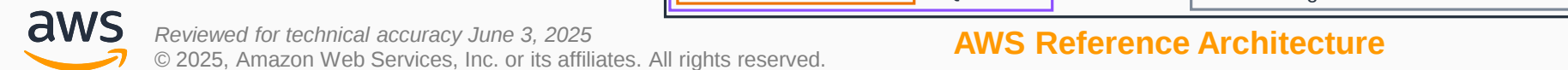


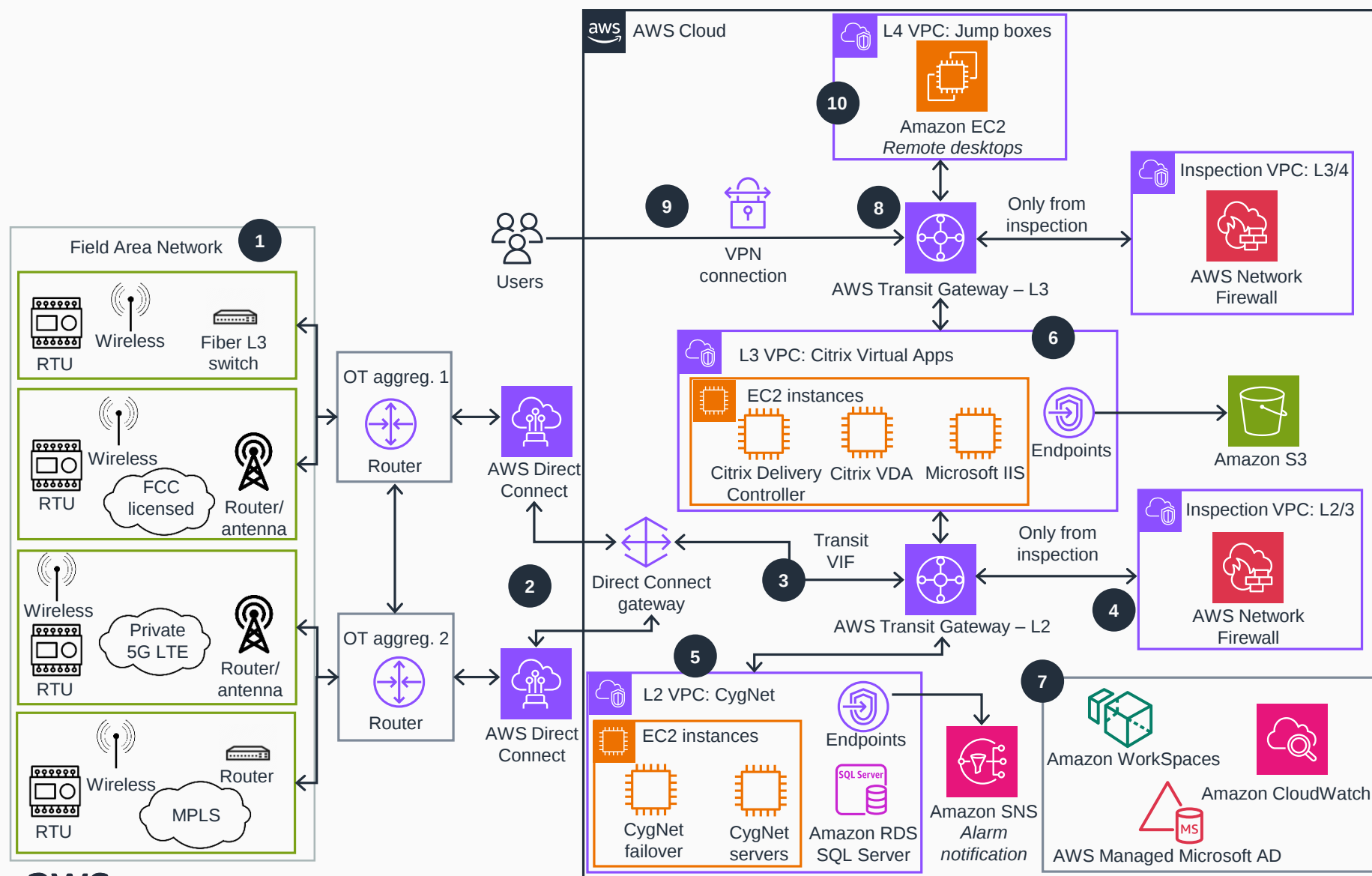
This architecture diagram shows a highly-available, private deployment of Weatherford's CygNet SCADA solution on AWS. The network is segmented to limit data flow between industrial and corporate environments—inserting firewalls and inspection appliances in between—in a design that mimics the Purdue security model. Although this architecture illustrates services at the Region level, all servers are deployed in at least two Availability Zones for high availability. This slide shows Steps 1-5.



5 Purdue Level-2 VPC (for OT) CygNet servers, failover, and database (**Amazon Relational Database Service [Amazon RDS] for SQL Server**) are deployed in a VPC. These are CygNet backend servers for processing. Scale and redundancy options are available for the database and compute nodes. The CygNet deployment will be broken into multiple **Amazon Elastic Compute Cloud (Amazon EC2)** instances based on disk, I/O, CPU, and memory consumption. **Amazon Simple Notification Service (Amazon SNS)** uses endpoints to send alarm notifications.

Guidance for Deploying CygNet SCADA on AWS

This architecture diagram shows a highly-available, private deployment of Weatherford's CygNet SCADA solution on AWS. The network is segmented to limit data flow between industrial and corporate environments—inserting firewalls and inspection appliances in between—in a design that mimics the Purdue security model. Although this architecture illustrates services at the Region level, all servers are deployed in at least two Availability Zones for high availability. This slide shows Steps 6-10.



- 6 A separate VPC exists at Purdue Level-3, serving as an intermediate network, also known as an OT-IT Demilitarized Zone (DMZ). This VPC contains multiple components: a Citrix Delivery Controller (which delivers the CygNet application), a Citrix Virtual Delivery Agent (VDA) for connection management, Microsoft Internet Information Services (IIS) for hosting CygNet's Thin Web Client, and additional Level-3 functions, including a data lake that uses **Amazon Simple Storage Service (Amazon S3)** through endpoints. This traffic is strictly separated by the Level 2/3 Inspection VPC. Scale and redundancy options are available for the database and compute nodes.
- 7 Supporting services include **AWS Managed Microsoft AD**, a fully managed cloud Active Directory Service. This service does not expose authentication traffic to VPCs. Additionally, **Amazon CloudWatch** gives you visibility into your infrastructure. **Amazon Workspaces** is a fully managed virtual desktop infrastructure (VDI) option that connects to servers and virtual apps.
- 8 Purdue Level-3 Transit Gateway is a second **AWS Transit Gateway** that forces separation between Level-3 and Level-4 VPCs. Inspection VPC contains an **AWS Network Firewall** to separate Level-3 from Level-4.
- 9 VPNs can be used to extend the network to users outside of AWS while still enforcing the use of firewalls.
- 10 The L4 VPC can host remote desktops for administrators and IT teams to access the private networks.



Reviewed for technical accuracy June 3, 2025

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture