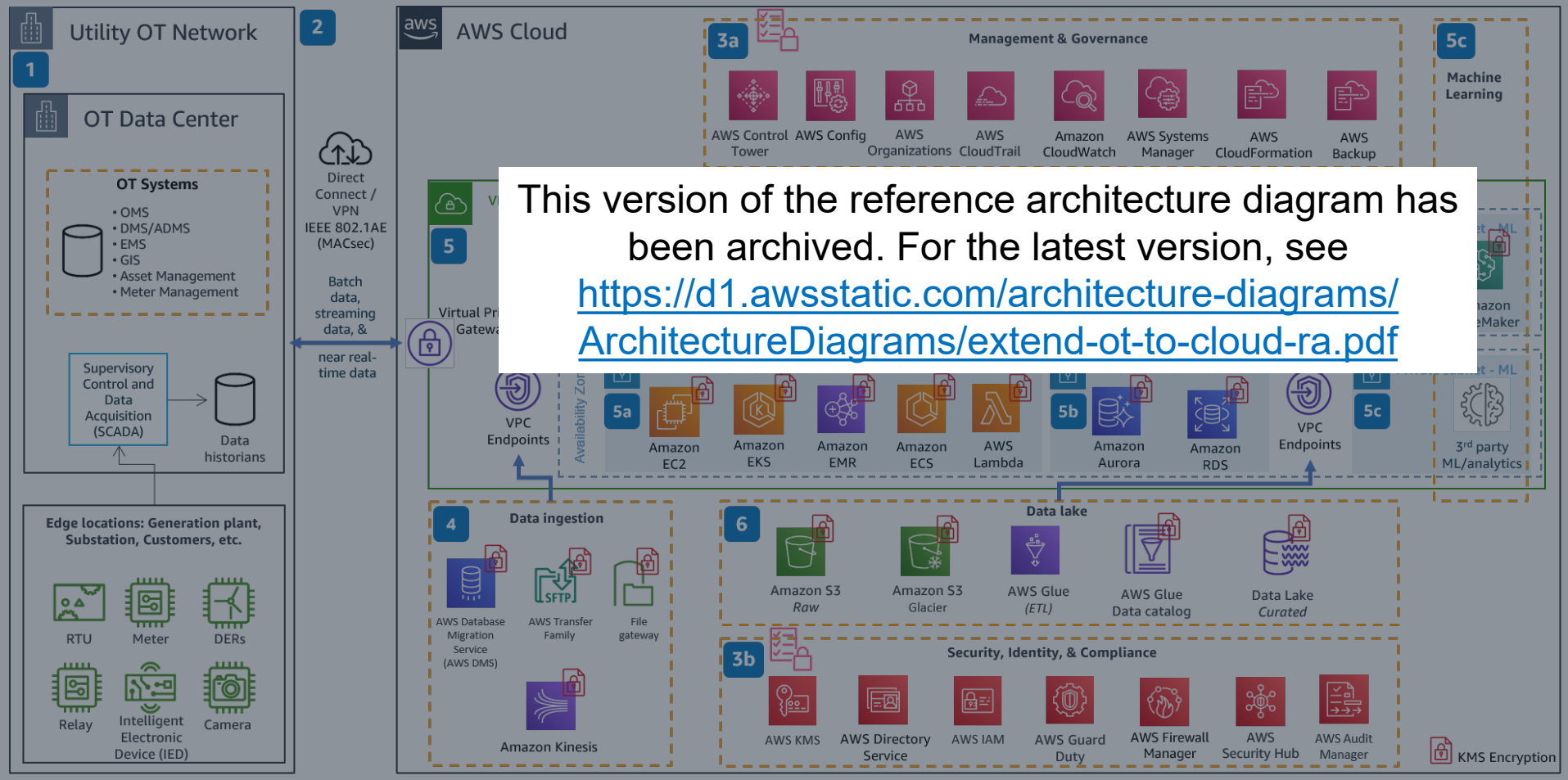
BES Cyber System Information (BCSI) on AWS

Build a secure extension of an Operations Technology (OT) data center into the cloud for ingestion of data from Bulk Electric System (BES) assets using the inherent security and isolation of an AWS VPC and other AWS services. Use AWS compute, analytics and AI/ML services, operating on a data lake, to conduct contingency analysis and planning, incident response, and advanced analytics. Show North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance for BES Cyber System Information (BCSI) using AWS services as noted in the steps at the right of this page. And in-depth exploration of this reference architecture can also be found here: https://aws.amazon.com/blogs/industries/extend-your-ot-network-to-the-cloud/



This version of the reference architecture diagram has been archived. For the latest version, see https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/extend-ot-to-cloud-ra.pdf

1 A utility company's OT network can include generation facilities, remote locations (substations), data centers, and customers.

2 Secure and highly reliable networking to AWS over VPN. For guaranteed bandwidth use **AWS Direct Connect** with IEEE 802.1AE (MACSec) encryption. (relates to CIP 11).

3a Manage and govern cloud resources at scale from a centralized location using services such as **AWS Control Tower**, **AWS Audit Manager**, and **AWS Systems Manager**. Log all account activity with **AWS CloudTrail**. Use **AWS Config** to assess all your cloud configurations and any changes (relates to CIP 11).

3b Control access with **AWS Identity and Access Management (IAM)** and **AWS Directory Service**. Monitor network traffic for malicious activity using **AWS GuardDuty**. Encrypt and protect data using **AWS Key Management Service (AWS KMS)**. (relates to CIP 4 and CIP 11).

4 Data ingest using services such **AWS Data Migration Service**, **AWS File Gateway**, **AWS Transfer Family**, or **Amazon Kinesis**. Data flows to **Amazon Virtual Private Cloud (Amazon VPC)** via VPC Endpoints. (relates to CIP 11).

5 Use **Amazon Virtual Private Cloud (Amazon VPC)** with its inherent security and isolation for hosting compute and database resources. (relates to CIP 11).

5a Do analysis and simulations for compute options including **Amazon EC2**, **AWS Lambda**, **Amazon EKS**, **ECS**, and **AWS Fargate** for containerized applications, and **Amazon EMR**, all using **AWS Key Management Service (KMS)** for encryption. (relates to CIP 11).

5b Store data securely in highly available RDBMS' using **AWS Relational Database Service (RDS)** and **Amazon Aurora**. Encrypt data at rest with **AWS KMS**. (relates to CIP 11).

5c Use AI/ML services such as **Amazon SageMaker** for analysis and assessment of BCSI.

6 Create OT data lake on **Amazon S3**. **AWS Glue** performs ETL and builds the data catalog. Archive data in **Amazon S3 Glacier.** Encrypt data using **KMS**. Restrict data access to the VPC using VPC endpoints. (relates to CIP 11).

Reviewed for technical accuracy May 18, 2022

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture