Cisco Industrial Automation Solution

**Improve business operations by securely digitizing production environments**

The Cisco® Validated Design (CVD) for Industrial Automation is your key to digitizing industrial production environments in order to significantly improve business operation outcomes. It provides network and security design and implementation guidance for production environments, including manufacturing, oil and gas, substation automation, mining and water treatment. The solution supports resilient, secure connectivity to Industrial Automation and Control Systems (IACS) and devices core to the operational environment and the personnel maintaining the environment.

Use this secure networking solution for the following applications:

- Connectivity of IACS devices, including sensors, actuators, and controllers; and assets such as robots, CNC machines, tools, process skids, and RTUs
- Secure production environments thru plant and cell/area zone segmentation, anomaly detection and policy deployment and enforcement
- Provide OT personnel visibility and continuous monitoring of the network and security status of the IACS devices and communication
- Enable remote access to production assets and personnel to improve uptime
- Support plant-wide applications such as manufacturing execution systems, Supervisory Control and Data Acquisition (SCADA), historians, asset management
- Implement relevant network services, including DNS, DHCP, sitewide Precise Time distribution
- Enable IoT applications with Edge Compute such as predictive analytics and maintenance, Digital Twin, and machine learning and optimization

The Cisco Industrial Automation validated solution can help you securely converge IT and OT operations through a partner and Cisco validated approach and architecture.

**Benefits**

- Secured connectivity of industrial automation systems:
  - Improves Operational Equipment Effectiveness (OEE) and asset utilization through increased production availability and asset visibility
  - Reduces risk to the production environment through industry-leading industrial cyber security
  - Reduces product defects through early indication of quality-impacting events or conditions
  - Enables faster deployment and troubleshooting of equipment
  - Drives innovation with production environments ready for edge-intelligent IoT applications

© 2020 Cisco and/or its affiliates. All rights reserved.
At a glance
Cisco public

Drive significant operational improvements with a leading industrial automation solution set
Are your core production and operational process systems disconnected and in un-secured operational silos? Get the assurance you need by using Cisco Industrial Automation’s premier integration of IT expertise with OT requirements and applications. Then you can deploy the technology for connecting, securing, and starting industrial IoT-based improvements.

For additional information, visit www.cisco.com/go/iotcvd.

What’s new in the solution:

- Support for Oil and Gas Process Control and refineries wireless networks integrating the new IW6300 Intrinsically safe Wi-Fi access points backhauling wireless sensor traffic
- Expanded resiliency and security support with Cisco Software-Defined Access ready infrastructure Catalyst IE3200, IE3300, IE3400 and IE3400 Heavy (IP67)
- Integrated Cisco’s Cyber Vision OT focused industrial cybersecurity visibility and monitoring

Confidently deploy networks and security in production environments
The Cisco Industrial Automation validated solution is unique and distinguished in the marketplace, integrating industry-leading IT expertise with OT requirements and applications. Using this solution gives customers, partners, and system implementers the confidence to deploy Cisco’s networking and security technology in any industrial automation setting. This unique solution outlines how to achieve a set of key OT requirements:

- High availability for all key industrial automation systems and services
- IT-preferred security architecture that integrates OT context and is applicable to Industrial applications
- Converged network to support communication from sensor to cloud
- Reliance on open standards to ensure vendor choice and protection from proprietary constraints
- Deploy IoT applications with support for Edge Compute
- Continuous cybersecurity monitoring of IACS devices and communications
- Secure production environments with firewall based Industrial De-Militarized zone and easy-to-deploy, TrustSec-based micro-segmentation for cell/area zones

- Distribute Precise Time across the site to support Motion applications and Schedule of Events data collection
- Real-time, deterministic application support with low network latency and jitter for the most challenging applications, such as motion control
- Deployable in a range of industrial environmental conditions with industrial-grade as well as COTS IT equipment
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s) deployments
- Intent-based manageability and ease of use to facilitate deployment and maintenance, especially by OT personnel with limited IT capabilities or knowledge

Proven to work with industrial vendors, including Rockwell Automation, Schneider Electric, Siemens, Mitsubishi Electric, Emerson, Honeywell, Omron, SEL, and Yokogawa. A broad set of customers from industries such as automotive, high technology, Consumer Packaged Goods (CPG), pharmaceutical, food and beverage, utilities, and oil and gas have utilized the solution.
## Industrial Automation Networking + Security Portfolio

<table>
<thead>
<tr>
<th>Industrial switching</th>
<th>IoT Gateways / Compute</th>
<th>Industrial Wi-Fi</th>
<th>Enterprise Network and Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE 1K, 2K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS</td>
<td>IR807, IR809, IR829, IR1101, IC 3000</td>
<td>AP1552, IW3702, IW6300</td>
<td>Cat 9300/9500, ASA5500, Aironet 1560 APs, 5520/9800 WLCs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA 3000 Cyber Vision</td>
<td>IOx Edge Intelligence</td>
<td>Field Network Director Gateway Management Module Industrial Network Director Control Center</td>
<td>Identity Services Engine, Cisco Prime, Stealthwatch Firepower Management Center</td>
</tr>
</tbody>
</table>

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)