google Cloud security playbooks to build secure architectures and enforce cyber-physical resilient systems, incident response and rapid recovery guidance, and compliance guidance and frameworks.
  - ❏ Leverage Audit Manager, compliance manager, and the self-service compliance resource center to obtain necessary artifacts and evidence needed for your internal and external audits.
  - ❏ For a multi-factory setting with business and engineering functions spread out across the world, leverage Sovereign Cloud solutions and Assured Workloads to run compliant workloads that may be country-dependent.

    Note: Google Cloud monitors security frameworks and standards such as the NIST CSF, 800-53, 800-82, 800-171, CMMC, C2M2, IEC 62443, and NERC CIP, among others.

---

[25] There are two Google Cloud technologies under GDC: Google Distributed Cloud air-gapped and Google Distributed Cloud connected. Companies should identify one of them based on their risk assessment and their regulatory and policy requirements.

[26] GDC can run almost all applications that could run on typical on-premises servers. The infrastructure can be configured to send logs to prominent SIEMs. Users can also pull machine learning models (for example, from Model Garden) and run them on-premises within Google Distributed Cloud Hosted or Google Distributed Cloud connected.

[27] Organizations in highly regulated spaces tend to configure unidirectional data flow from on-premises to cloud and deny all OT level push and pull commands from cloud to on-premises. With the emerging efforts like cloud SCADA, such architecture may evolve with controlled bidirectional flows by leveraging additional security measures, such as machine identity, microsegmentation, and zero-trust at OT.

[28] Google Cloud partner solutions can also facilitate secure streaming of edge device data to cloud (for example, IIoT/OT on-field/edge device encrypted unidirectional data streaming to cloud).

- Build a data-driven business and engineering strategy and workflow (see Figure 7) to enforce data connectedness and operational OT data for business and engineering decisions.
  - Use Pub/Sub to ingest real-time OT sensor data for analysis.
  - Use Dataflow to process and transform high volumes of OT data streams for real-time insights.
  - Use BigQuery to analyze historical OT data to identify trends, anomalies, and discovery opportunities to optimize operations.
  - Use Bigtable to store and access large volumes of time-series OT data for long-term analysis.
  - Use Cloud Storage to store and manage OT data lakes, backups, and historical records.
  - Use Firestore to store and synchronize operational settings and configurations for distributed OT systems.
  - Use Spanner to manage critical, globally distributed OT data systems that require high consistency and availability.
  - Use Looker to visualize and analyze OT data, gain operational insights, and create engineering and business dashboards.
  - Use Security with Generative AI to analyze logs and events to detect anomalies and potential threats in the OT network (note that the AI models are integrated into Google SecOps)
  - Use Visual Inspection AI/Vision AI to automate visual inspection of equipment and processes in the OT networks. Improve production quality and efficiency without compromising security.

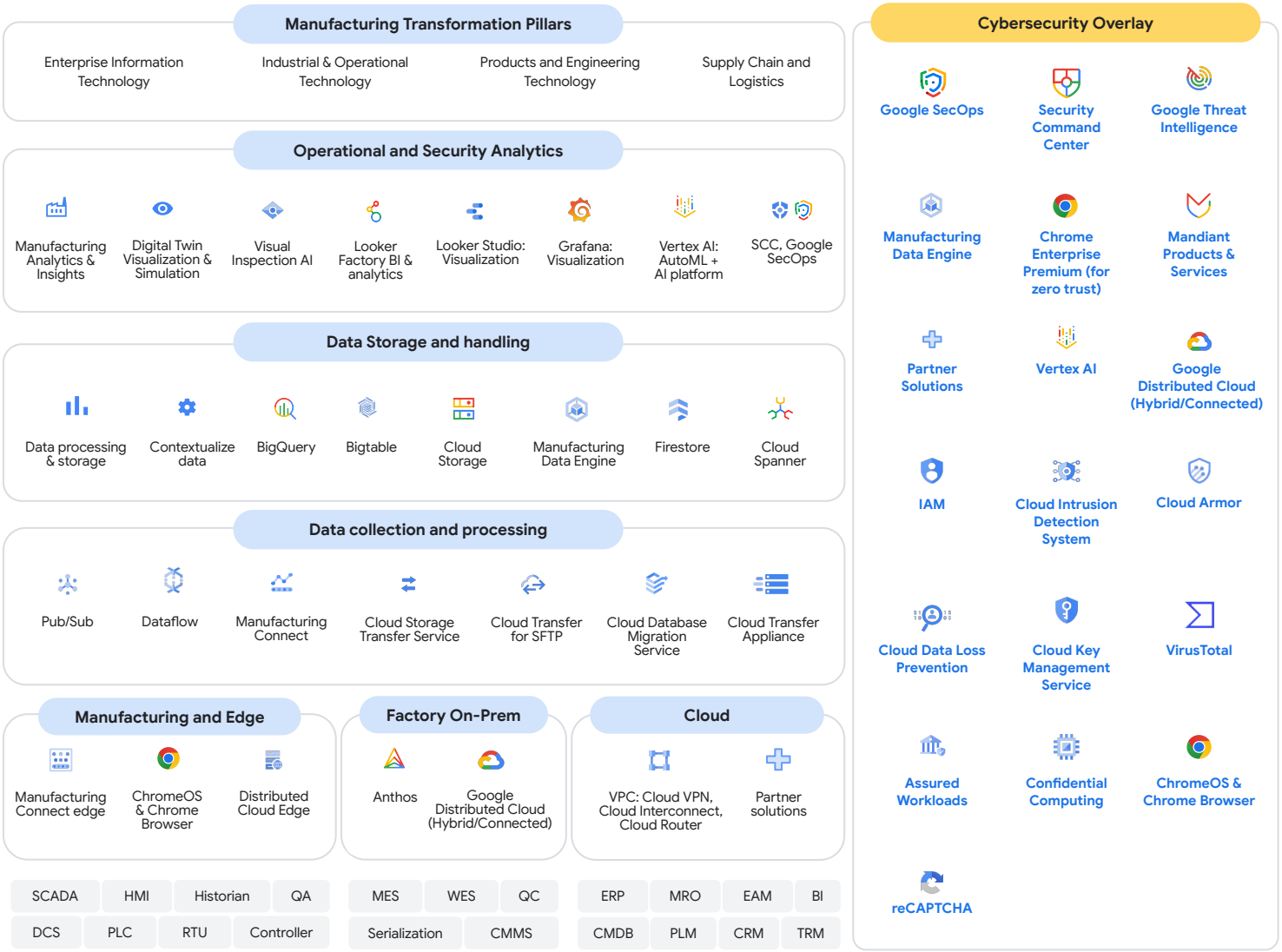

Figure 7. Data engineering and management workflow for OT and hybrid cloud networks

4. Summary

In this report, we recommended a strategic and operational security and resilience checklist for on-premises and hybrid OT networks, stressing security-by-design, security-by-default, and security-in-deployment principles. It is essential to equip security teams with expertise in both OT and cloud security. Key recommendations include:

- Maintaining a current inventory of OT assets and their connections within and across the trust zones
- Establishing hard-restart recovery plans
- Ensuring cyber-physical modularity via segmentation
- Limiting unnecessary OT exposure to the internet

The guidance advocates for manual operations of the most critical systems as a backup option in case of catastrophic failures, a defense-in-depth architecture, reproducible software and hardware processes, regular maintenance and testing, comprehensive incident response and recovery policies, thorough safety and security testing, and transparent supply chain management. Additionally, the report outlines a strategic approach to secure hybrid cloud adoption. Organizations should focus on both on-premises OT security and operationalizing a secure cloud environment for OT. Tactical considerations are provided for security and engineering teams to establish secure on-premises architectures and utilize Google Cloud products and services for comprehensive hybrid network security. See the appendix for a comprehensive mapping between the strategic, operational, and tactical components enumerated in this report.

The strategic and operational security and resilience checklists provided in this report are meant to be actionable for decision-makers. Google Cloud's OCISO, Google Cloud Consulting, and Mandiant Cybersecurity Consulting can assist customers in their discovery journey. What's more, Google Cloud offers a multitude of secure cloud transformation resources.

5. Appendix

Strategic facet	Operational components	Tactical components (cloud and on-premises technologies)	
Cybersecurity leadership and strategy	• Vision and mission • Roadmap and strategy • Short-term and long-term goals • Upskilling and empowerment • Resources and leadership buy-in		
Governance, risk, and compliance	Policies, procedures, and standards	• Blueprints • IaaC modules • Playbooks	• Templates • OCISO advisory services
	Security assessments Risk assessments and management	• Security Command Center • Web Security Scanner • Control Navigator	• Posture assessment • Assured Workloads
	Audits and evidence collections	• Cloud Logging • Cloud Audit Logs	• Audit Manager • Compliance Manager
	Third-party risk management	• Security Command Center • Partner solutions	
	Supply chain security processes	• Software supply chain security • Binary Authorization • Artifact Registry	• Artifact Analysis (software composition analysis [SCA], SBOM) • Software Delivery Shield • Supply-Chain Levels for Software Artifacts (SLSA) framework
	Internal and external training	• ThreatSpace • Google Cloud Skills Boost • Mandiant Academy	• Table-top exercises • Security Command Center's attack path simulation
	Disaster recovery and business continuity plans and orchestration	• Backup and Disaster Recovery (DR) Service	• Cyber Incident Response Service
	Security metrics definition (KPI, KRI, resilience metrics)	• Google SecOps • Cloud Monitoring	• Security Command Center
Cybersecurity engineering and architecture	Identity and access management	• Google Cloud's Identity and Access Management (IAM)	
	Asset management	• Cloud Asset Inventory • Security Command Center	• Partner solutions
	System and network hardening	• Security Command Center • Shielded VMs • Assured Workloads	• Virtual Private Cloud (VPC) • Google Cloud Armor • ChromeOS
	Security tooling deployment	• Terraform	
	Zero-trust network architecture	• Chrome Enterprise Premium	
	Segmentation and perimeter control	• VPC • Cloud Firewall	• Google Cloud Armor
	Container security	• Binary Authorization • Container scanning	• Google Kubernetes Engine (GKE) security
	Data security and privacy	• Cloud Data Loss Prevention (Cloud DLP) • Cloud Key Management Service (Cloud KMS)	• Cloud HSM • Confidential Computing
	Dala loss prevention	• Cloud DLP	
	Cryptography and key management	• Cloud KMS • Cloud HSM	• Cloud External Key Manager
	Security of and security with AI	• Secure AI Framework (SAIF) • Vertex AI • Google SecOps	• Vision AI • SecLM
	OT and IoT security enclaves	• Manufacturing Data Engine (MDE) • Anthos • Google Distributed Cloud connected	• Google Distributed Cloud air-gapped • Mandiant services • Partner solutions
	Security analytics design	• Security Command Center	• Google SecOps
	Product security design and testing	• Security Command Center • Cloud Build	• Software Delivery Shield
	Consequence-driven, cyber-informed engineering	• Security Command Center	• Google SecOps

Appendix (cont.)

Strategic facet	Operational components	Tactical components (cloud and on-premises technologies)
Cybersecurity operations	Log, monitor, and alert Detect and monitor sensor tuning	• Cloud Logging • Cloud Monitoring • Alerting • Security Command Center • OT partner solutions • Google SecOps
	Vulnerability management	• Security Command Center • Web Security Scanner • Container scanning • Google SecOps
	Threat intelligence and modeling Threat hunting and penetration testing Adversarial attack simulation Table-top exercises and red teaming	• Google Threat Intelligence (also powered by Mandiant Threat Intelligence and VirusTotal) • VirusTotal • Google SecOps • Security Command Center • ThreatSpace • Security Command Center's attack path simulation • Mandiant services
	Event and incident analysis and response Digital forensics	• SCC • Google SecOps • Partner solutions
	Malware analysis and reverse engineering	• VirusTotal • Mandiant services • Partner solutions
	Root-cause analysis	• Cloud Logging • Cloud Monitoring • Security Command Center • Google SecOps
	Incident containment	• Security Command Center • Cloud Firewall • Google Cloud Armor
	Incident handling and recovery	• Security Command Center • Backup and Disaster Recovery (DR) Service
	Deception system deployment	• Partner solutions
	Security data analytics	• Google SecOps • BigQuery • Looker • Vertex AI
	SIEM and SOAR monitoring and analysis	• Google SecOps • Cloud Run functions