GridOps Management Suite 3.10

Enterprise Integration Platform

Functional Specification

Document Version: 1.0

Updated: June, 2024

Table of Contents

Table of Figures

1. REFERENCES

#	Title	Description
1.	Security Data Classification	The document provides a brief overview on data security requirements as special attention is needed when developing EcoStruxure ADMS or managing data generated by customer's EcoStruxure ADMS solutions. The content of the document differs based on the software solution. The document is located within the Security Documentation for individual offers.
2.	EcoStruxure GridOps Management Suite 3.10 Secure Operations Guideline	The document describes different practices such as expected staff screening procedures, protection of user and service accounts, valuable assets, and operational resilience of the EcoStruxure GridOps Management Suite 3.10.
3.	IEC 61970–301	Common information model (CIM) base.
4.	IEC 61970–403	Common information model (CIM) base.
5.	IEC 61970–501	Generic data access.
6.	IEC 61970–552	Common information model resource description framework (CIM RDF) Schema.
7.	IEC 61968–1	CIM XML Model Exchange Format.
8.	IEC 61968–1–1	Interface architecture and general requirements.
9.	IEC 61968–1–2	Enterprise Service Bus Implementation Profile.
10.	IEC 61968–11	Naming and Design Rules for Web Services.
11.	IEC 61968–13	Common Information Model (CIM) Extensions for Distribution.
12.	IEC 61968–100	Common Information Model (CIM) RDF Model exchange format for distribution.
13.	IEC 62325	Implementation profiles.
14.	IEC 61968–5	Standards related to energy market models & communications.
15.	IEC 61968–9	Interfaces for Distributed Energy Optimization [DER].
16.	EcoStruxure GridOps Management Suite 3.10 Advanced Metering Infrastructure Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with the third-party AMI HES, following the IEC61968-100 and IEC61968-9 standards.

#	Title	Description
17.	EcoStruxure GridOps Management Suite 3.10 Automatic Vehicle Location Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with various automatic vehicle location systems.
18.	EcoStruxure GridOps Management Suite 3.10 Customer Relationship Management Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with various customer service management systems.
19.	EcoStruxure GridOps Management Suite 3.10 DERMS Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with the third-party DER management system, following the IEC61968-100 and IEC61968-5 standards.
20.	EcoStruxure GridOps Management Suite 3.10 Email and SMS Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for forwarding the notification messages from the EcoStruxure GridOps to the end users.
21.	EcoStruxure GridOps Management Suite 3.10 File Claim Check Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for importing the files in the EcoStruxure GridOps. It follows the Claim Check integration pattern.
22.	EcoStruxure GridOps Management Suite 3.10 File Monitoring Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for importing the files in the EcoStruxure GridOps by monitoring the predefined shared location.
23.	EcoStruxure GridOps Management Suite 3.10 File Uploading Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for sending various data contained in a file from the EcoStruxure GridOps to the external systems via the predefined shared location.
24.	EcoStruxure GridOps Management Suite 3.10 Internal External Notifications Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for sending the outage-related event notifications to the end users.
25.	EcoStruxure ADMS 3.10 Major Event Mitigation Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed for importing the major natural event risk factors for all geographical areas from the third-party weather providers or other risk management systems. The content of the document applies only to the EcoStruxure ADMS solution.

#	Title	Description
26.	EcoStruxure GridOps Management Suite 3.10 Network Import Notification Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to provide the extract and changeset state transition and equipment state transition notifications to the GIS system.
27.	EcoStruxure GridOps Management Suite 3.10 Outage Management Notification Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to provide all relevant information about the changes in the EcoStruxure GridOps incident model to the external systems of interest in near real-time.
28.	EcoStruxure GridOps Management Suite 3.10 Outage Reporting Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with various outage portals, IVR, third-party analytic services, etc.
29.	EcoStruxure GridOps Management Suite 3.10 Redlining Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with any GIS system which supports the redlining concept.
30.	EcoStruxure GridOps Management Suite 3.10 Seamless Site Switch Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with the Network Load Balancing application.
31.	EcoStruxure GridOps Management Suite 3.10 Site Note Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to provide the site note synchronization between the utility's CIS and the EcoStruxure GridOps systems.
32.	EcoStruxure GridOps Management Suite 3.10 Switching Management Notification Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to send all notifications related to the planned work to the external systems of interest.
33.	EcoStruxure GridOps Management Suite 3.10 Switching Management Reporting Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with various work order management systems.
34.	EcoStruxure GridOps Management Suite 3.10 Weather Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with the third-party weather providers.
35.	EcoStruxure GridOps Management Suite 3.10 Workforce Management Interface - Functional Specification	The document describes an out-of-the-box integration adapter designed to be integrated with various workforce management systems.

2. ASSUMPTIONS

- SE is not responsible for the requirement implementation related to the external system.
- SE is not responsible for creation and maintenance of certificates and public-private key pairs.
- All message payloads are defined according to the CIM standards (IEC61970 CIM16v33, IEC61968 CIM11v13, IEC62325 CIM01v07).
- All timestamps will be in accordance with the ISO 8601 standard. The ISO 8601 standard is used to define the representations of time values that are conveyed through interfaces. This avoids issues related to time zones and daylight savings time changes. Timestamps in messages generated by systems can have representation in the UTC (Zulu) time (*"2007-04-05T14:30Z"*) or in the local time with time zone offset (*"2007-04-05T12:30-02:00"*). Milliseconds can also be specified.
- Different integration triggers, data formats and enterprise integration patterns (file transfer, messaging, shared database) can be supported and those approaches require additional, custom development on the SE side.

3. INTRODUCTION

EcoStruxure GridOps Management Suite is a family of solutions designed to help electric utilities in the operations and management of their grid. It is offered as EcoStruxure ADMS, EcoStruxure Grid Operation, EcoStruxure DERMS or EcoStruxure Energy Transmission Operation solutions, which share the same technology platform.

NOTE: The functionality described in this document applies to all solutions.

NOTE: Most images presented in this document are related to the EcoStruxure ADMS solution and should be used as an example. The images for other solutions may differ slightly.

Implementation of EcoStruxure GridOps brings large benefits to the utility. These benefits are also visible in seamless, standard-based integrations of EcoStruxure GridOps with other utility systems providing the firm ground for information-based business process optimizations, resulting in improved safety, security, and ultimately, cost savings.

EcoStruxure GridOps is integrated starting from the legacy systems, all the way through the integrations with the new systems implemented after the EcoStruxure GridOps productization. Driven by the business processes' need and basic requirements for interoperability, all integrations between EcoStruxure GridOps and external (legacy) systems are implemented through enterprise systems integration platform. The integration platform is constructed from the set of specific integration adapters. Those adapters are developed to expose models and business logic of EcoStruxure GridOps. The described approach makes it easier to expose broad EcoStruxure GridOps functionality through external IEC 61968 (CIM) compliant interfaces, in order to be utilized within enterprise architecture.

EcoStruxure GridOps enterprise systems integration platform delivers following benefits:

- Provides secure and reliable data exchange through interoperable technologies in near real-time
- Supports standard utility's business processes with granularity
- Guarantees industry quality through auto-testing framework
- Simplifies extensions with project specific needs:
  - Customization-ready architecture
  - Reduced risks and development costs
- Ensures additional benefits through CIM standards utilization:
  - Certified as Compliant with IEC 61968-100:2013 Implementation Profiles
  - Market Leader in CIM Compliance
  - Ready for rapid integration of future systems
  - Reduced data modeling and schema design efforts
  - Analytics-ready by using CIM-based semantics
  - Reduced maintenance costs.

4. ENTERPRISE INTEGRATION PLATFORM COMPOSITION

EcoStruxure GridOps is structured as a set of independent services, where each service hosts its internal model and implements the business logic on that model. Services never expose the model and business logic to the external use, and for this reason, the integration adapters are used.

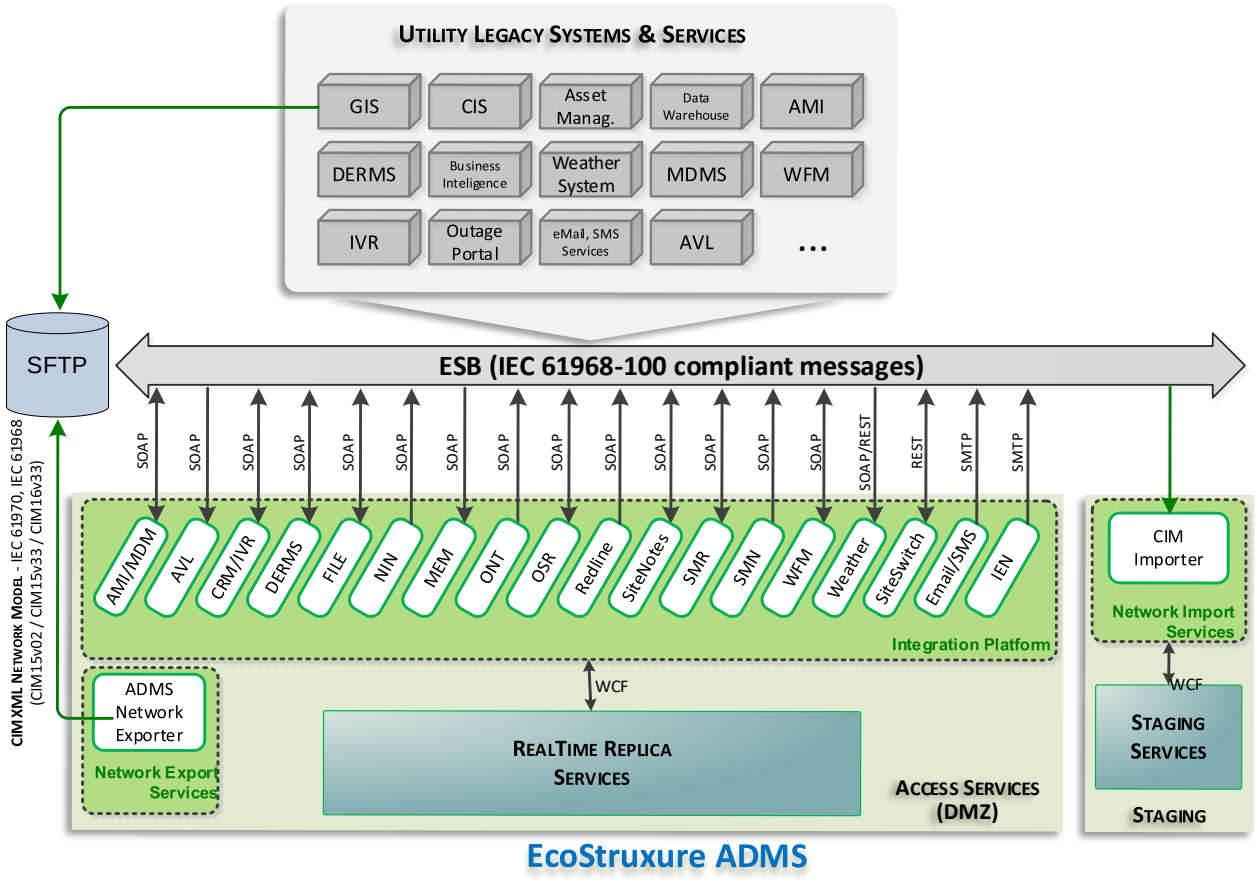

Figure 4.1 – EcoStruxure GridOps Enterprise Integration Platform

Based on the vast experience in integrating EcoStruxure GridOps with various external utility systems all integrations (interfaces) are implemented under the following guidelines:

- A canonical model (CIM) is exposed and exchanged via selected middleware.
- All SOAP web services are defined according to the IEC 61968–100 standard.
- All SOAP integration messages exchanged between external (legacy) systems and EcoStruxure GridOps are defined and named according to the IEC 61968–100 standard.
- Depending on the integration capabilities of external (legacy) systems and available middleware solutions, other messaging integration patterns (JMS, MSMQ, AMQP, MQ, etc.) can be supported additionally via interface extensions.

The following list defines specific benefits for each integration adapter exposed within enterprise integration platform:

- Advanced Metering Infrastructure (AMI):

  - Faster incident locations identification
  - Prediction accuracy increase
  - Increased efficiency using outage validation
  - Increase situational awareness
- Automated Vehicle Location (AVL):
  - Seamless, real-time data update
  - Increased situational awareness
  - Faster crew dispatching
  - Increased customer satisfaction due to faster incident dispatch and resolution
- Customer Relationship Management (CRM/IVR):
  - Faster incident locations identification
  - Prediction accuracy increase
  - Smooth upgrade with minimal risk and cost
  - Scalable implementation
- Distributed Energy Resource Management System Client Interface (DERMS):
  - Broad range of functionality that supports reporting, notification, and business intelligence use cases:
    - Periodic querying of DER group statuses and forecasts
    - Processing of proactive DER group status and forecasts updates
    - Executing DER group dispatches
- Email/SMS:
  - Increased internal transparency
  - Improved collaborative communication
- File Download:
  - Reduction of the manual effort
  - Model management automation
  - Simple (re)configuration
- File Upload:
  - Increase transparency by supplying information to customers via SMS, mails and social media on planned outages
  - Simple (re)configuration
- Internal External Notifications (IEN):
  - Prompt, proactive outage related event notifications
  - Simple publish-subscribe model
  - Customizable e-mail/SMS notification templates
- Major Event Mitigation (MEM):
  - Offers increased situational awareness by importing major natural event risk factors for geographical areas
- Network Import Notifications (NIN):
  - Automatic error propagation to the GIS
  - Can lead to implementation of automatic correction processes within GIS
  - Reduces the potential communication gap
  - Generic error reports readable by machine/human
  - Simple (re)configuration - does not require down time

- Enable additional notifications
- Outage Notification (ONT):
  - Near real-time incident/trouble call/hazard publishing
  - Proactive customers notification
  - Improved customer satisfaction through increased transparency
- Outage Status and Reporting (OSR):
  - Broad range of functionality that supports reporting, notification, and business intelligence use cases:
    - Generic incident problem processing
    - Advanced incident filtering and retrieval
    - Comprehensive incident handling
    - Affected customers retrieval
- Redlining (RLN):
  - Automatic GIS model update request propagation
  - Can lead to implementation of automatic correction processes within GIS
  - Reduces the potential communication gap
  - Increased collaborative awareness and communication between utility's departments
- Site Notes Integration (SNI):
  - Increased situational and operational awareness through additional customers' details
  - Reduced data maintenance due to automatic alignment
- Seamless Site Switch (SSS):
  - Integration interface health monitoring
  - Network load balancing support
- Switching Management and Reporting (SMR):
  - Broad range of functionality that supports reporting, notification, and business intelligence use cases:
    - Generic switching management entities processing
    - Advanced switching management entities filtering
- Switching Management Notification (SMN):
  - Increase transparency by supplying information to employees/customers via SMS, mails, and social media on planned outages
- Weather Data Integration (WDI):
  - Actual weather data update for one or all weather regions
  - Forecast weather data update for one or all weather regions
- Workforce Management (WFM):
  - Simplified workforce data import and maintenance
  - Generic crew assignment update
  - Support for single and batch assignments status updates

5. INTERFACE LIST

The following is a list of all available web services/web service clients exposed through dedicated integration adapters that can be used in various web service orchestrations and compositions in order to accomplish the most challenging business processes:

- **Advanced Metering Infrastructure (AMI)**
  - *GetMeterReadingsService* – used for on demand obtaining of the meter status, voltage, current, active and reactive power. Since asynchronous communication is used between the EcoStruxure GridOps and AMI Head End (or MDMS), this interface is used only for sending requests, while *ReceiveMeterReadingsService* is used as a callback service, for receiving asynchronous responses:
    - *GetMeterReadings* operation
  - *ReceiveEndDeviceEventsService* – used for receiving the power down, power up, undervoltage, overvoltage and return to normal meter events:
    - *CreatedEndDeviceEvents* operation
  - *ReceiveMeterReadingsService* – used for receiving the unsolicited meter readings and asynchronous responses for on demand reads (status, voltage, current, active and reactive power):
    - *CreatedMeterReadings* operation
  - *SendConfigurationEventsService* – used to enable/disable sending of the end device events from the AMI HES (or MDMS) to EcoStruxure GridOps:
    - *CreatedConfigurationEvents* operation
- **Automated Vehicle Location (AVL)**
  - *ReceiveVehicleCoordinatesService* – used for updating vehicle coordinates:
    - *ChangedVehiclesCoordinates* operation
- **Customer Relationship Management (CRM/IVR)**
  - *ReceiveTroubleTicketsService* – used for creating and updating trouble tickets:
    - *CreatedTroubleTickets* operation
    - *ChangedTroubleTickets* operation
  - *GetTroubleTicketsService* – used for pulling active and archived trouble tickets:
    - *GetTroubleTickets* operation
  - *GetCallBacksService* – used for pulling active callbacks:
    - *GetCallBacks* operation
  - *ReceiveCallBacksResultsService* – used for receiving callback results:
    - *CreatedCallBacksResults* operation
  - *SendCallBacksClient* – used for sending callbacks to the external system:
    - *SendCallBacks* operation
- **DERMS**
  - *QueryDERGroupStatuses* service:
    - *QueryDERGroupStatuses* operation – Periodically queries information about DER group statuses from external DERMS and updates status information.
  - *QueryDERGroupForecasts* service:

        - *QueryDERGroupForecasts* operation – Periodically queries information about DER group forecasts schedule for the preconfigured time period that follows and stores the information.
    - *ExecuteDERGroupDispatches* service:
        - *CreateDERGroupDispatches* operation – Notifies the external DERMS upon the creation of a new DER group dispatch.
    - *ReceiveDERGroupStatuses* service:
        - *ChangedDERGroupStatuses* operation – External DERMS proactively sends information about DER group statuses modifications.
    - *ReceiveDERGroupForecasts* service:
        - *CreatedDERGroupForecasts* operation – External DERMS proactively sends information upon the creation of a new DER group forecast schedule.
- **Email/SMS**
    - *SendEmailNotification* service:
        - *SendEmail* operation – Used for sending an email notification to predefined set of recipients obtained from the address book or manually entered.
    - *SendSMSNotification* service:
        - *SendSMS* operation – Used for sending SMS notification to predefined set of recipients.
- **File Download**
    - *ReceiveFileNotificationService* – used for receiving file notifications:
        - *CreatedFileNotification* operation
- **File Upload**
    - *SendFileNotificationService* – used for sending file notifications:
        - *CreatedFileNotification* operation
- **Internal/External Notifications (IEN)**
    - *SendNotification* – Sending email or SMS notification messages based on predefined notification subscriptions. Subscriptions are maintained via dedicated user interface incorporated in the DMD application:
        - Send Email notification
        - Send SMS notification
- **Major Event Mitigation**
    - *ReceiveGeographicalAreaIndexService* – web service hosted on EcoStruxure GridOps side and used for receiving area risk index values for Geographical Area from external system:
        - *ChangedGeographicalAreaIndex* operation
- **Network Import Notifications (NIN)**
    - *SendNetworkImportNotificationsService* – used for sending changesets' state transition notifications and uploading import reports to predefined shared location:
        - *CreatedNetworkImportNotifications* operation
        - *CreatedImportReports* operation
    - *SendEquipmentStatesService* – used for sending information about network elements whose service state has transitioned to a new service state:
        - *ChangedEquipmentStates* operation
- **Outage Management Notification (OMN)**
    - *SendIncidents* – used for sending incident related data to corresponding external web service:

        - *CreatedIncidents* operation
        - *ChangedIncidents* operation
        - *DeletedIncidents* operation
    - *SendIncidentUsagePoints* – used for sending incident usage points to corresponding external web service:
        - *ChangedIncidentUsagePoints* operation
    - *SendIncidentTroubleTickets* – used for sending incident trouble tickets to corresponding external web service:
        - *ChangedIncidentTroubleTickets* operation
    - Integrity update – used for systems alignment. Uses existing service clients for invoking following external web service operations:
        - *ChangedIncidents* operation
        - *ChangedIncidentUsagePoints* operation
        - *ChangedIncidentTroubleTickets* operation
- **Outage Status and Reporting (OSR)**
    - *ReceiveIncidentHazardsService* – used for creating and updating incident hazards:
        - *CreatedIncidentHazards* operation
        - *ChangedIncidentHazards* operation
    - *GetIncidentHazardsService* – used for pulling active and archived incident hazards:
        - *GetIncidentHazards* operation
    - *ReceiveIncidentsService* – used for updating incidents:
        - *ChangedIncidents* operation
    - *GetIncidentsService* – used for pulling active and archived incidents:
        - *GetIncidents* operation
    - *GetIncidentUsagePointsService* – used for pulling active (affected/unrestored) and archived usage points by an incident.
- **Redlining (RLN)**
    - *SendRedlinesService* – used for sending Redline notes to the GIS system:
        - *CreatedRedlines* operation
        - *ChangedRedlines* operation
        - *DeletedRedlines* operation
- **Seamless Site Switch (SSS)**
    - *IsActive* service operation – Used for querying information about the currently active site.
- **Site Notes Integration (SNI)**
    - *ReceiveUsagePointSiteNotesService* - used for dynamic update of Customer database from CIS:
        - *ChangedUsagePointSiteNotes* operation
    - *ExecuteSiteNotesService* – used for dynamic update of CIS database:
        - *CreateSiteNotes* operation
- **Switching Management Notification (SMN)**
    - *SendWorks* – used for sending work requests related data to corresponding external web service:
        - *CreatedWorks* operation
        - *ChangedWorks* operation

        - *DeletedWorks* operation
    - *SendSwitchingPlans* – used for sending switching plans data to corresponding external web service:
        - *CreatedSwitchingPlans* operation
        - *ChangedSwitchingPlans* operation
        - *DeletedSwitchingPlans* opertion
    - *SendSwitchingSteps* – used for sending switching steps data to corresponding external web service:
        - *CreatedSwitchingSteps* operation
        - *ChangedSwitchingSteps* operation
        - *DeletedSwitchingSteps* operation
- **Switching Management Reporting (SMR)**
    - *ReceiveWorksService* – used for creating and updating work requests:
        - *CreatedWorks* operation
        - *ChangedWorks* operation
    - *ReceiveSwitchingPlansService* – used for updating switching plans:
        - *ChangedSwitchingPlans* operation
    - *ReceiveSwitchingStepsService* – used for updating switching steps:
        - *ChangedSwitchingSteps* operation
    - *GetWorksService* – used for pulling active work requests:
        - *GetWorks* operation
    - *GetSwitchingPlansService* – used for pulling active switching plans:
        - *GetSwitchingPlans* operation
- **Weather Data Integration (WDI)**
    - *ChangeActualWeatherDataService:*
        - SOAP:
            - *ChangedActualWeatherData*
        - REST:
            - POST */WeatherRegions/UpdateActual*
            - POST */WeatherRegions/{id}/UpdateActual*
    - *ChangedForecastWeatherDataService*
        - SOAP:
            - *ChangedForecastWeatherData*
        - REST:
            - POST */WeatherRegions/UpdateForecast*
            - POST */WeatherRegions/{id}/UpdateForecast*
- **Workforce Management (WFM)**
    - *ReceiveCrewModelService* – used for aligning crew data with WFM system data:
        - *CreatedCrewModel* operation
    - *ReceiveCrewAssignmentsService* – used for crew assignment management:
        - *CreatedCrewAssignments* operation – initial creation of the crew assignment
        - *ChangedCrewAssignments* operation – two modes of execution:
            - Incremental mode: update of the existing crew assignment. Used when external system sends the changes of individual crew assignments only.

- Bulk mode: generation of delta (incremental crew assignment model update). Used when external system sends the snapshot of all assignments per crew, when one of the crew assignments changes.

- *DeletedCrewAssignments* operation – deletion of the crew assignment.

- *ReceiveCrewsService* – used for updating crew data (availability and connection status):
  - *ChangedCrews* operation
- *ReceiveVehiclesService* – used for updating vehicle data:
  - *ChangedVehicles* operation

More details about each web service/web service client is given within the appropriate functional specification.

6. ARCHITECTURE

6.1. Integration Adapter Architecture

EcoStruxure GridOps enterprise systems integration platform is composed of product integration adapters, importers, and exporters. Components are designed in accordance with the latest IEC standards – series of IEC 61970 and IEC 61968. Integration adapters are developed in microservice-like architecture. Each integration adapter exposes a set of web services exchanging standard-based messages ensuring interoperability readiness. Application of WS-Security specification on top of the enterprise integration patterns (request/reply, publish/subscribe, file transfer, etc.) enables secure and reliable data exchange. Well-defined and up-to-date functional specifications describe the architecture, scenarios (use cases), validation rules, message mappings, error handling, data flows, auditing, etc. An important benefit of product integration adapters is the readiness to support the most challenging utility business processes through the usage of web service composition and orchestration. Maximum quality is ensured through every product increment by the execution of continuous automatic test scenarios. Test scenarios are run daily on a dedicated enterprise test system. By maintaining backward compatibility within the product integration adapters, SE's clients already experienced smoother transition and upgrade to a newer version of EcoStruxure GridOps.

EcoStruxure GridOps integration adapters are implemented in the client-server distributed architectural style by using the multitier architecture pattern. The multitier approach is the most accepted solution to the enterprise applications which requires scalability, modularity, and easy maintenance.

The integration adapters share the common architecture and design while the business-specific logic is implemented in compliance with the specific integration interface for which the adapter is intended. Each interface implements diverse types of use cases to satisfy all the requirements.

All integration interfaces are implemented by using one of the four main integration styles (and the appropriate integration pattern):

- File Transfer (FT) – each application produces the files of the shared data for the others to consume and consumes the files which the others produce.
- Shared Database (SD) – the applications store the data to be shared in a common database.
- Remote Procedure Invocation (RPI) – each application exposes some of its procedures so that they can be remotely invoked, making those applications perform a particular behavior and exchange the data.
- Messaging (MES) – each application connects to a common messaging system, exchanges the data, and invokes the behavior by using the messages.

Depending of the style, the adapters implement one of the integration patterns to facilitate the information exchange.

6.2. Development Platform

Development platform of integration adapters is provided in the following table:

Table 6.1 – Development platform

Development Platform	
Operating system	Microsoft Windows
Software framework	.NET
Programming languages	C#
Hosted under service	OASyS DMS Integration Service (Windows service)
Hosted as	Separate process

6.3. Views

6.3.1. Logical View

The integration adapter is an application which is used to adapt the data to the EcoStruxure GridOps needs from the external systems and vice versa. For this reason, it represents the mandatory central point in the information exchange between the external and EcoStruxure GridOps system (Figure 6.1).

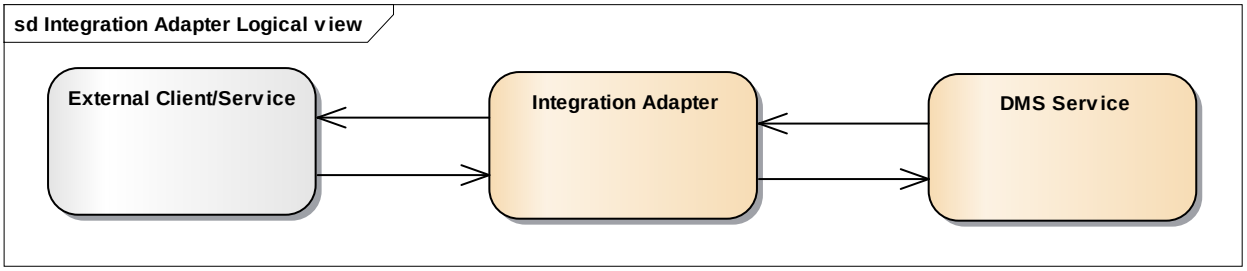

Figure 6.1 – The logical view of the integration adapter

6.3.2. Component View

The multitier architecture contains the following layers:

- External layer
- Integration communication layer
- Integration business layer
- Internal service layer

The external layer is an external application which can have a client or server role, depending on the integration. It is responsible for the data management within the external system. This layer is in the direct interaction with the integration communication layer.

The integration communication layer is the first part of the integration adapter, which is used for the communication with the external application. The communication adapter component of the integration adapter represents this layer. Its purpose is to transfer the data in a specific way from/to the external system to/from the integration business layer.

The integration business layer is the second part of the integration adapter. The business adapter component of the integration adapter represents this layer. It is used for the syntax data validation, transformation, orchestration and interaction with the internal service layer.

Similarly, to the external layer, the internal service layer is responsible for the data management of the EcoStruxure GridOps. It encapsulates the rest of the EcoStruxure GridOps system.

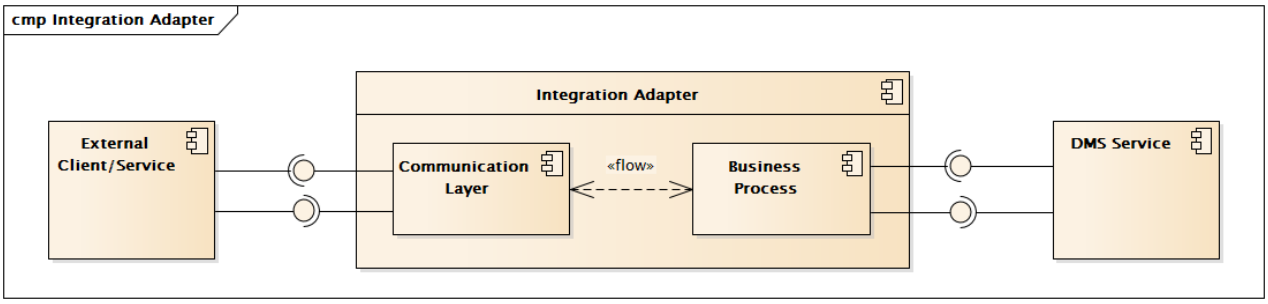

Figure 6.2 – The component view of the integration adapter

6.3.3. Deployment View

The adapters are the self-hosted services deployed into the OASyS infrastructure in the demilitarized zone (DMZ).

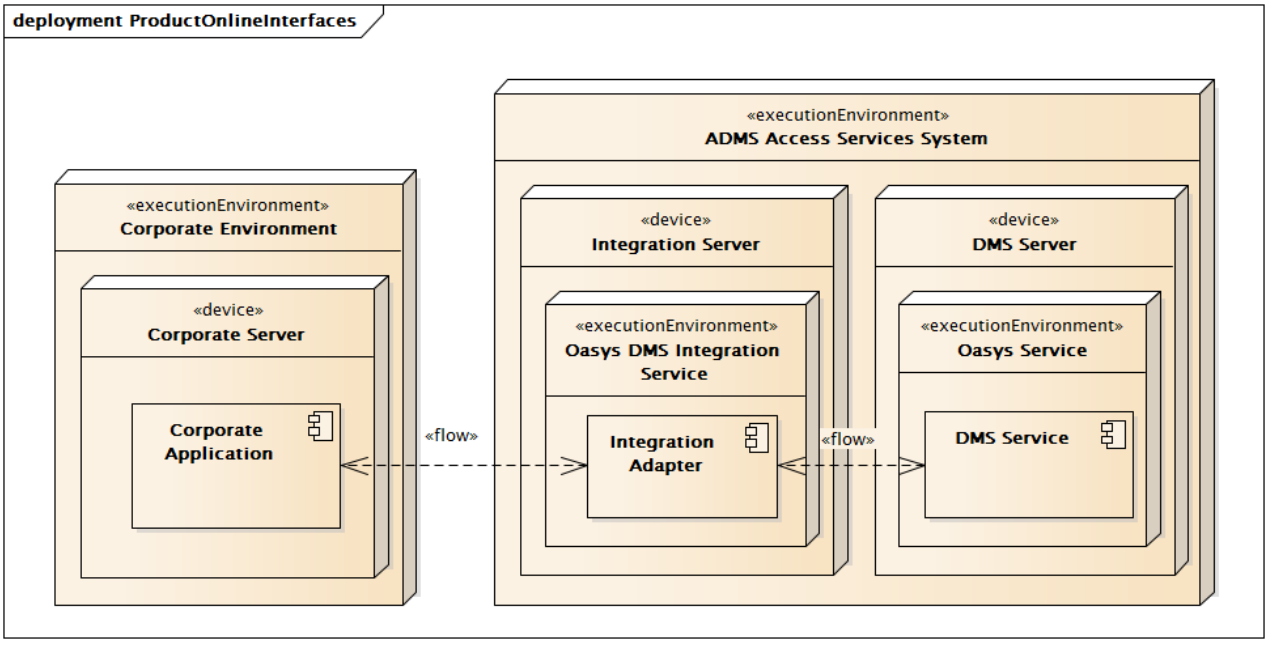

Figure 6.3 – The logical deployment view of the integration adapter

The Access Services (DMZ) system is used as a perimeter network segment placed between two security zones, with the aim of preventing the network traffic from passing directly between the corporate (technical) systems and the Core system.

The DMZ architecture uses the firewalls which are placed between two networks to disable the external users to directly access the production systems. The DMZ system is designed to hold the components constructed to communicate with the external systems since the DMZ zone is of the lowest security level.

This is the main reason why the adapters are deployed in the aforementioned environment in almost all system deployment plans.

Each adapter is a separate process inside one OASyS service. A pair of integration servers are designated to run the adapters in the high-availability (HA) cluster.

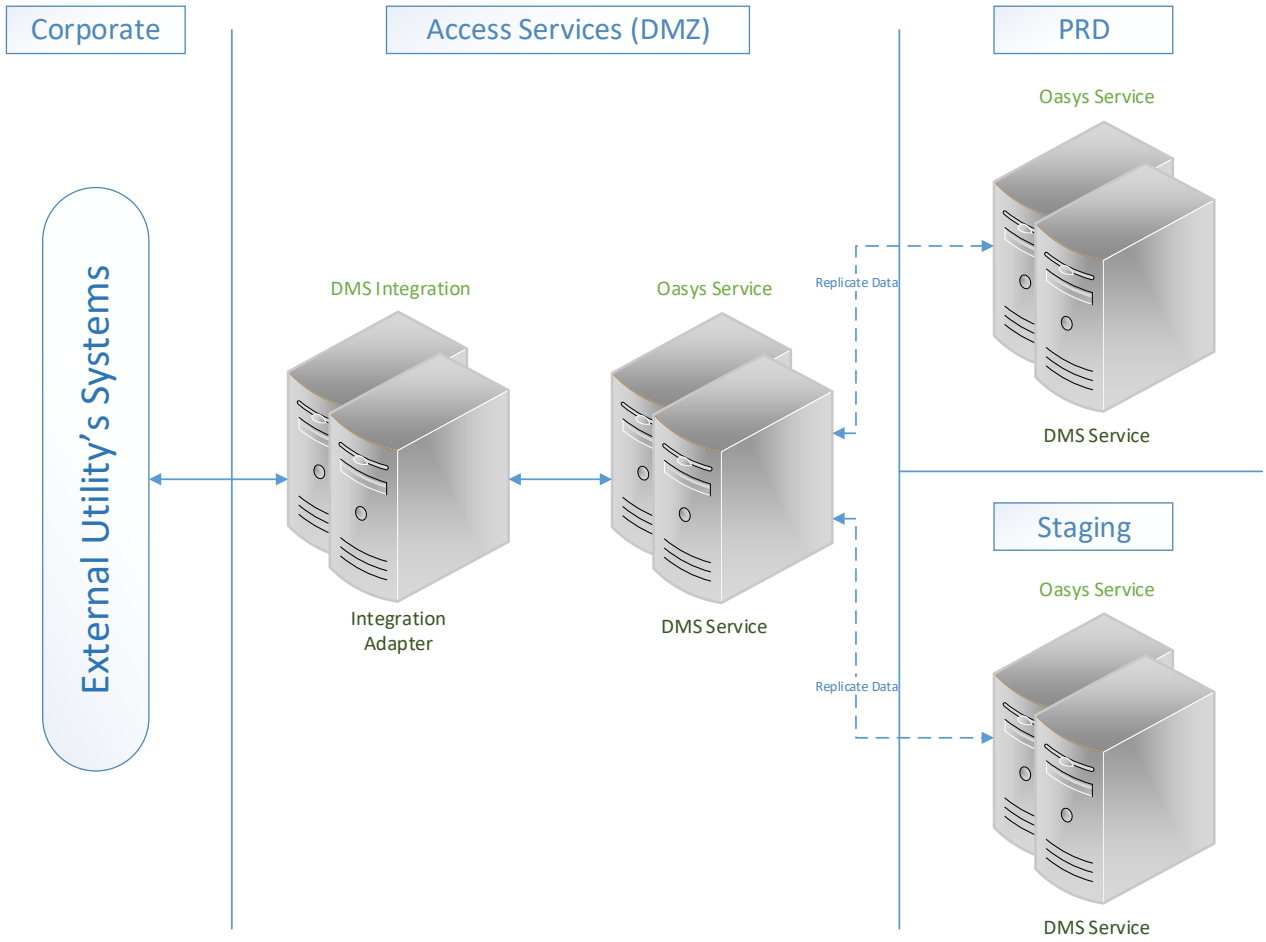

Figure 6.4 – The physical deployment view and data flow of the integration adapter

6.4. Availability

The availability tactics are designed to enable a system to endure the system faults so that a service being delivered by the system remains compliant with its specification.

Table 6.2 – The fault detection methods specification

Fault Detection Methods Specification	
Name	**Implementation**
Ping/Echo	This tactic is used only (manually) during the system setup and troubleshooting.

Fault Detection Methods Specification	
Name	**Implementation**
Monitor	Integration adapters relay on the OASyS infrastructure which is manageable through the Network Management Console (NMC). The NMC is used for the system monitoring.
Exception Detection	Each exception detected by the adapter is properly logged.

Other fault detection methods (heartbeat, timestamp, sanity checking, condition monitoring, voting, self-test) can be implemented if there are specific business requirements for them.

Table 6.3 – Fault recovery methods specification

Fault Recovery Methods Specification	
Name	**Implementation**
Spare (cold spare)	A pair of integration servers are designated to run the integration adapters in the high-availability (HA) cluster (failover cluster).
Exception Handling	Detected exception is logged and handled in a proper way and the information about the fault is sent back through the response. A list of possible faults is specified for each integration.
Software Upgrade	Standard SE hotfix or patch delivery.
Retry	Retry mechanism of the failure can be used by specifying the number of retries and the time between the retries.
Degradation	Integration adapter process can be set up to be critical or non-critical. A failure in the critical process will stop all the processes hosted by the OASyS DMS Integration Service, while a failure in the non-critical process will stop just that process.
Reconfiguration	Criticality of the process and startup of this tactic is configurable.

Other fault recovery methods (rollback, ignore faulty behavior, shadow, state resynchronization, escalating restart, non-stop forwarding) can be implemented if there are specific business requirements for them.

Table 6.4 – Prevent faults tactics specification

Prevent Faults Methods Specification	
Name	**Implementation**
Removal from service	Integration adapter can be removed from startup.

Prevent Faults Methods Specification	
Name	**Implementation**
Transactions	When a message is transformed by the adapter, in most cases, the adapter sends the message to one of the internal services which process and store the messages by using the transaction.

Other prevent faults methods (predictive model, exception prevention, increase competence set) can be implemented if there are specific business requirements for them.

6.5. Configuration

For the establishment of the end-to-end connection, the appropriate information needs to be provided from both sides. The virtual host names and virtual IP addresses of the DMS_Integration service on different sites are given in Table 6.5.

Table 6.5 – The DMS_Integration service information

Site	Virtual Host Name	Virtual IP Address
Primary	pdmzDMS_Integration	TBD
Backup	bdmzDMS_Integration	TBD

The Virtual IP Address is related to one pair of servers (Hot/Stand by). In case of a failover, the Standby server becomes HOT but the IP address used for accessing the web service stays the same. Therefore, the client applications are not aware of the failover. This is provided by the OASyS infrastructure and the Arbitration service. More details about the system configuration can be found in the appropriate System Configuration Plan document.

Integration adapter components provide certain amount of configurability so that smaller adjustments in the functionality can be easily applied to the system, without interface down time. Such feature is provided through dedicated configuration files of the adapter components. Note that besides the registry configuration file, not all configuration files are shared by individual adapters. Common adapter configuration files are following:

- **Registry configuration** – Primary configuration file of the integration adapter. Contains data needed for the adapter initialization and startup, as well as references to additional configuration files. Additionally, it contains process related parameters which can enable small modifications to business process. Can be overridden with project specific data.
- **Web service configuration** – Web service configuration file contains for initializing service hosts, as well as service clients. It contains common properties for defining web service binding, security, retry configuration and auditing. Normally utilized by web service host/client adapters.
- **Error configuration** – offers a possibility for customizing error details, which are either returned as fault responses from the integration adapters, and (or) published as a system event/alarm. It covers all adapter use cases. It can be split into multiple error configuration files, dependent on the interface implementation. This configuration is normally utilized only for web service host integration adapters.

Each error contains two sections, ADMS and CIM. ADMS section influences the internal validation rules, while the CIM section represents the CIM based reply error attributes returned to the operation invoker.

Besides the configurable errors, error configuration files contain an additional attribute "ErrorSeverityEventingThreshold", which defines which error's will be stored in ADMS event summary. By default, errors with greater ADMS severity than warning will be stored in the event database.

ADMS severity levels, from least to highest are:

- Info
- Warning
- Error
- Critical

- **Filter configuration** – offers a possibility for defining custom message filtering, defining custom event triggers. Normally present with publish subscribe integration adapters.

Following table offers details about integration adapter common configuration files.

Table 6.6 – Integration Adapter common configuration files

Configuration type	Document type	Mandatory	Root Directory
Registry	XML	Yes	…\OaSyS\Servers\Registry\Config
WebService	XML	No	…\ADMS\configuration\DMSIntegration
Error	XML	No	…\ADMS\configuration\DMSIntegration
Filter	XML	No	…\ADMS\configuration\DMSIntegration

As aforementioned, registry configuration files can be overrider in order to change configurable parameters. Overrides can be done automatically by defining custom override rules for a specific project installation and running the config tool process, or manually by creating the override file by hand. Details about registry configuration overrides should be found in specific system configuration and deployment documents.

Other adapter configuration files are not configurable in the same manner. In order to modify them, user needs to create a new configuration file of desired type and update the document reference in the registry configuration file.

6.6. Security

One of the main concerns in the integrations is how to secure the data in transit, which security techniques to use to support the CIA triad: confidentiality, integrity, availability and nonrepudiation (additional).

Using the authentication, authorization, auditing (AAA) main techniques, the system creates the secure context between the security principals which prove the confidentiality, integrity, availability and nonrepudiation. The following list of security techniques is provided in order to implement the CIA triad in the integration adapters:

- Transfer security mode & data encryption
- Security principal identity
- Security principal authentication
- Security principal authorization
- Access limitation
- Exposure limitation
- Auditing

Depending on the integration style and pattern, different protocol and AAA techniques are used to create the secure context.

6.6.1. Authentication

The EcoStruxure GridOps applications (e.g., Integration adapters) are often required to establish connections with different external systems residing in an untrusted environment, relying on different protocols/messaging systems (e.g., HTTP, SFTP, JMS, etc.). When the secure communication is required between the non-trusted environments, the certificates are used to support mutual authentication and data encryption.

Depending on the requirements, the following type of transfer security can be selected:

- Transport Security
- Message Security

Schneider Electric suggests the usage of the Transport Security where the user credentials and claims are passed by using the transport layer, meaning that the user credentials are transport dependent. The Transport Security secures the entire communication channel (e.g., by using SSL/TLS) and is used to provide the point-to-point security between the two endpoints (the service and client, without a proxy). Some of the advantages that are offered by the usage of the Transport Security are:

- It provides interoperability, meaning that communicating parties do not need to understand the WS-Security specifications.
- It may result in better performance.
- Hardware accelerators can be used to further improve performance.

The following out of the box types of web service security and authentication are supported through dedicated configuration:

- **None** – the SOAP message is not secured during transfer. The service is not authenticated by the client, nor vice versa.
- **OneWaySslAuthentication** – the security is provided using HTTPS. The service must be configured with the SSL/TLS certificates. The SOAP message is protected as a whole using HTTPS. The service is authenticated by the client using the service's SSL/TLS certificate. The client is not authenticated by the service.
- **TwoWaySslAuthentication** – the security is provided using HTTPS. Both the client and the service must be configured with the SSL/TLS certificates. The SOAP message is protected as a whole using HTTPS. The service is authenticated by the client using the service's SSL certificate. The client is authenticated by the service using the client's SSL certificate.

- **TransportWithMessageCredentialAuthentication** – the security is provided using HTTPS. The service must be configured with the SSL/TLS certificates. The SOAP message is protected as a whole using HTTPS. The service is authenticated by the client using the service's SSL certificate. The client is authenticated by the service with credentials from the HTTP header.
- **MessageSecurityCertificate** – the security is provided using the SOAP message security. Both the client and the service must be configured with the SSL/TLS certificates. The service is authenticated by the client using the service's SSL/TLS certificate. The client is authenticated by the service using the client's SSL/TLS certificate.

6.6.2. Authorization

The authorization of external systems to EcoStruxure GridOps is part of the baseline integration framework and it is performed using certificates. Every external system has a unique certificate with which it authenticates to the EcoStruxure GridOps. The authorization is achieved by controlling which external system is allowed to communicate with integration adapter (each adapter has a whitelist of authorized certificates). The same applies vice-versa, when adapter acts as a web service client for the external systems.

6.6.3. Auditing

Integration between systems could be interrupted due to the various reasons. Usually, such interruptions are caused due to some hardware malfunction or network (communication) problem which results in the different types of errors. Such issues can cause that both systems are not in sync. Due to that fact detailed error scenarios are defined in the appropriate chapters per each operation.

All integration adapters are logging activity in their own log file that is located on the server where the adapter is running. All log files are located at:

C:\SchneiderElectricData\OASyS\Servers\log and have following name format:

{AdapterScope}Adapter_PROCESSID#.log

Example:

AmiAdapter_12091.log

When a certain use case fails, the adapter stores appropriate entry within its application log. Through a dedicated configuration file, adapter can be configured to report an event (visible in the DMD and Windows Event Log) for the failed use case. Event creation is configurable based on the error severity. Next to the brief log entry and the event, a request message that caused the error can also be logged within the application log. Inbound and outbound messages are logged on a configurable log level that can be adjusted through a dedicated configuration file. Only exception to this rule is when the messages exchanged contain sensitive data.

The mentioned logging component also provides the functionality to monitor the data traffic through endpoints (web services and web service clients) that are exposed by the adapter. In case when there is no data traffic longer than a configurable period of time, through one of the endpoints, the mentioned component can generate an appropriate notification (alarm, event) that shall be displayed to the system administrators or operators within CORE DMD application. Such functionality is completely configurable through dedicated configuration file.

6.6.3.1. Sensitive Data

The messages which are exchanged via product online interfaces can often contain sensitive client or customer information. Integration configuration details, error exception messages may also contain sensitive data. It is important to have that data omitted from potentially malicious parties. Auditing of this data is performed in specialized log files. These specialized log files are located in the same directory as process logged files:

C:\SchneiderElectricData\OASyS\Servers\log and have following name format:

{AdapterScope}Adapter_PROCESSID#.sensitive.log

Example:

AmiAdapter_12091.sensitive.log

Auditing of sensitive data is implemented based on security guidelines and principles described in the *Security Data Classification - Data Anonymization Requirements* document which differs based on the software solution [1] and *EcoStruxure GridOps Management Suite 3.10 Secure Operations Guideline* document [2].

7. ENTERPRISE SYSTEMS INTEGRATION EXPERIENCES

EcoStruxure GridOps enterprise integration platform is already proved in production in over 80 utilities worldwide via some of the standard middleware products: Apache MQ, IBM Integration Bus, IBM WebSphere MQ, JBoss Fuse, Microsoft BizTalk, Mule ESB, Oracle Service Bus, SAP PI, Software AG Web Methods, TIBCO EMS.

So far EcoStruxure GridOps was integrated with following types of systems with help of out-of-the-box integration adapters:

- AMI Head End and MDMS Systems:
  - AMM Service Platform
  - DCC
  - ELSTER
  - L&G AMI Command Center
  - L&G MDMS
  - One Nordic
  - Sensus FlexNet
  - Siemens eMeter
- Automatic Vehicle Location:
  - Arcoda WS
  - CEMA TRACKING – Tracker
  - CompassCom – Tracking System
  - IBM Maximo
  - Smartrak - GPS Tracking System
  - Utilimarc Fleet Locate
  - URA – homegrown AVL System
- Asset Management Systems:
  - CBM – homegrown asset management
  - IBM Maximo
  - PSS6 – protection settings storage
  - SAP ECC6
- Customer Relationship Management and Interactive Voice Response:
  - 21st Century (IVR) Interactive Voice Response
  - AECall – Call Tacking Application
  - APS Notification Center
  - ATC Call Center
  - BCH email service – homegrown customer notification system
  - Blue Idea SMS gateway
  - Bosse – homegrown customer notification system
  - CaCe – homegrown customer notification system
  - CISCO Voice Portal
  - iFactor Storm Center
  - InfoSys
  - Gentrack CRM
  - RapidTalk SMS gateway

  - Selta Sip, TIBCO
- Customer Care and Billing, Customer Information System:
  - Carla CIS
  - DADS – customer load data
  - Oracle CC&B (Customer Care and Billing)
  - SAP CR&B
- Geographic Information System:
  - ArcFM
  - AutoCAD
  - Autodesk Map 3D
  - ESRI ArcGIS
  - GE Electric Office
  - GE Smallworld
  - GeoTech GIS
  - Intergraph
  - Mapinfo
  - Netbas
  - PowerGrid
  - SiGraph
  - STM
  - Tekla Trimble GIS
- Grid Engineering Software:
  - Feeder Load Analysis (FLA)
  - Siemens STM
  - TNEI – IPSA
  - Siemens PSSE
- Outage Management System:
  - ABB Abillity
  - GE Power On
  - Intergraph InService
  - CGI PragmaLINE
  - ExtenSys ORMS
  - Oracle NMS
- Outage Maps/Portals:
  - Appius – Fault Measles Map
  - APS Outage Portal – homegrown outage portal solution
  - Kubra (former iFactor) Storm Center
- Systems Monitoring:
  - Splunk
  - HHR – homegrown monitoring system
  - HP OpenView
- Telephony Systems:
  - Mitel
  - Turret Support Server

- Vegetation Management Systems:
  - GSI Forester
- Video Walls:
  - PTech Primate Video Wall (PVW) server + BARCO Video Wall
- Weather Data Providers:
  - Amec
  - Arso
  - DTN
  - Radar Meteo
  - Weatherzone
- Work Order Management:
  - IBM Maximo
  - SAP PM
  - Soter – homegrown work order management system
  - SunNet TOA
- Workforce Management System:
  - AMT-SYBEX / Ellipse
  - Bosse – homegrown workforce management system
  - C2B MEDIA Limited – TOAD
  - CGI / PragmaCAD
  - CityWorks
  - IBM Maximo
  - Oracle workforce management
  - ServiceHub/G4
  - Ventyx Service Suite Software

List of projects on which listed systems were integrated with EcoStruxure GridOps, can be delivered separately.

8. DEFINITIONS AND ABBREVIATIONS

Definition/Abbreviation	Description
AAA	Authentication, Authorization, Auditing
ADMS	Advanced Distribution Management System
CIA	Confidentiality, Integrity, Availability
DMZ	Demilitarized Zone
FT	File Transfer
GDA	Generic Data Access
HA	High Availability
MES	Messaging
RPI	Remote Procedure Invocation
SD	Shared Database
SE	Schneider Electric
WCF	Windows Communication Foundation