C-DAX Deliverable D2.1:

C-DAX Requirements

Use Case Descriptions for Domains 1, 2 and 3 and Derived C-DAX Requirements

Release 1.0

Final version

April 30, 2013

Contributors:

Alcatel-Lucent Bell, Liander, Eberhard Karls Universitaet Tuebingen, iMinds, University College London, University Of Surrey, Radboud University Nijmegen, Ecole Polytechnique Fédérale De Lausanne

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Document History

December 21, 2012	First draft of the document. Requirements for the first two use cases will be added later
February 15, 2013	Substantial revision including re-definition of the first two cases and requirements thereof
April 18, 2013	Reworked version with new materials on the 3 use cases and changes from the in-depth March and April reviews
April 30, 2013	Final release

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Abstract

The progressive penetration of conventional and renewable distributed generation is driving major changes in the whole power systems infrastructure justifying the introduction of more intelligence, in particular, in power distribution networks. The availability of an advanced information infrastructure plays a central role as future power systems cannot be supported by centralized information infrastructures on which today's power systems rely.

The C-DAX project aims at providing a cyber-secure distributed information infrastructure to the energy distribution networks. The C-DAX architecture adopts an information-centric networking (ICN) architecture that shows properties beneficial to the smart grids such as security, resiliency and flexibility, versus conventional information systems. C-DAX is tailored to the specific needs of smart grids for efficient support of massive integration of renewable energy resources and a heterogeneous set of co-existing smart grid applications.

This deliverable describes the use cases under the consideration of the C-DAX project and their corresponding functional requirements. The use case descriptions covers the following 3 use case domains: low voltage pervasive distributed energy resources, medium voltage distributed energy resources and retail energy transactions.

The C-DAX platform requirements include requirements that are general in scope. They cover fundamental system requirements that are required for the basic operation of the platform, such as configuration, communication, data management and security requirements. Further, additional requirements are defined in the specific scope of C-DAX supporting the three applications exemplified by three use cases defined as follows:

- Use Case 1: This use case considers the communication between Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs) in distribution substations with Supervisory Control and Data Acquisition (SCADA) master control and other systems in the utility Distribution Control Center (DCC);
- Use Case 2: This use case considers the communication between the Phasor Measurement Units (PMUs) deployed along the MV distribution lines and PMU Data Concentrators (PDCs) located at the distribution substations and other communication required for distribution management implementation based on state estimation using the PMU measurements;
- Use Case 3: This use case considers Retail Energy Transactions (RETs) between the consumers of energy and owners of distributed generation (DG) including those owned and located at consumer premises. These transactions facilitate the matching of demand with supply and/or the operation of Demand Response (DR) mechanisms.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Table of Contents

1. Introduction ... 6
1.1. Objectives ... 6
1.2. Deliverable structure ... 8
1.3. Energy distribution network infrastructure overview ... 6
2. Selection of the Use Cases and Methodology ... 9
3. C-DAX Scope of Work ... 12
3.1. Functional Objectives ... 12
3.2. Operational Objectives ... 12
3.3. Evaluation Considerations ... 13
3.4. Data Management with C-DAX ... 13
3.5. Scope of the Requirements ... 13
3.6. Terminology ... 14
3.7. Assumptions ... 14
4. General C-DAX Platform Requirements ... 16
4.1. General Description and System Requirements ... 16
4.2. General Communication Requirements ... 17
4.3. General C-DAX Configuration Requirements ... 18
4.4. General Data Management Requirements ... 18
4.5. General Security Requirements ... 19
4.5.1. Physical Protection ... 19
4.5.2. Communication Protection ... 19
4.5.3. System Protection ... 22
4.6. Cryptographic issues and NIST recommendations ... 22
5. Use Case 1: RTU/IEDs at Distribution Substations ... 24
5.1. Remote Terminal Units ... 24
5.1.1. Description of RTU/IED Operation ... 24
5.1.2. Communicating Entities ... 25
5.2. Assumptions: Use Case 1: RTU/IEDs at Distribution Substations ... 26
5.3. Requirements: Use Case 1: RTU/IEDs at Distribution Substations ... 26
5.3.1. C-DAX Clients ... 26
5.3.2. Topics ... 27
6. Use Case 2: Pervasive Synchrophasor Deployment at MV Level ... 29
6.1. Synchrophasors ... 29
6.1.1. Description of Synchrophasor Operation ... 29
6.1.2. C-DAX Clients ... 30
6.2. Assumptions: Use Case 2: Pervasive Synchrophasor Deployment ... 30

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

6.3. Requirements: Use Case 2: Pervasive Synchrophasor Deployment 31
6.3.1. C-DAX Clients 31
6.3.2. Topics 32
7. Use Case 3: Retail Energy Transactions 34
7.1. Actors 35
7.2. Application scenarios 36
7.2.1. Demand Response (Application Scenario I) 36
7.2.2. Flexibility offerings (Application Scenario II) 38
7.2.3. Electric Vehicle support (Application Scenario III) 40
7.2.4. Hybrid scenarios (Application Scenario IV) 40
7.3. Additional features 40
7.3.1. Data aggregation 41
7.3.2. Data filtering 42
7.4. Assumptions 42
7.5. Requirements 43
7.5.1. Network Scale 43
7.5.2. Message priorities and delay requirements 43
8. Concluding Remarks 45

List of Appendixes

APPENDIX A An example of distribution grid 46
APPENDIX B A Framework for Communication Network Architectures.....47
APPENDIX C Priority and Delay Objectives for Traffic of Smart Grid and Other Utility Applications.....49

References.....51

List of Acronyms.....52

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

1. Introduction

The progressive penetration of conventional and renewable distributed generation is driving major changes in the whole power systems infrastructure justifying the introduction of more intelligence, in particular, in power distribution networks. The availability of an advanced information infrastructure plays a central role as future power systems cannot be supported by centralized information infrastructures on which today's power systems rely.

The C-DAX project aims at providing a cyber-secure distributed information infrastructure to the energy distribution networks. Because of the increasing deployment of Distributed Energy Resources (DERs), be it large solar and wind farms connected to the medium voltage (MV) distribution grid or smaller consumer photovoltaic (PV) infrastructures connected to the low voltage grid, we need to revisit the way we monitor and control energy distribution networks. The energy flows, which used to be predictable unidirectional flows from the power generation plants down to the consumers, have now become less predictable, also following the reverse direction. Indeed, local and distributed energy resources may send energy flows back to the distribution infrastructure that were initially not conceived to accept such reverse flows. This creates a risk of instability in the distribution grid. Consequently, a primary objective for the C-DAX project is to ensure reliable, safe and efficient delivery of energy between generation and consumption end-points at the Distribution Service Operator (DSO) level, with a focus on distribution network stability. This priority setting will facilitate the identification of the use cases that will be selected for further study in C-DAX.

1.1. Objectives

The C-DAX architecture will adopt an information-centric networking (ICN) architecture that shows properties beneficial to the smart grids such as security, resiliency and flexibility, versus conventional information systems. C-DAX will be tailored to the specific needs of smart grids for efficient support of massive integration of renewable energy resources and a heterogeneous set of co-existing smart grid applications.

The C-DAX architecture aims at providing smart grids with:

- the flexibility to integrate renewable energy resources of different sizes to support communication with individual consumers to facilitate the growing number of active subjects connected to electrical grids;
- the secure, synchronized and timely delivery of measurement and control data to ensure stable and reliable supply;
- the security and reliability required by distributed control systems;
- the provisioning of a resilient cyber-secure layer to currently used protocols in the electrical grids infrastructure.

1.2. Energy distribution network infrastructure overview

In order to clarify the context of the use cases that are detailed in this document, it is important to understand the general topology of the electrical distribution networks to which these use cases apply. In particular, we make reference to the medium and low voltage grids where we may expect to interface a certain number of monitoring and control devices, energy resources as well as consumers. The monitoring devices can be: (i) Phasor Measurement Units (PMUs, especially in medium voltage networks) and (ii) metering devices (voltage, current and power meters). It is worth noting that, in general, metering devices are Remote Terminal Units (RTUs) or Intelligent Electronic Devices (IEDs). In Figure 1 the two categories monitoring devices are shown. As it can be seen, PMUs are placed in correspondence of the network busses (e.g., secondary medium-to-low-voltage substations). RTUs can be composed by general metering devices placed everywhere in the network (in Figure 1, the RTU is supposed to measure, and stream, general electrical quantities on the medium voltage side of the primary substation). IED are composed by breakers of protections equipped with metering

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

systems; in this respect they can be placed everywhere in the network and, in Figure 1, the IED is associated to the breaker 'Ctrl_Br' that is expected to be equipped with local sensors capable of metering general electrical quantities.

The control devices we consider include on-load tap changers of power transformers, controllable reactive power compensators (capacitor / inductance banks, static-var compensators), remote-controllable breakers, etc. Finally, the energy resources are composed of active generators, storage systems or controllable loads/customers. These elements are illustrated in Figure 1 with a particular reference to a medium-voltage power distribution network. The figure is not meant to be exhaustive but to provide a first overview of the ecosystem in which the C-DAX problem statement takes place.

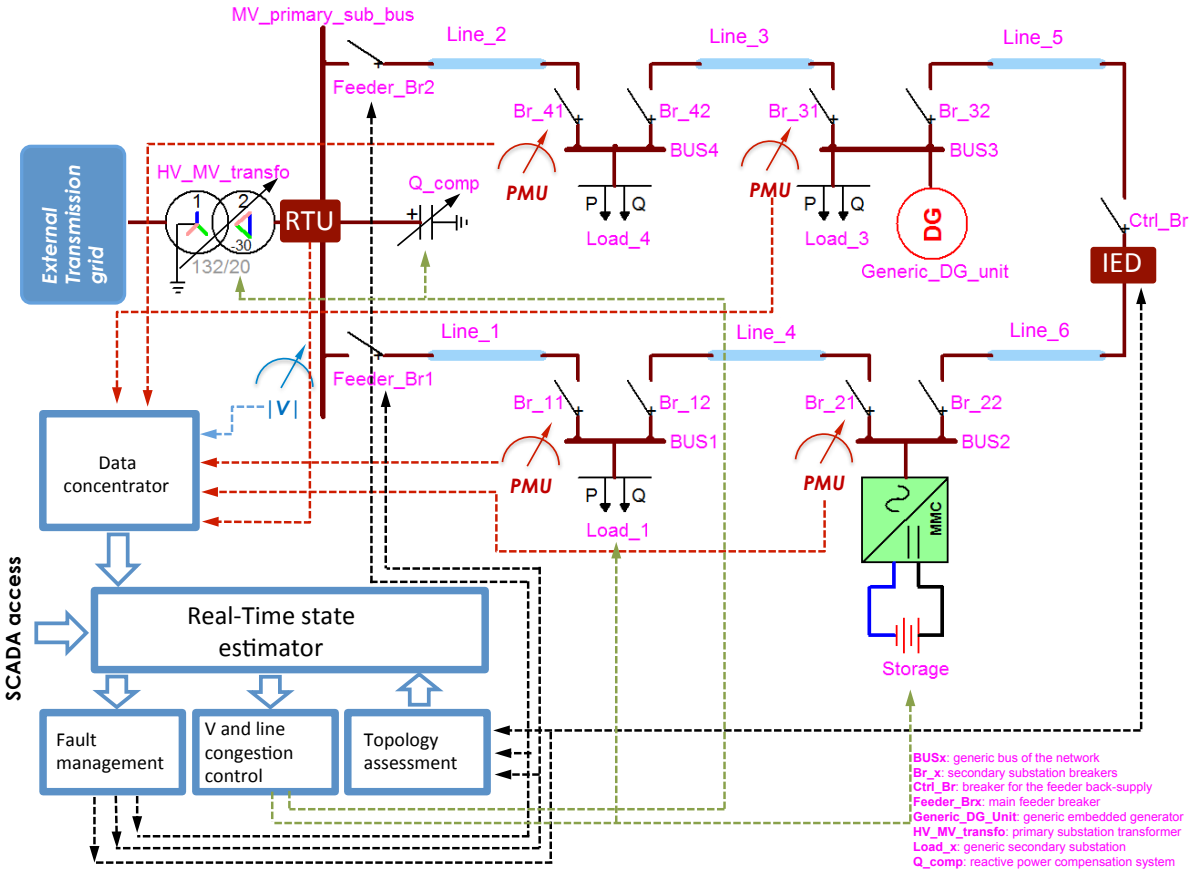

Figure 1: *Structure of the targeted medium-voltage power distribution networks and elements relevant to the C-DAX platform.*

The topology shown in the figure allows us to highlight the following functionalities that serve for the definition of the use cases described next:

- **Monitoring:** this functionality is realized by the following sub-functions:
  - Concentration of data coming from (i) PMUs (phasors with absolute time stamps) and (ii) Remote Terminal Units (RTUs) like traditional meters (scalar quantities with / without absolute time stamps).
  - Concentration of data coming from network breakers (marked by Br_* in the figure). Their status is represented by a Boolean value with an absolute time stamp.
  - Topological assessment of the network status by using data coming from network breaker monitoring.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

  - The Real-Time State Estimation (RT-SE) of the network is achieved by linking the phasor data concentrator and the network topology processor with the RT state estimator algorithm. The output of this process (composed by phasors of the network node voltages, lines' currents and power flows) is subsequently reported to an RT database.
  - In addition to its use for state estimation, the raw data from PMUs and RTUs, combined with state estimator outputs, can be used in time-critical (e.g., fault management, voltage and congestion controls) and non-time-critical functionalities (e.g., energy trading).
- **Voltage control, line congestion management:** these functions take the status of the grid provided by the RT-SE and implement specific control algorithms. The controlled variables of these algorithms are the network node voltages and/or the lines power flows (the uncontrolled variables become the line power flows in case they are not the target of the control and the power flows from the external transmission grid), whilst the control variables are (i) the power injected into the grid of selected number of energy resources, (ii) set-points of primary substation tap changers and (iii) set-points of variable-reactive power compensators.
- **Fault management:** this functionality can be separated in two sub-functions:
  - Fault detection/identification: it refers to the function that identifies a fault in the grid and also its type. The input data is (i) the raw PMUs/RTUs streamed data or (ii) the RT network state. The output data consists of tripping signals sent to specific breakers, thus remotely controlling them.
  - Fault location: it refers to the function that identifies the faulted line (branch) or the exact fault location along a line. The input data is the RT network state and the output data consists of tripping signals send to specific breakers allows their remote control. This functionality is usually performed off-line.

1.3. Deliverable structure

This deliverable describes the use cases under the consideration of the C-DAX project and their corresponding functional requirements. The use case descriptions will cover the following 3 use case domains: low voltage pervasive distributed energy resources, medium voltage distributed energy resources and retail energy transactions.

This deliverable is structured as follows:

- Section 2 explains the methodology for use cases definition and prioritization; it concludes with the selection of three use cases for further specification in C-DAX;
- Section 3 defines the C-DAX scope of work and specific terminology; it provides a modeling overview and lists technical assumptions taken to further scope the work;
- Section 4 provides the generic C-DAX platform requirements;
- Sections 5, 6 and 7 describe use cases 1, 2 and 3, respectively;
- Section 8 draws the conclusions on the use cases based requirements.

At the end of the document, a number of appendixes are also provided to further detail certain technological aspects of the work that are regularly referred to throughout the document. Background information on distribution grids can be found in Appendix A. In Appendix B, a framework for communication architecture is briefly described to provide a context for these requirements and the terminology used in this document. Appendix C provides reference material on performance objectives for traffic of smart grid and other utility applications.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

2. Selection of the Use Cases and Methodology

A use case description as provided in a use case analysis may at first appear as being loose in nature. However, applying the use case methodology to a technological ecosystem allows to list and describe its business stakeholders and to deduce actors, functions and data elements, thereby providing valuable information for the functional and informational layers of a system's architecture.

The reference for our work on use cases analysis for C-DAX is the European Commission's mandated Smart Grid Coordination Group (SG-CG) that collects, analyzes and harmonizes smart grid use cases in order to allow a Use Case Management (UCM) process, also reflected in their corresponding UCM document [21].

The UCM document follows an agreement by CEN, CENELEC and ETSI on a set of European use cases for the smart grid. The document contains a prioritized list of high-level use cases for the smart grid. The UCM work is relevant because its materials were provided by a broad set of players in the European energy sector, thereby guaranteeing an exhaustive coverage of the problem domain by means of a set of broadly accepted use cases.

Because of the vast number of use cases that apply to the electricity grid and the variety of domains they apply to, the M/490 document structures the use cases as follows: use cases are clustered in Use Case Groups (UCG) that contain high level use cases that are considered more generic as well as primary use cases that are more detailed. The primary use cases contain the primary use case scenarios that define sequences of events that may realistically take place in these primary use cases.

The Working Group Sustainable Processes (WGSP) that is in charge of the UCM document has defined a series of use case groups, and a series of use cases in each of these groups. **Table I** provides an overview of the main use case groups and use cases in the UCM document together with a brief use case description.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Table I: *UCM Use Case Groups and Descriptions*

M/490 UCM Use Cases	Use Case Description from Sustainable Processes document V 1.0
Use Case Group Market Facilitation, *Retail*	**Use Cases that act between Production, Retail, Service Operators, Grid Managers, DER, Con- and prosumers**[1]
WGSP 2110 Receiving consumption, price or environmental information for further action by consumer or a local energy manager	The objective of this use case is to exchange information between external actors and the home premises in order to provide energy consumption awareness, energy trading, status in home energy devices, monitor consumption. A combination of the functions described in this use case can be labeled as "Demand Response". This high level use case comprises four different primary use cases: 1. Exchange information regarding power consumption or generation 2. Exchange price and/or environmental information 3. Send warning signals 4. Retrieve status of smart devices.
WGSP 2120 Direct load / generation management	The objective of this use case is to manage in-home devices in order to control power consumption, generation or storage resources for example to avoid the risk of black out, react to real-time peak power signals, balance the load between consumption and local production.
WGSP 2128 Flexibility offerings	The objectives of this use case are the exchange of offerings of the use of flexibility in supply and demand with another party, negotiation of these offerings and activation.
WGSP 1003 Generic Smart Charging	Smart charging makes it possible that even with limited network capacity multiple electric vehicles can simultaneously be charged if the charging is done in a "smart" way. Smart charging enables peak shaving, demand side management for all purposes and can postpone or even prevent network expansion.
Use Cases for Grid controlling "Normal operating Network Stability in MV Networks"	**Use cases that act on MV level**
WGSP 0100 Fault Location, Isolation and Restoration (FLIR)	FLIR automates the management of faults in the distribution grid. It supports the localization of the fault, the isolation of the fault and the restoration of energy delivery.
WGSP 0200 Voltage control and power flows optimization, i.e., Volt and Var control and Optimization (VVO)	The voltage profile of the distribution grid is continuously monitored and optimized using the available network flexibilities.
Monitoring the Distribution Grid	**Use cases that act on MV level**
WGSP 0600 Monitoring the distribution grid	No Description available in the standard, we will use Use Case 2.
WGSP 2300 Emergency Signals	For emergency situations in the grid the grid operator has a portfolio of options available in order to influence the situation (e.g. via reserve power). This use case describes the option to shut down consumption by intelligent load shedding via direct load management.

[1] *Prosumers* are entities that are both consumers and DERs (see also Section 7.1).

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

As shown in the table, the WGSP defined the following use case groups:

- **Retail and market facilitation:** this is an interesting use case group that potentially covers 'many to many' type of messaging between the communicating entities, which is required for evaluating the communication abilities of the platform. It fits in two application categories (domains): domain 1: Low Voltage (LV) pervasive DER and domain 3: market retail transactions. The selected use case in this group is: *WGSP 2110: receiving consumption, price or environmental information for further action by consumer or a local energy manager*. It will be further identified as "Use Case 3".
- **Grid controlling normal operating network stability in MV networks:** this use case group refers to normal operations for controlling the stability of the MV grid infrastructure. This category is important to demonstrate C-DAX's ability to connect to normal grid control operations. It fits in one application category: domain 2: medium voltage grid (MV DER and Microgrids). The selected use case in this group is: *WGSP 0200: voltage control and power flows optimization (VVO)*. It will be further identified as "Use Case 1".
- **Monitoring the distribution grid:** this use case group refers to the constant monitoring in real time of the status of the medium voltage grid thanks to the information collected from a pervasive network of synchrophasors (PMUs) deployed across the medium voltage grid. This deployment of advanced prototypes of PMUs deployed on the MV grid is instrumental in the definition of the project. It fits in two application categories: domain 1: LV pervasive DER (in the sense that the reverse energy flows imply an advanced distribution grid monitoring) and domain 2: MV DER and Microgrids. The selected use case in this group is: *WGSP 0600: monitoring the distribution grid*. It will be further identified as "Use Case 2".

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

3. C-DAX Scope of Work

The C-DAX platform requirements will include requirements that are general in scope. They cover fundamental system requirements that are required for the basic operation of the platform, such as configuration, communication, data management and security requirements. Further, additional requirements will be defined in the specific scope of C-DAX supporting the three applications exemplified by the three *use cases* (as selected in the previous section).These three use cases can be further described as follows:

1. *Use Case 1 (UCG Grid controlling normal operating network stability in MV networks):*
   For this use case we consider the communication between Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs) in distribution substations with Supervisory Control and Data Acquisition (SCADA) master control and other systems in the utility Distribution Control Center (DCC);
2. *Use Case 2 (UCG monitoring the distribution grid):*
   For this use case we consider the communication between the PMUs deployed along the MV distribution lines and PMU Data Concentrators (PDCs) located at the distribution substations and other communication required for distribution management implementation based on state estimation using the PMU measurements;
3. *Use Case 3 (UCG retail and market facilitation):*
   For this use case we consider Retail Energy Transactions (RETs) between the consumers of energy and owners of distributed generation (DG) including those owned and located at consumer premises. These transactions facilitate the matching of demand with supply and/or the operation of Demand Response (DR) mechanisms.

3.1. Functional Objectives

This selection of use cases allows covering the following three important high level functionalities of the C-DAX platform:

- Its ability to inter-operate with normal grid operation to ease deployment and integration of the C-DAX platform with the installed base, thereby facilitating migration scenarios. This is covered by Use Case 1.
- Its ability to constantly monitor in real time the status of the medium voltage grid, thanks to the information collected from PMUs deployed across the medium voltage grid. This is relevant to the objective of stability of the distribution grid. This is covered by Use Case 2.
- Its ability to handle many retail energy transactions with various topologies, in order to facilitate sale and purchase of energy between consumers, producers and prosumers of energy. Note that these retail operations are also instrumental to contribute to the stability of the grid by allowing energy peak shaving. The retail operations are covered by Use Case 3.

3.2. Operational Objectives

On the operational level, use cases 1 and 2 are based on the utility's objective of reduction in power outage as quantified in the metric *Cumulative Lost Minutes* (CML). In addition to providing improved consumer satisfaction with minimal disruption in their daily lives, very low values of CML will also significantly reduce utility's financial liabilities based on regulatory rules.

Some of the main functions associated with effective management of the distribution grid are state estimation, fault management, and voltage control based on power flow analysis. Consequently, the current operations of monitoring the power grid at distribution substation based on IEC 61850 standards and control of the power grid based on such monitoring should be the goals of Use Case 1 to be supported by C-DAX. Deployment of PMU in the MV grid has the promise of markedly improved estimation of the states of the distribution grid contributing to rapid grid stability, particularly with the ever-increasing deployment of DERs at the MV level. Therefore, management of

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

the PMU data, consequent power grid state estimation, and its control will be the goals of Use Case 2. Thus both these use cases will address the MV distribution grid. Use cases corresponding to operations at the LV grid are deferred to future C-DAX development.

Use Case 3 allows answering the business need of handling many retail energy transactions to facilitate sale and purchase of energy between consumers, producers and prosumers of energy. Retail Energy Markets (REM) are expected to be developed with very large growth in deployment of DER at medium voltage level and at consumer locations at the low voltage level as well as the increased consumer awareness in energy management and access to lower cost energy supply. These retail operations can also contribute to the stability of the grid by allowing energy peak shaving.

3.3. Evaluation Considerations

In terms of complexity and priority for implementation in the C-DAX project, we have selected the use cases for simulation only, for test-bed testing or for field trial, according to criteria as follows:

- Due to its complexity, Use Case 3 cannot realistically be tested in the field or even on a test-bed due to the high number of consumers and providers it requires. Hence, this use case is selected for simulation only.
- Because of the impracticality of the deployment of PMUs in the field solely for the C-DAX testing (and the verification of its validation), Use Case 2 cannot realistically be tested in the field either. However, this use case fits the test-bed testing, even though deploying a large number of PMUs would be difficult and too costly for the project.
- Due to its monitoring nature and its inter-operation with field elements, Use Case 1 fits the requirements for a field trial.

3.4. Data Management with C-DAX

Data management in C-DAX is based on a distributed storage cloud that is accessed using the *publish-subscribe* (pub/sub) paradigm. *Publishers* of data transmit (push) data to C-DAX where it is stored. Subscribers receive (pull) data from C-DAX as needed (as subscribed to). This pub/sub architecture provides for added security and data privacy. In most cases the direct transfer of data between a publisher of data and its subscriber(s) is not permitted, except in the case of control signals and other mission-critical applications that have a very low delay requirement.

Examples of publishers for Use Case 1 are the RTUs / IEDs pushing SCADA measurements and events and the DMS systems in the DCC pushing control signals to the RTU/IEDs. These elements are also the subscribers pulling the corresponding data pushed by the other systems. E.g., DMS systems subscribe to the measurements and events published by the RTU/IEDs, whereas the RTU/IEDs are the subscribers of the control signals and polling commands issued by the DMS systems.

Examples of publishers for Use Case 2 are the PMUs pushing measurements and status information collected at the respective grid points and utility applications pushing periodic poll messages and control signals for operating relays and other actuators.

For the third use case of RET, examples of publishers are the consumers, prosumers (i.e., entities that are both consumers and DERs) and stand-alone DERs, sending transaction requests. The same entities are examples of subscribers receiving the transaction information.

3.5. Scope of the Requirements

The functional requirements in this deliverable address only those C-DAX functions that are actually used for receiving data from the publishers and for transmitting data to the subscribers. While C-DAX needs to be "aware" of the performance (for example, network delays) of the underlying communication networks for determining the best routing between the C-DAX servers, C-DAX itself

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

cannot influence the performance of those networks. Thus, the end-to-end performance of client applications cannot be considered the sole responsibility of the C-DAX platform. Also note that the "awareness" of the performance of underlying networks is not inherent in C-DAX: the C-DAX operators or some network management system(s) need to feed the C-DAX platform with up-to-date network performance information.

3.6. Terminology

The following terminology will be used throughout this requirements document:

1. C-DAX will mean the C-DAX platform or C-DAX "cloud", which consists of one or more "C-DAX nodes", interconnected by the communication network[2].
2. Depending on the context a "C-DAX client" or just a "client" will refer to a subscriber or a publisher in the pub-sub mechanism. However, in the context of a use case, C-DAX clients are also "clients" in the use case. To avoid confusion, we will only use the word client alone when denoting a client in a use case.
3. Since this document considers requirements for the overlay networking mechanism of the C-DAX platform, the term "routing" is generally used to refer to the routing between C-DAX nodes, i.e., C-DAX nodes applying the forwarding rules to determine the path followed by a message sent by a C-DAX node to another C-DAX node. It is the overlay routing between C-DAX nodes. Thus, the C-DAX routing is not related and is independent of the Internet Protocol (IP) routing used in the underlying IP networks (when they exist for interconnection between the C-DAX nodes).
4. A "message" or "data message" is the basic unit of data that must be handled by the C-DAX cloud. C-DAX shall support storing messages with multiple formats and sizes as determined by the publishers for the underlying protocols (the transfer of messages) between publishers and subscribers.
5. The verb form "shall" is used for the specification of a requirement. For referencing purpose, each requirement can be identified by the number of the (sub) section in which it appears followed by a "numbered" hierarchy of a paragraph containing the requirement.

3.7. Assumptions

In this document the following assumptions are made:

1. It is assumed that each C-DAX client (publisher, subscriber, or both) is equipped with communication network interfaces for the sending and/or receiving of data to/from a C-DAX node. Such an interface corresponds to the actual network technology used for connecting that client. Thus, no requirements are provided for the network interfaces for connecting the client. Note that in the context of a network a client is sometimes called a network endpoint or just an endpoint in this document.
2. The client connects to a Field Area Network (FAN) for communicating with C-DAX[3]. Refer to Annex B for the definition of FAN and other communications terms commonly used in communication network architectures of the smart grid.
3. There may be multiple clients at a single location connected over a local network to an aggregation point such as a router or a gateway. Examples of local networks are a substation LAN, a DCC LAN, a Home Area Network (HAN), or a local network connecting the

[2] The C-DAX platform requires connectivity from communication networks. However, the networks used for such interconnection are not considered part of the C-DAX platform.

[3] In the taxonomy of communication networks, utilities use the term FAN to refer to a network that connects a remote network endpoint to the utility core network. Utilities limit the use of the term WAN (Wide Area Network) to the core network.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

microgrid clients. In that case it is the FAN/WAN that connects the aggregation point for the transfer of data from the clients that are connected in that local network. It is assumed that such an aggregation point may exist at a location with multiple clients, but no requirements are provided for the local network or for the aggregation point. In the case of a HAN, there may be a home gateway or a smart meter at such location that connects to the FAN and is acting as an aggregation point at that location. It is also possible that there may be two different aggregation points at one location: say the meter at a home for Use Case 1 and a home gateway for Use Case 3, possibly using two different FANs.

4. A C-DAX node may be collocated at locations with one or more clients and other systems. For example, if the C-DAX node is located at a distribution substation, it will connect to the substation router over the substation LAN along with other clients and systems at the substation. Another example is if the C-DAX node is located at the utility DCC. Again the C-DAX node connects to the DCC router over a LAN along with clients and other systems in the DCC. The router may connect to a FAN or a WAN depending on the C-DAX node location. In the case that the router is connected to the WAN, a remote client connection to the C-DAX goes through the FAN connecting the client to the WAN.
5. Multiple FAN connections may be carried over the same network. For example, a C-DAX node may communicate with multiple clients over a single RF mesh network.
6. It is assumed that all communication between a client and C-DAX is carried over IP as end-to-end networking protocol.
7. With the pub-sub data management model, it is assumed that all clients communicate with C-DAX for publishing data and subscribing to receiving data, *including for the communication of control signals.*
8. It is assumed that a data unit received from a client is delivered without any changes and provided as a single data unit to the subscriber, irrespective of the fact that the data unit may have been packetized at the IP layer as needed by the packet size supported by the network.
9. We do not make assumptions about the traffic being carried over the utility's communication network. In particular, the WAN and FAN links carrying traffic to and from the C-DAX cloud may be carried over network links that also carry traffic from other utility applications. The requirements for performance, reliability, and security of the C-DAX traffic must be maintained irrespective of shared links in the network. Further, in the eventuality that the utility's communication network includes carrier (service provider) services over a shared infrastructure that also carries other carrier customers' traffic, it is assumed that the utility has sufficient service level agreements (SLA) with the carrier to guarantee its performance, reliability, and security objectives. In that case, again, the requirements for performance, reliability, and security of the C-DAX traffic must be maintained irrespective of the use of such carrier services. The assumptions in this point do not imply that a shared infrastructure such as the public Internet may or may not be used.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

4. General C-DAX Platform Requirements

For ensuring reliable and safe C-DAX operation, the high availability of access to transferred or stored data are mandated. Thus, communication messages must be delivered to intending destination in a reliable and timely manner. Confidentiality, integrity and authenticity of communication messages must be supported in an end-to-end and scalable manner. Accessing computation resources or data need to be strictly controlled in fine-grained manners. System must be protected against internal failures or cyber-threats such as Denial of Service (DoS) attacks and malware intrusion and restored after service disruption in self-configurable and self-healing manners. Furthermore, we shall provide C-DAX interfaces to C-DAX users such as application designers and developers to allow them to easily develop and deploy applications (or services) over C-DAX platforms. These interfaces will be designed such as to hide from these users the complexity and technical details such as communication specifics, security, reliability issues, and so on.

In this section, the general requirements for the C-DAX platform are discussed.

4.1. General Description and System Requirements

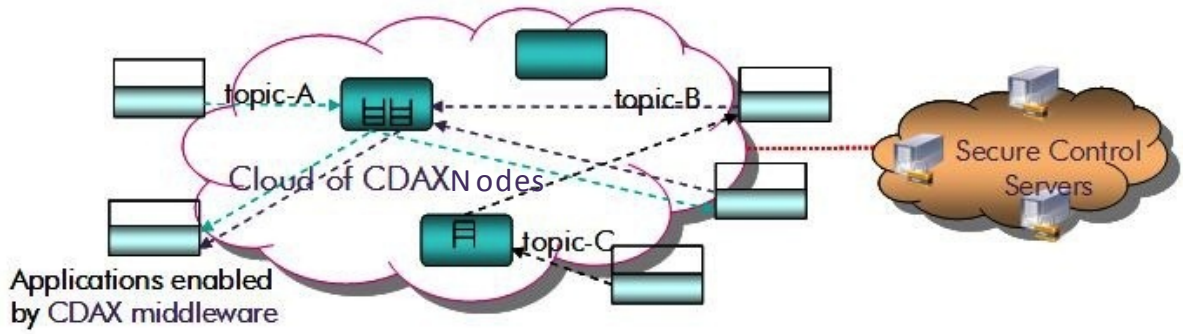

Figure 2: *The components of a C-DAX platform.*

Before discussing the details, we briefly review the components and basic principles of the C-DAX platform.

As shown in Figure 2, a C-DAX platform consists of three major components: the C-DAX middleware that provides *publisher-subscriber* interfaces to clients such as a field devices or application servers, C-DAX nodes that take responsibility for the resolution and delivery of messages exchanged between publishers and subscribers in resilient, self-configurable, and scalable manners, and security servers that authenticate instances of the middleware and are responsible for the distribution of keys used to secure communications.

The main idea of the C-DAX platform is that, instead of applying host-centric and point-to-point communication, it supports group communication that is data-centric (in that its concepts are developed around the data being communicated) and topic-based (as the routing of data is based on identified topics). In topic-based communication, a topic can be defined as an element of information that sufficiently characterizes a data unit such that platform clients that need to exchange (send or receive) data units are able to identify whether such a data unit is pertinent to them or not. The data units are routed by C-DAX nodes based on the topic that characterizes them. The appropriate C-DAX node for storing a given topic is located using a reliable, secure and scalable location-resolution service that may be centralized or decentralized, thereby eliminating the need for existing name resolution services such as DNS that are known to be exposed to various security threats such as DNS spoofing and DNS poisoning.

1. For C-DAX nodes and high-powered clients, RedHat Enterprise operating system is recommended for commercial distributions and support. In contrast, for low-powered embedded clients, any variant of Linux distributions can be used.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

2. Hardware requirements are application-specific. E.g., if a C-DAX client is an application in a utility DCC, it needs Intel-blade level hardware with one or more 100/1000M Ethernet cards. If PMU data-sharing applications are deployed, C-DAX nodes need similar hardware requirements. However, C-DAX clients running over low-cost embedded devices do not have such requirements.

4.2. General Communication Requirements

1. Various layer 1 (or layer 2) communication solutions such as Ethernet, optical networking, Long Term Evolution (LTE, the 4th generation of the European mobile standard), Power Line Communication (PLC), RF mesh and so on can be used, since our approach as an overlay system is *agnostic to physical connectivity* (as long as the bandwidth, capacity and latency requirements are met by these communication infrastructures). However, for supporting embedding into end field devices such as meters, sensors, PMU, Electric Vehicles (EVs), and Electric Vehicle Supply Equipment (EVSE), C-DAX must consider specific low layer connectivity, for example for the sake of end-to-end QoS (delay) requirement.
2. Also, C-DAX node shall allow for connecting to the clients directly over respective FANs. For that purpose the C-DAX shall support network interfaces corresponding to each of these FAN technologies at the respective Physical (PHY) layer, Medium Access Control (MAC) layer, and Logical Link Control layer (if necessary). While the number of network technologies that may need to be supported will depend on utility networking arrangement, the C-DAX shall support at least the following network interfaces.
    a. PHY and MAC layers for RF mesh such as IEEE 802.15.4g or IEEE 802.11ah
    b. PHY and MAC layers for narrow-band PLCs such as IEEE P1900.2
3. The C-DAX platform communication will take place in overlay to an IP infrastructure. Consequently, all C-DAX components including field devices shall be *IP-addressable*. Note that field devices operated in non-IP networks need to communicate via a gateway function and as a result can be recognized as IP-addressable devices. However, the detailed description of the gateway function is not covered in this document.
4. C-DAX nodes shall allow for connecting to the clients over an Ethernet LAN interface. The connection to the client will be directly over the Ethernet for the clients on that LAN. For clients connected through FAN (or WAN) connections through the router, the Ethernet interface between the C-DAX node and the router will be used. In other words, a functional path is needed between a client and a node.
5. In many instances networking "solutions" are available from networking vendors for collecting data from multiple field devices at a head-end (or a data collector). In that case:
    a. It is sufficient (for the satisfaction of this requirement) that C-DAX provides communication.
    b. C-DAX shall allow to be connected among publishers (i.e., field devices) and subscribers (i.e., head-ends) over an IP network connection.
        i. C-DAX shall maintain mapping between the device IP address and its identifier used by the vendor-specific network solution.
        ii. C-DAX shall support the vendor specific commands for sending data to the subscriber and receiving data from the publisher, or C-DAX will provide a common API such that vendors can inter-operate with C-DAX.
        iii. For a pair of C-DAX publisher-subscriber, the delay objective for message transfer shall include the delay added by all communication entities such as switch/router, network filters, and proxy servers between the pair.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

6. Depending on the client and the underlying application, C-DAX shall support the following corresponding protocols for transfer of a message between the C-DAX node and the client:
    a. TCP is used for communications between C-DAX nodes and high-powered clients with broadband communication channels.
    b. UDP shall be used for communications between C-DAX nodes and low-powered clients (meters or grid-sensors) due to two reasons. First, TCP is inappropriate for supporting large-number of field devices such as meters since C-DAX nodes must keep TCP state per associated field device and as a result it imposes significantly-high memory requirements. Second, the reduced complexity of UDP and UDT-based protocols versus TCP makes them better suited for real time data transfer over low-bandwidth and lossy links such as PLC and RF mesh (IEEE 802.15.14g) that would be dominantly deployed for FANs for utility. However, when working over a lossy link, errors, flow and congestion control will either have to be dealt with, possibly on a higher layer, or have to be explicitly ignored by making an assumption such as, e.g., streaming media that can tolerate packet losses.

4.3. General C-DAX Configuration Requirements

1. In static scenarios, system operators shall configure C-DAX via management interfaces.
2. The need for interworking when C-DAX runs across multiple administrative domains and so works over various middle boxes such as firewalls and NATs, will be addressed in self-configuration / self-organizing scenarios. E.g., the connectivity among C-DAX components should be dynamically managed in terms of routing, load balancing, and security.
3. In dynamic scenarios, service discovery and neighbor discovery across various middle boxes shall be supported across multiple administrative domains.
4. In order to support an efficient overlay routing, load balancing and resiliency, C-DAX shall support *location-awareness* for nodes, clients and stored information. An example for such a mechanism would be the integration of a network coordinates system.

4.4. General Data Management Requirements

1. For a group (subscribers that are subscribed to the same topic), C-DAX shall provide either of data access operations for subscribing clients: streaming-based or query-based. For the former, a subscribing client can continuously receive messages after a one time subscription to the group. In contrast, for the latter, it must send query messages to a C-DAX node that manages the group and then obtains data from the host node.
2. For applications requiring end-to-end security where only traffic aggregation is possible but data fusion or aggregation is impossible, topic-based group communication shall be employed;
3. For applications that want to achieve better communication bandwidth utilization and do not need end-to-end security, content-based group communication where data fusion or aggregation is possible and data from publishers can be "partly" forwarded to each subscriber using "content filter" in C-DAX nodes can be employed. However, high-power C-DAX nodes are required since decryption, filter-matching, and encryption is performed per received message.
4. The groups and their granularity are determined in static and centralized manners due to group security provisioning. For supporting various scenarios flexibly, we need to create and manage groups in a dynamic and distributed manner. However, dynamic group management requires dynamic security handling and traffic management.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

5. For resilient data management, a C-DAX node shall support storing and replication of data in a group that is managed by the host node. Specifically, from the point of view of streaming-based subscribers (i.e., their subscription to a streaming service needs to be stored in a C-DAX node), the failure of their associated C-DAX node is critical. If C-DAX nodes do not store and replicate messages from publishers, they have no way to retrieve messages sent by publishers after failures.
6. For the load balance across C-DAX nodes, intelligent load-balancing schemes involving all the active groups/topics need to be investigated.

4.5. General Security Requirements

4.5.1. Physical Protection

All field devices in C-DAX need be enclosed in hardened cases to ensure that opening the cases is only possible by authorized personnel using special tools. Also, when a field device is opened or moved for any purpose, be it maintenance or theft, the physical event must be detected and reported.

4.5.2. Communication Protection

For ensuring the reliability and safety of C-DAX operations, all communicating nodes (e.g., devices, software modules, and so on) must be *authenticated* and *authorized* in a cryptographic manner before participating in any communicating session. In addition, messages exchanged over communication networks must be *signed* and/or *encrypted* using strong-and-efficient *ciphers* with given *keys*.

Ideally, the C-DAX cloud should be able to provide end-to-end security, by which we mean end-to-end authentication, integrity and end-to-end confidentiality. For some of the use cases only integrity may be important. Here end-to-end authentication means that subscribers can authenticate a message without having to trust the C-DAX infrastructure, except for – unavoidably –having to trust the publisher of that message (who is responsible for authenticating the message and protecting the associated keys) and having to trust the key distribution done by the C-DAX infrastructure (which might also potentially compromise keys). Similarly, end-to-end-confidentiality means that for confidentiality between communicating clients is guaranteed irrespective of any security flaws in the C-DAX infrastructure, again, except for – unavoidably – having to trust key distribution by the C-DAX infrastructure. The importance of end-to-end security is for instance underlined by ISO/IEC Technical Specification TS 62351 (for Power System Management and Associated Information Exchange – Data and Communication Security).

Conceptually, one can consider the provision of integrity and confidentiality as a separate security layer on top of a transport layer that provides the basic publish and subscribe functionality; however, one would still want that in such a transport layer the C-DAX nodes authenticate clients and their data (in order to provide access control) and that the same key management infrastructure is used for this authentication as it is used to ensure the end-to-end authentication.

Ensuring the security objectives discussed above involves:

1. Cryptography for client and node authentication:

   At the beginning of communication phase, each node must once prove itself as a legitimate communicating player. *RSA* method, which is a form of public-key cryptography and has been popularly employed for Internet protocols such as IP Security (IPSec), Secure Sockets Layer (SSL) and Transport Layer Security (TLS), can be considered for the authentication of these use cases. However, it is relatively communication-intensive and computation-intensive; its operations need 100-1000 times computation resources compared with symmetric-key operations, and more importantly public-key certificates required to be exchanged for authentications are not small (typically more than 2K bytes) due to larger key size and digital signature. As a result, over low-band and lossy communication networks, RSA-based authentications may be incomplete or show severely-slow performance. Thus, *pre-shared key-*

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

based authentications that address *tampering-resistance* and *mobility support* (caused by grid-connected EV charging) need to be considered. Still, some caveats for the additional communication and computation overhead for asymmetric crypto should be noted:

- The extra communication overhead for the certificate exchange only has to happen once for each certificate. If these certificates have a long lifetime, the average overhead over time may be minimal. Moreover, this overhead can be avoided altogether if certificates are not distributed over the network, but are pre-installed in the devices as they are rolled out in the field. For instance, a field device could be equipped with the certificate by which it can authenticate instructions from its remote owner.
- The extra computation overhead can be reduced if public-key cryptography is used to establish symmetric sessions which are then used for a period of time, as all session protocols such as IPsec and SSL/TLS do.

2. Ciphers for Message Encryption, Integrity, and Authentication

   During communications, all authenticated nodes shall use ciphers that can ensure message confidentiality and privacy (via encryption), message integrity (against accidental or incidental modification), and message origin authentication (against spoofing). Messages may also need to be equipped with time-stamps or sequence numbers to ensure not just integrity of individual messages, but also the order of messages and the freshness of messages.

   Symmetric-key ciphers typically outperform public-key ciphers in terms of performance and efficiency. Among symmetric-key cipher candidates for C-DAX, AES [1] that has been recommended by NIST due to its security strength must be first considered for the usage. Even though AES Counter mode operation (or Cipher-Block Chain mode) are preferred, choosing a specific AES mode operation required for the use cases is still open due to a broad spectrum of computation constraints of devices in these use cases. Note that commercial general-purpose processors (i.e., Intel Core processor family since 2010) inherently support AES instructions.

   Cryptographic hash functions (or keyed hash functions) need be used to authenticate a message and to detect message tampering and forgery. We recommend to use SHA (Secure Hash Algorithm) published by NIST. Among the four SHA algorithms (i.e., SHA-0, SHA-1, SHA-2, and SHA-3), SHA-1 and SHA-2 are desirable candidates for our usage. Note that although SHA-1 has a theoretical vulnerability [3], it is still much more popular than SHA-2 due to performance overhead and code-accessibility.

3. Key Distribution

   After successful authentication, each authenticated node need to be assigned keys that will be used for message encryption, message integrity, and message source authentication. Key distribution and management must address key-exposure resilience, key-management scalability, and rekeying complexity. We recommend the use of DHKE [4] or ECDH [5] that ensure perfect forward and backward secrecy and show strength against brute-force attacks. Together with these, a group key management scheme like REMP [6] needs to be considered to address the simple key management for massive number of communicating nodes.

4. Key size

   The size of keys must be sufficient to resist known attacks. For example for symmetric-key ciphers (e.g., AES), keys that are at least 128 bits shall be used and 2048 bits long key for public-key ciphers (e.g., RSA). For example in the case of AES, both AES-128 and AES-256 are vulnerable against brute-force attacks. However, the time and memory complexity required to break the ciphers are significantly high. *E.g.,* key-recovery attacks on full AES require $2^{126.1}$ operations and $2^{254.4}$ operations to recover an AES-128 key and an AES-256, respectively [1]. I.e., key recovery attacks against those ciphers are not effective within any meaningful time bound. When deploying keys to field devices, one may be tempted to resort to short keys. However, it is shown in [7, 8] that short keys are seriously vulnerable against brute-force key

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

search attacks. In these papers the authors demonstrated that in field RFID applications short keys such as 40-bits (or 48-bits) encryption keys used for RFID device authentication can be recovered in the order of hours using commodity equipments rather than super computers.

5. Tamper-Resistance, Identification and Credential Protection

   The identity uniquely assigned to each client and each node must be safely protected against forge to avoid spoofing attacks. However, many devices in C-DAX are highly exposed to unauthorized physical access. Hence, we need to employ a forge-proofing identification solution such as smartcard IC that is popularly used by credit card companies and cellular service providers.

   Indeed, direct attacks against messages exchanged over communication networks are difficult. In contrast, tampering attacks after successfully accessing long-term credentials and secrets for authentication and message encryption are highly possible since adversaries can physically access to field devices and so recover long-term secrets in the devices or duplicate the devices. One possible approach to prevent this is to store credentials on tamper-resistant hardware (e.g. a smartcard) such that even with physical access an attacker may not be able to retrieve the credentials and duplicate devices. If credentials are stored in a state-of-the-art smartcard (or some other form of tamper-resistant hardware) then even with physical access an attacker should not be able to retrieve the credentials and then duplicate devices without a disproportionate effort. Still, one concern here is the lifetime of such hardware in the field. Given the constantly evolving arms race between attacks and defenses in hardware security, it is hard to provide guarantees about tamper-resistance in the longer run. For example, many countries choose to issue passports with a lifetime of 5 rather than 10 years because of concerns of the physical security of the passport chips over time.

   As techniques exist to recover keys from tamper-resistant hardware, Physically Un-clonable Functions (PUF, see [10]) may also be investigated as another means to prevent duplication of devices, doing away with traditional keys. The function provided by a PUF can be used for un-forgeable authentication in the same way as a signed hash or digital signature computed by a smartcard. From a key/device management perspective, a difference here is that PUFs need to be enrolled, as the function they provide cannot be configured, whereas a smartcard can be pre-configured with a particular key. A downside is that this may complicate key management. An upside is that exposure of long-term credentials intrinsically provided by a PUF might be theoretically impossible and practically harder than exposure of credentials stored on a smartcard.

   Recommendations for ciphers, key sizes, and protocol variants as discussed above can also be found in the various parts of IEC 62351, which are specifically about power system, and in the more generic guidelines of NIST (detailed in Section 4.6). Whenever possible we would of course follow these recommendations, especially those in IEC 62351. Still, as we are building a new networking solution that is not one of the standard network solutions considered in IEC 62351, we may stick to the spirit of its recommendations rather than the letter. Also, unfortunately some parts of IEC 62351 are still work in progress, notably Part 9 on Key Management.

   Clients can always choose to implement their own ad-hoc security measures on top of the generic security measures provided by C-DAX. In fact, where we draw the line between what we consider as security provided by the C-DAX overlay and what we consider to be additional security implemented by clients themselves is only a matter of definition. Indeed, clients could choose not to trust the C-DAX infrastructure at all and arrange for their only confidentiality and integrity measures independent of what C-DAX provides. However, as stated above, we consider end-to-end integrity and confidentiality generic security objectives provided by the C-DAX infrastructure. For very specific additional security requirements which may arise in the use cases, it is conceptually simpler to consider these as a separate security layer rather than an integral part of C-DAX (in sticking to the principle of separations of concerns). Whether one then considers this as an optional C-DAX layer or a security layer in the clients is then a

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

meaningless distinction. Examples of such security requirements are supporting operations, such as filtering or aggregation on encrypted data (filtering and or aggregation). Of course, in providing such additional security guarantees one would want to reuse as much of the standard C-DAX management infrastructure as possible.

4.5.3. System Protection

In the last subsection, we have been focused on communication/cached message protection and node authentication. For ensuring the reliability and safety of C-DAX operations, server systems used to run C-DAX nodes must be able to minimize service disruption or abnormal operations that can be caused by cyber-attacks or internal system failures. Hence, more comprehensive security considerations are required:

1. All received data must be screened before processing to detect anomalies caused by adversaries, hardware or software errors.
2. Server systems must show resilience against security-threats such as replay attacks, DoS Attacks, and distributed DoS attacks (DDoS) that suddenly consume a huge amount of computation resources and as a result can make C-DAX system slow or service-disrupted.
3. Accessing to C-DAX resources (hardware, software, and stored data) must be strictly controlled in fine-grained role-based manners.
4. For protection against malware or virus that can be intruded via networks, media, or physical access, the use of IDS (Intrusion Detection System) and trusted computing environment such as TPM (Trusted Platform Module) can be considered.

4.6. Cryptographic issues and NIST recommendations

The NIST report identifies several issues related with the application of standard cryptographic schemes and key management to the smart grid systems. It also points out some recommendations for the use of those schemes and highlights several research directions that appear due to the impossibility of adapting the standard schemes to the smart grid scope.

In a nutshell, the design and development of the security architecture of C-DAX have to take into account the peculiarities/issues described next:

- **Limited computational power of the devices:** several devices like current home meters may have limited computational power; one of the solutions would be to include low-cost embedded processors with built-in cryptographic capabilities (e.g. smart cards);
- **Channel bandwidth:** variations in communications bandwidth can be a problem to implement efficient cryptographic schemes in the software systems of the grid; e.g. though symmetric ciphers do not introduce significant overhead in the packages length, increasing the message with MACs in low-bandwidth (slow) channels only used for communicating short messages, might be a problem; current communication architectures of the power grid can have this constrains, since in some cases the messages are exchanged over the power line conductors;
- **Connectivity:** it might be the case that not all the devices of the grid are connected between each other and it might not even be necessary, e.g., current home meters might do not have connectivity to certification authorities (CAs), key servers, etc: so when adopting communication protocols such as SSL/TLS, validation of the certificates has to be done offline; pre-installation of CAs certificates/keys (or any other data) at device's roll out must be taken into consideration;
- **Entropy:** many devices might not have access to sufficient sources of entropy, not generating sufficiently good random keys; including deterministic random bit generators or key derivation functions in some devices, can be a very efficient solution to have access to sufficient entropy and provide good sources of true randomness;

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

- **Cipher suite:** the appropriate cipher suite for the grid must be based on the existing standards (e.g. for block ciphers and operation modes); for instance, the use of elliptic curve cryptography (ECC) in the smart grid infrastructure can be supported by the NSA Suite B, approved by NIST; besides cryptographic software implementations to be used in the grid should be publicly available to be subject of a high-level of scrutiny and test, in order to minimize the possible security flaws (i.e., it is not recommended the implementation of cryptographic software, existing libraries such as OpenSSL and NaCl, should be used instead);
- **Key management issues:** provisioning all the devices with (symmetric) secret keys certainly implies many security vulnerabilities; on the other hand, the use of digital certificates can represent additional costs in distribution and maintenance. Notice that provisioning all the devices with symmetric keys for topic-based communication implies that all the devices publishing/subscribing such topic have to share the same key. Pre-shared keys are a problem to securely distribute and when devices are compromised. Still, PKI-based solutions introduce a huge overhead inherent from certificate generation and revocation, specification of certificate policies, securing the CA responsible for issue the certificates and so on. All these issues must be carefully deliberated when designing and implementing the security architecture of C-DAX to identify which of the existing solutions provide better guarantees for the long run.
- **Devices lifetime:** substitution/upgrade of the cryptographic modules included in the devices have to take into account devices lifetime, e.g. smart meters have a lifetime of 20 years, being extremely important to reason about the way the cryptographic modules are updated before deploying them in the field;
- **Autonomous authentication mechanisms:** authentication mechanisms, especially in Use Cases 1 and 2, must be independent from the connectivity, being possible to operate autonomously. For instance, the occurrence of a power outage must not prevent/impede a system or entity to locally authenticate itself within a substation area.
- **Availability:** availability of some smart grid devices is more important than security, being preferable to simply report the security issue than deny the connection because of a key or certificate expiration, since it can cause interruption of critical communications;
- **Physical protection:** physical protection of critical security parameters and cryptographic modules, must be embodied at the devices; as stated, tamper resistant security modules, hardware security modules and authentication module cards are examples of embedded devices used to provide physical protection;
- **PKI issues:** the use of PKI increases complexity and may introduce difficulties:
    - **High-availability issues:** requiring high-availability of the servers to certificate authentication, symmetric key based credentials, etc, can be a problem. Hence, it is recommended the use of different methodologies such as digital certificates instead of symmetric key-based credentials;
    - **Hardware security modules (HSM):** storing keys in HSM can be costly and worthless, instead, smart cards exhibit additional functionalities (e.g. capable of performing cryptographic operations) and when purchased in large quantities can be very cheap;
    - **Trust management:** define a hierarchy of trust for PKI digital certificates can be a very difficult and costly task within an organization;
    - **Certificates policy:** establishing a policy model for issuing a PKI certificates requires specification of the requirements and definition of liability limits that the PKI is willing to accept.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

5. Use Case 1: RTU/IEDs at Distribution Substations

In this section, C-DAX requirements for Use Case 1 are specified. We begin with a description of the use case.

5.1. Remote Terminal Units

SCADA systems are used by utilities for collecting power grid data (such as measurements of voltages and currents at several points in the substation) at periodic intervals as well as reporting of asynchronous events (alarms) in the grid based on detected faults and for automatically controlling operations of actuating elements such as circuit breakers. For that purpose RTUs are deployed at the substations that communicate with the SCADA Master Control and other systems in the utility DCCs. Substations are evolving to support IEC 61850[4] set of standards [11] that will eventually replace an RTU and associated substation equipment with IEDs.

5.1.1. Description of RTU/IED Operation

Figure 3 is an illustration of the communication required between the RTU and systems in the utility DCC. The elements depicted in the Figure are further described in Table I.

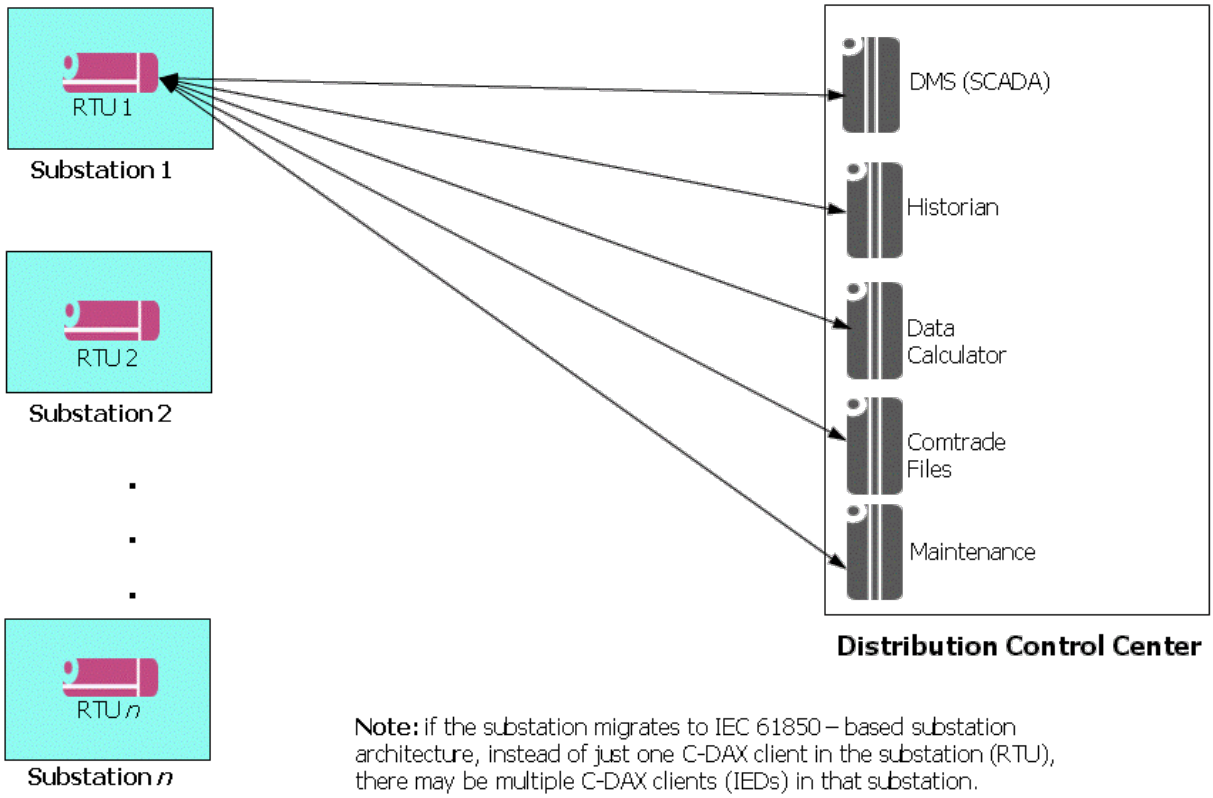

Figure 3: *Reference Architecture for Use Case 1: RTUs at Distribution Substations*

Traditionally, an RTU is responsible for collecting all measurements data and generated events in a substation for forwarding them to the DCC as well as receiving the control signals from the SCADA systems in the DCC and forwarding them to the actuators in the substations, as the case may be.

With the ongoing development of the substation architecture based on the IEC 61850 standards, IEDs are deployed throughout the substation, both for the purpose of collecting measurements, events , and

[4] The IEC standard for the design of electrical substation automation.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

other data from the substation as well as receiving the control signals and other messages from the systems in the DCCs and initiating the corresponding actions. Thus the IEDs are replacing the conventional systems in the substations as well as the RTUs, since the individual IEDs communicate with the SCADA system(s) in the DCC. In that case, instead of just one element (RTU) in the substation, there may be several IEDs (independently communicating with the DCC systems). Note that it is possible that until the time that the migration to the IEC 61850 substation is complete, there may be a mix of substations – some with only an RTU, some with an RTU and one or more IEDs, and the rest with only the IEDs.

5.1.2. Communicating Entities

There can be many different systems in the DCC that communicate with the RTU/IED. While in most cases there are standards for specification of the contents of the messages between an RTU/IED and a system as well as for communication between them, in some cases, it may be necessary to use proprietary formats for contents of the messages and for message transfer for certain function. For Use Case 1, we assume that there are five different DCC systems that communicate with the RTU/IED as shown in Figure 11 in Appendix A. Note that one or more of these systems may be collocated in a single server.

The clients for Use Case 1 are described in Table II.

Table II: *Clients in Use Case 1: RTU/IEDs at distribution substations*

Client	Description
RTU/IED	One RTU per substation communicates with the DCC systems. In substations developed based on IEC 61850 standards, there is no RTU but there may be more than one IED at the substation
SCADA (DMS)	SCADA master control system, often residing in the utility Distribution Management system (DMS) uses standards protocol such as DNP3 or IEC 61850 protocols for communicating with RTU/IED. IEC 60870-5-104 [12] provides specifications for communication functions between the RTU/IED and the SCADA master control.
Historian	Records and maintains historical database of the SCADA measurements from RTU/IED for data analysis, trending, record-keeping and other purposes. We assume that an RTU/IED sends data to the Historian *separately* from and in addition to the data sent to the SCADA (DMS), even if the content of the messages sent to these two systems is the same.
Data Calculator	Computes in real-time, required grid information based on the data received from the RTU/IED. We assume that an RTU sends data to the Data Calculator *separately* and in addition to the data sent to the SCADA (DMS), even if the contents of the messages sent to these two systems are the same,
COMTRADE	Maintains data files for the types of fault, tests, or simulation data for electrical power systems using the IEEE C37.111 standard [13] for formats and interchange of such files. An example is power quality measurements based on the EN 50160 [14] of the IEEE 1159 standards [15]
RTU/IED Maintenance	Provides vendor proprietary communication for maintenance of the RTU/IEDs based on proprietary protocols and RTU/IED configuration, firmware/software upgrade, and other functions for the maintenance of RTU/IEDs

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

5.2. Assumptions: Use Case 1: RTU/IEDs at Distribution Substations

1. It is assumed that there is one primary DCC by default. If there is a backup DCC, it is assumed that the backup DCC will receive all messages from the C-DAX that the primary control receives. All messages received from the backup DCC will be sent to the appropriate RTU/IEDs. Further, all functions and requirements related to a system client in DCC is applicable the same system in both the primary and backup DCCs.
2. It is assumed that the utility and C-DAX administration have agreed on mapping of messages between the entities in a substation and an entity in the DCC to topics specified in the requirements.

5.3. Requirements: Use Case 1: RTU/IEDs at Distribution Substations

5.3.1. C-DAX Clients

A schematic of the C-DAX clients' communication with the C-DAX is shown in Figure 4.

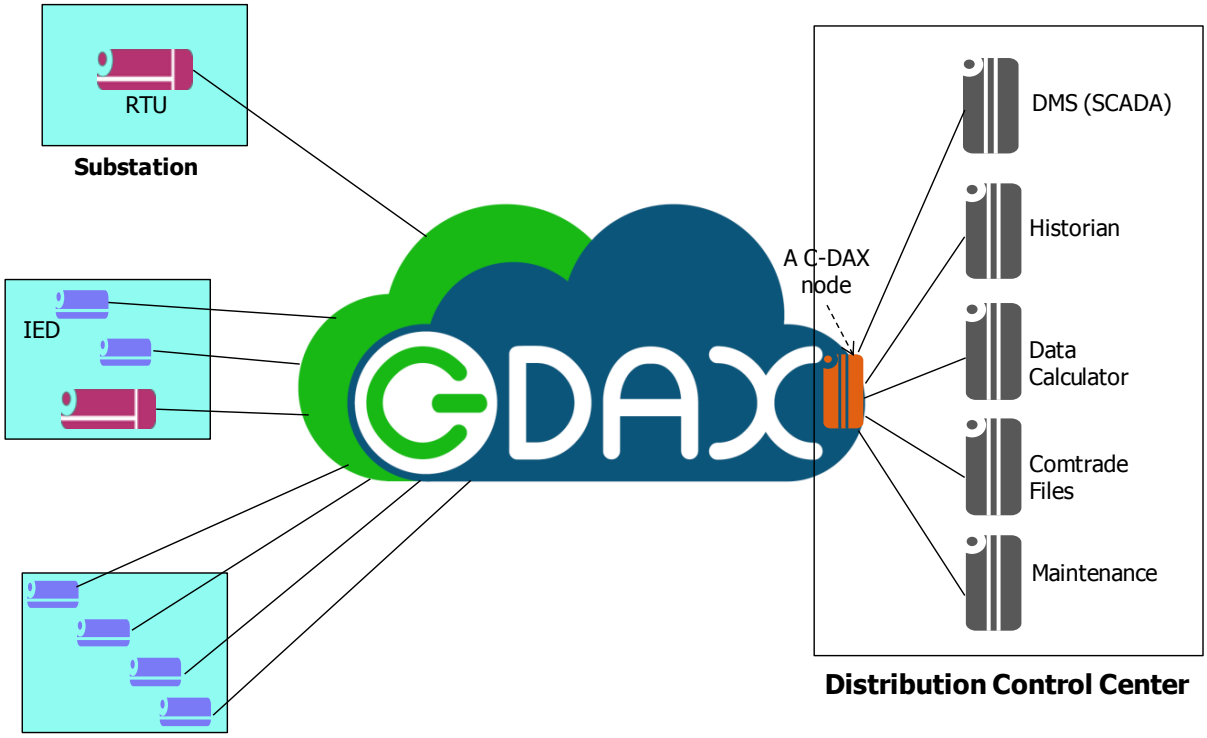

Figure 4: *Communication between C-DAX Clients and C-DAX cloud and nodes*

1. Since there are multiple entities at the DCC that communicate with all substations, it is recommended (*but not required*) that a C-DAX node be located at the DCC connecting to the clients in the DCC. These connections may be carried over a LAN. Such placement of a C-DAX node at the DCC will help maintain the delay requirements for high priority messages to/from a DCC server;
2. If there exists more than one RTU/IEDs at a substation the communication between an IED/RTU may be carried through a substation router (Figure 13 in Annex B) or a *data concentrator* located at the substation;
3. C-DAX shall support communicating with C-DAX clients in Table II. Communication links between the clients and C-DAX are shown in Figure 4;

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

4. C-DAX has to support the minimum number of clients of each type as given in Table III to properly support use case 1.

Table III: *Minimum number of clients to be supported by C-DAX for use case 1*

Entity	**Number**
DCC	2 (one primary and the other secondary)
Substations	500
Substations migrated to IEC 61850	50%
RTU in each substation	1
IEDs	6 (average number of IEDs in a substation)

5. All clients shall be allowed to be both publishers and subscriber for any topic for which they are registered with C-DAX (i.e. being publisher or subscriber for any given topic is not mutually exclusive).
6. Each client instance registered with C-DAX shall be uniquely identified by the C-DAX cloud.
    a. Indeed, it is possible that a client instance may de-register with C-DAX, re-register at a later time and in the mean time new client instances may register. Therefore, sufficient number of bits shall be allocated to the integer field of the client identifier to maintain uniqueness of the identifiers over a long period of time. For example a client identifier may be structured as a character string concatenating the client name (or abbreviation thereof) and a number.
    b. At any time there can be only one registered instance of each client in a DCC.

5.3.2. Topics

Note that all point-to-point communication is between a client in a substation and a client in the DCC. There are many types of messages exchanged between the two clients at the end of the communication, see [12] for the description of many of these messages. While the contents of these messages are transparent to C-DAX, C-DAX must be aware of the priorities and QoS required for these messages to take the corresponding appropriate action.

Here are examples of priorities for some of the messages:

High priority: Measurements and events (alarms) from RTU/IED to systems in the DCC and polls and control signals from systems in the DCC to RTU/IED

Medium priority: Other critical messages between RTU/IED and systems in the DCC

Low Priority: All other messages (*e.g.,* file transfer, software/firmware updates and maintenance messages)

Note that the topic definition *does not* depend on any individual RTU or IED or on any individual system in the DCC.

1. C-DAX shall support the topics as defined in Table IV

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Table IV: *Necessary topics supported by C-DAX for* Use Case 1

Topic Description	Proposed Abbreviation	Publisher Client*	Subscriber Client*	Priority	Client-Client Delay Objective (maximum)
High priority messages from RTU/IED to systems in DCC.	**From_SS_H**	RTU/IED	System in DCC	High (25-35)	100 ms
Medium priority messages from RTU/IED to systems in DCC.	**From_SS_M**	RTU/IED	System in DCC	Medium (36-50)	200 ms
Low priority messages from RTU/IED to systems in DCC.	**From_SS_L**	RTU/IED	System in DCC	Low (>70)	1000 ms
High priority messages from systems in DCC to RTU/IED.	**From_DCC_H**	System(s) in DCC	RTU/IED	High (25-35)	100 ms
Medium priority messages from systems in DCC to RTU/IED	**from_DCC_M**	System(s) in DCC	RTU/IED	Medium (36-50)	200 ms
Low priority messages from systems in DCC to RTU/IED.	**From_DCC_L**	System(s) in DCC	RTU/IED	Low (>70)	1000 ms

* The actual publisher or subscriber DCC systems clients will depend on the specific topics that are published or subscribed to.

The relative priority numbers and the delay objective values in Table IV are consistent with Table XII in Appendix C, where priorities and delay objectives are presented for traffic for a large number of smart grid and utility applications carried over an integrated IP network. Note that the traffic priority decreases as the relative priority number increases.

2. For each received message from a client, the C-DAX shall read values of the following fields in that message: topic identified (ID) and timestamp.
3. The C-DAX shall store each received message[5].
4. Upon receiving of a message, the C-DAX shall schedule transmission of that received message over the designated route for that destination client.
   In the message queue, if there is any message whose priority (see Table IV) is lower (*i.e.* priority numeric value higher in Table IV), then the C-DAX shall place this newly scheduled message ahead all messages in the message queue with lower priorities. Note that a message is considered to have left the queue if the transmission of that message has already begun on that port. Thus no preemption of any message is allowed.

[5] There is a limited time period for which the data topic is made available in C-DAX, after which point depending on the type of data it is sent for archival and flushed from the C-DAX node.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

6. Use Case 2: Pervasive Synchrophasor Deployment at MV Level

While RTUs/IEDs in the substation (as described in Use Case 1) and other grid measurements such as for power quality have been in use for many years, the deployment of PMUs is becoming increasingly important due to DER installations characterized by rated power in the range between 0.1 to 1 MW that are directly connected to the distribution grid at the MV level. They include DERs in the (multi-dwelling) microgrids.

The wide-spread deployment of PMUs throughout the distribution grid has potential to markedly improved distribution grid observability with voltage and current phasor measurements together with frequency and frequency variation measurements. The deployment of PMUs in the distribution grid is still in its infancy, but some utilities are planning to deploy them in the distribution grid.

6.1. Synchrophasors

Synchrophasors are PMUs that collect phasor frequency measurements and send them out with a timestamp synchronized to a clock derived from GPS to the PDC.

6.1.1. Description of Synchrophasor Operation

Each PMU sends measurements every 10, 25, or 50 times per second based on the PMU configuration required by the utility deployment[6]. In addition to the timestamp, each measurement message from the PMU to the PDC includes the voltage and current phasors (amplitudes and angles), frequency, and frequency variation. IEEE C37.118.1 [17] specifies the synchrophasor measurements while IEEE C37.118.2 standard [18] specifies the communication between the PMU and PDC including the message format.

PMUs are deployed along the MV feeders and the PDCs are often located at the distribution substation, as shown in Figure 5.

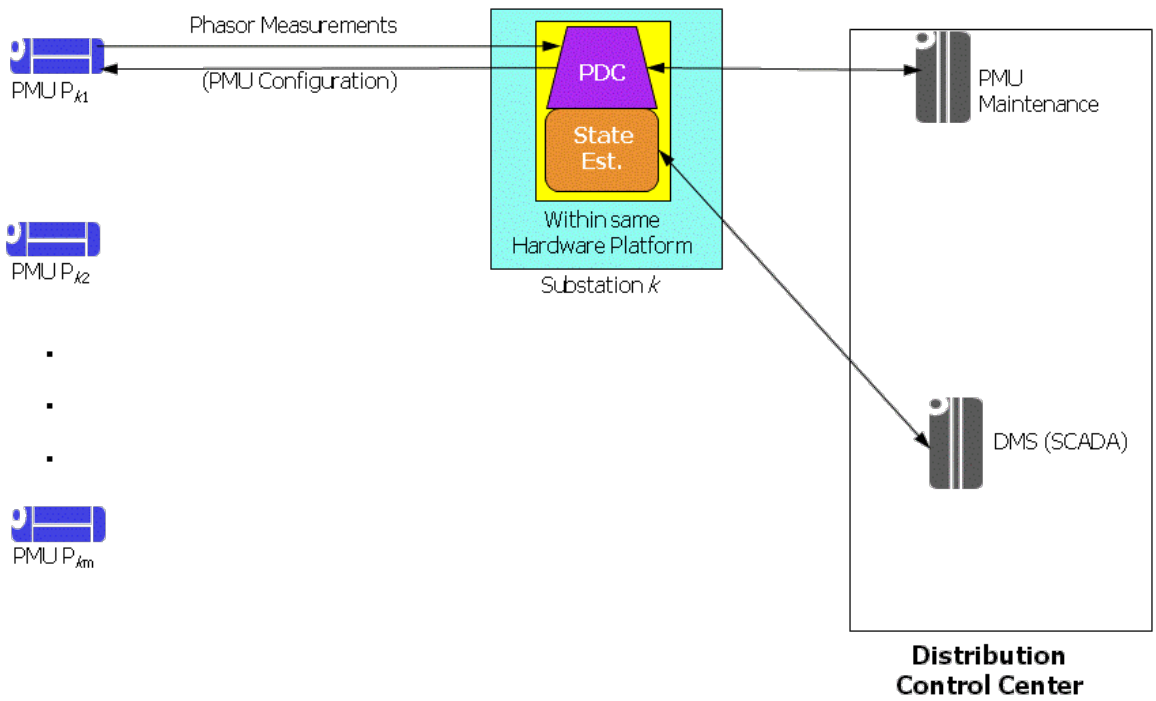

Figure 5: *Reference architecture for Use Case 2: Pervasive Synchrophasor Deployment*

[6] For PMU deployment in the US, Canada, and other countries with 60 Hz as line frequency: 10, 12, 20, 24, 30, 60 times per second

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Note that each PMU on a feeder communicates only with the PDC that is located at the substation that supports that feeder. The PMU measurements received at the PDC are used for state estimation to help in fault detection, voltage control, and other distribution system functions including set point control of the DER for accurate management of power flows in the presence of DERs like wind power and PV with large variability is their power outputs.

Phasor measurements with very high frequency provide accuracy required for these functions. For real time processing of the PMU data, it is necessary that there is minimal delay between processing of two successive sets of measurements from the PMUs at the state estimator (SE). The delay of not more than one time interval between phasor measurements is required (*i.e.* 20 ms for the measurement frequency of 50 times per second[7]). Note that the "measurement interval" here denotes the interval between two successive transmissions of PMU data. A PMU may sample the voltages, currents and other quantities at a very higher frequency. Therefore the communication delay between the PMU and PDC should be even much smaller (5-15 ms, typically 8 ms) to allow addition time for data accumulation at the PMUs and for SE. To avoid additional network delay between the PDC and the SE, these two systems are collocated within the same server at the substation as shown in Figure 5.

6.1.2. C-DAX Clients

Clients for Use Case 2 are described in **Table V**.

Table V: *Clients of Use Case 2: Pervasive Synchrophasor Deployment*

Client	Description
PMU	Collects and sends out phasor measurements t and timestamp of measurements every 10, 25, or 50 times a second to the PDC
PDC+SE	From the C-DAX perspective, we include the PDC and SE functions in the same client called PDC+SE.
SCADA (DMS)	In addition to the PMU measurement data, the state estimator may use data from other data sources from the field such as from the power quality measurement sensors. It is assumed that the SE system receives these measurements through the SCADA (DMS) system[8]. Based on the results of state estimation, the estimator may send events (such as detected faults, voltage control, *etc.*) to the SCADA system, so that the DMS can take the necessary actions.
PMU_Maint_System	The PMU maintenance system communicates with the PDC for sending changes in the grid topology, maintenance of the PMUs, firmware//software upgrades, and other management functions. The PDC may send the PMU configuration changes and firmware/software upgrades to the PMUs as required.

6.2. Assumptions: Use Case 2: Pervasive Synchrophasor Deployment

1. It is assumed that PDC and SE functions are collocated in the same server.
2. It is assumed that SE receives field data (such as power quality measurements) through SCADA (DMS) rather than directly from the measurement sensors[8].
3. It is assumed that the DNO and C-DAX administration have agreed on mapping of messages to topics specified in the requirements.

[7] For PMU deployment in the US, Canada, and other countries with 60 Hz as line frequency: 60 times per second.

[8] I.e., SCADA data will be a separate topic on C-DAX with a higher level of security.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

6.3. Requirements: Use Case 2: Pervasive Synchrophasor Deployment

6.3.1. C-DAX Clients

A schematic of the C-DAX clients' communication with the C-DAX is shown in Figure 6.

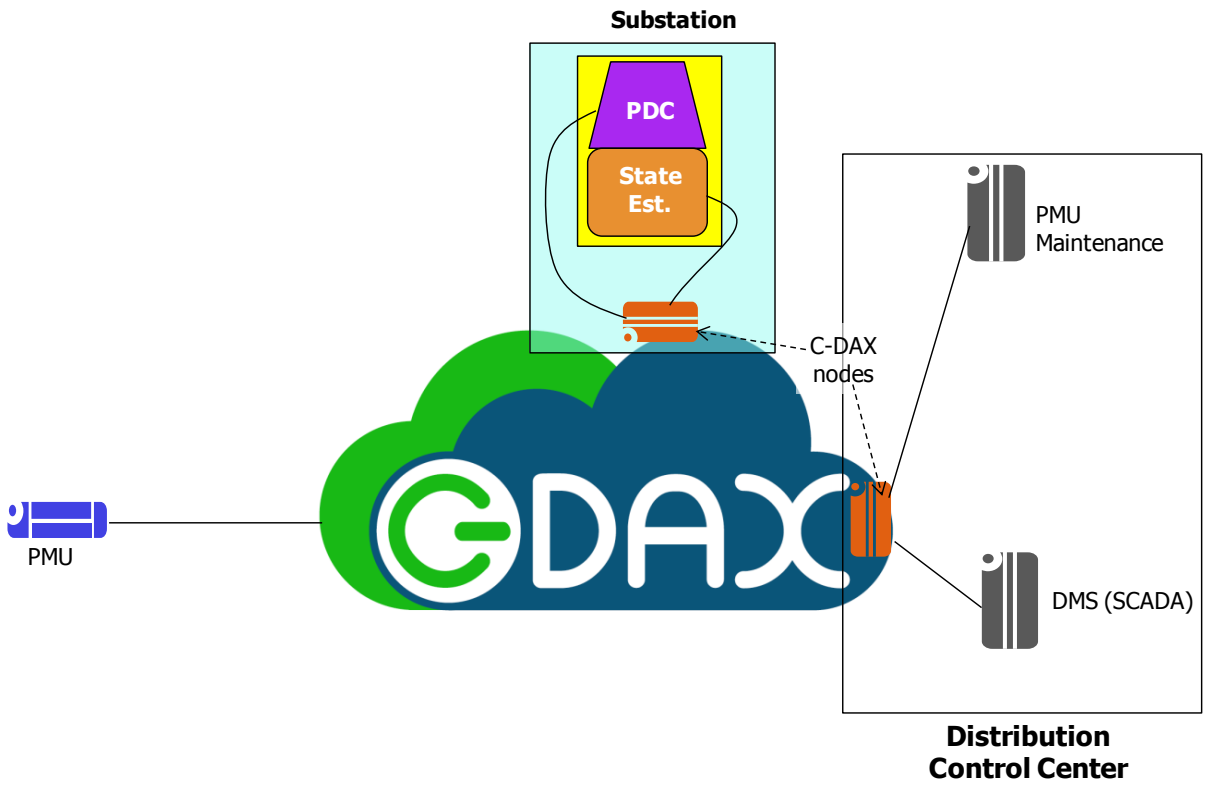

Figure 6: *Communication between C-DAX clients and C-DAX cloud and nodes*

1. Since there are multiple servers at the DCC, it may be recommended (*but not required*) that a C-DAX node is located at the DCC connecting to the clients in the DCC. These connections may be carried over a LAN. Such placement of a C-DAX node at the DCC will help maintain the delay requirements for high priority messages to/from a DCC server.
2. The delay requirement for PMU measurement data between a PMU and the PDC at the substation is extremely small (8 ms), such that it is imperative that a C-DAX node be located at each substation connected to the PDC/SE system over a LAN.
3. C-DAX shall support communicating with C-DAX clients in Table V. Communication links between the clients and C-DAX are shown in Figure 6.
4. C-DAX has to support the minimum number of clients of each type as given in Table VI to properly support use case 2.

Table VI: *Minimum number of clients that have to be supported by C-DAX for use case 2*

Entity	**Number**
DCC	2 (one primary and the other secondary)
Substations	500
Average number of PMUs supported by the PDC at a substation (over multiple feeders from the substation). It is expected that the number of PMUs will be about half the number of distribution transformers on these	60

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Entity	**Number**
feeders	

5. All clients shall be allowed to be both publishers and subscriber for any topic for which they are registered with C-DAX (i.e. being publisher or subscriber for any given topic is not mutually exclusive).
6. Each client instance registered with C-DAX shall be uniquely identified by the C-DAX cloud.
    a. Indeed, it is possible that a client instance may de-register with C-DAX, re-register at a later time and in the mean time new client instances may register. Therefore, sufficient number of bits shall be allocated to the integer field of the client identifier to maintain uniqueness of the identifiers over a long period of time. For example a client identifier may be structured as a character string concatenating the client name (or abbreviation thereof) and a number.
    b. At any time, there can be only one registered instance of each client in a DCC.

6.3.2. Topics

Point-to-point communication is between clients as obvious from Figure 6.

Here are examples of the priorities of some of the messages:

1. C-DAX shall support the topics as defined inTable VII.

Table VII: *Necessary topics supported by C-DAX for use case 2: pervasive synchrophasor deployment*

Topic	**Proposed Abbreviation**	**Publisher Client**	**Subscriber Client**	**Priority**	**Client-Client Delay Objective (maximum)**
PMU Measurement	**PMU_Meas**	PMU	PDC+SE	Very High (10)	8 ms
PMU configuration, PMU firmware/software upgrade, and all other messages from PDC+SE *to* PMU	**to_PMU**	PDC+SE	PMU	Low (>70)	1000 ms
All PMU Maintenance messages	**PMU_Maint**	PMU_Maint_Sys	PDC+SE	Low (>70)	1000 ms
All events generated by the State Estimator	**SE_Event**	PDC+SE	SCADA (DMS)	High (25-35)	100 ms
Measurements and events in the grid originating from other than PMUs	**Other_Meas**	SCADA (DMS)	PDC+SE	High (25-35)	100 ms

The relative priority numbers and delay objective values inTable VII are consistent with Table XII in Appendix C, where priorities and delay objectives were presented for traffic for

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

a large number of smart grid and other utility applications carried over an integrated IP network. Note that traffic priority decreases as the relative priority number increases.

2. For each received message from a client, the C-DAX cloud shall read the values of the following fields of that message: topic identifier (ID) and timestamp.
3. The C-DAX shall store each received message[9].
4. Upon receiving of a message, the C-DAX shall schedule transmission of that received message over the designated route for that destination actor.
   In the message queue, if there is any message whose priority (see Table VII) is lower (*i.e.,* priority numeric value higher in Table VII), then the C-DAX shall place this newly schedule message ahead all messages in the message queue with lower priorities. Note that a message is considered to have left the queue if the transmission of that message has already begun on that port. Thus no preemption of any message is allowed.

[9] There is a limited time period for which the data topic is made available in C-DAX, after which point depending on the type of data it is sent for archival and flushed from the C-DAX node.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

7. Use Case 3: Retail Energy Transactions

Retail Energy Transactions (RETs) are the transactions between consumers of energy and suppliers of energy in the *Retail Energy Markets* (REMs). It is worth noting that a so-called *Retailer*, buys electrical energy on wholesale markets (WMs) and resells it through a retail market to consumers not participating to the WMs. Distribution network operators typical *Retailers*. Large consumers buy electrical energy through WM whilst small consumers buy electrical energy through REM directly or from the Retailer to which they are connected. A general scheme of the difference between the WM and the REM is reported in Fig. 1

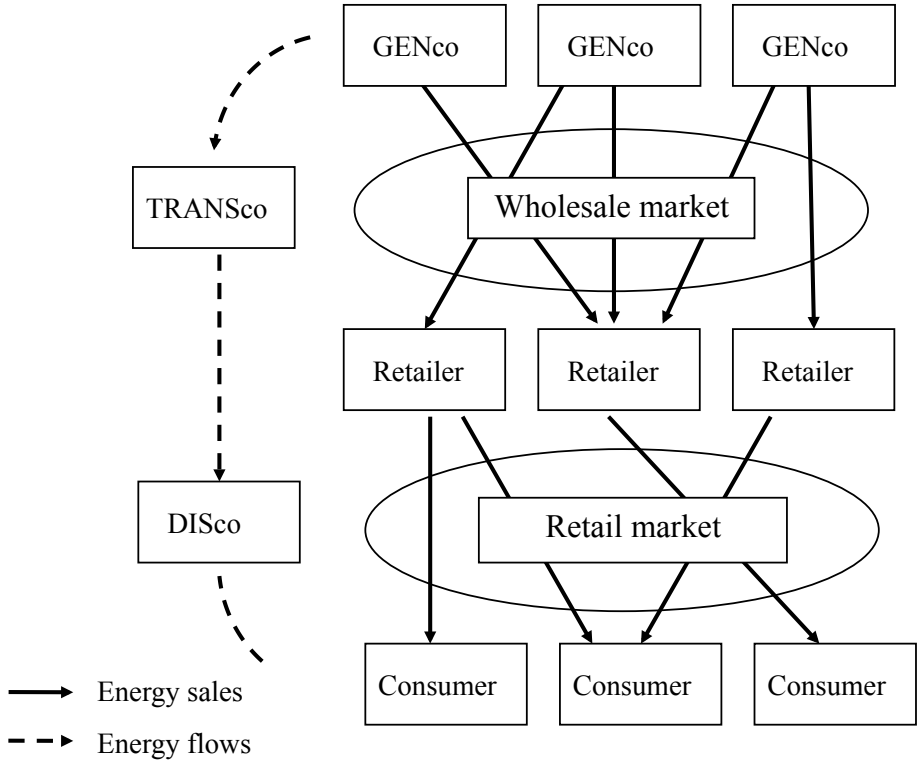

Figure 7: *Energy sales and energy flows in REMs vs WMs (GENco – Generation Company, TRANSco – Transmission Company).*

These transactions may have several forms, ranging from the matching of consumers' demand requests with supply offers, to pricing negotiations for Demand Response (DR), and from the itemized billing and settlement for individual consumers to transactions for power rebalancing. Here we select only a subset of these transaction types, in the form of specific application scenarios, with the purpose of revealing the basic challenges emerging in the context of REMs that need to be addressed by the C-DAX architecture, while preserving the simplicity and focus of the use case framework.

The basic concept behind the selected application scenarios of Use Case 3 is to focus on the support of an extremely high number of energy transactions between the participating actors. The challenge stems from the volume of distinct DERs and consumers, their geographical distribution and the dynamic character of both power generation and consumption with respect to weather conditions, location of consumers, etc. In the following, we elaborate on the details of these application scenarios, in order to precisely define the set of requirements to be fulfilled by the C-DAX architecture. In this effort, we also take into account the work carried out by the CEN, CENELEC and ETSI standardization bodies, as a response to the M/490 mandate in which the European Commission requested the collection, analysis and harmonization of use cases as well as the establishment of a UCM process [21]. Wherever applicable, we provide a mapping between the foreseen application scenarios in the context of C-DAX and use cases described in [21] (the UCM document).

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

7.1. Actors

There are six classes of primary REM participants who are considered to be actively engaged in RET:

1. **Consumers (cnsmr):** These are the consumers who receive energy from energy providers, including from the utility. These may be residential or business/industrial consumers. For this class of consumers, it is assumed that the local energy production (if any) is not sufficient for the consumer to offer the (excess) energy for sale.

   It is noted that every customer need not be a REM participant. Some customers may be completely satisfied in the traditional arrangement with the utility for their electric energy demand satisfied by the utility.

2. **Prosumers (pro):** These are consumers that also act as providers of energy to the grid. In the most typical case, prosumers have the capability of consuming and producing energy at the same time. In general, the two in/out electrical power flows are uncorrelated and two different tariffs are applied. In addition to individual residential, business, and industrial consumers with local energy production, microgrids, large buildings of multiple dwellings and local generation, and campuses with local generation are examples of prosumers. Electric Vehicles (EVs) can also take the role of prosumers, by providing their stored energy to the grid while plugged in a charging station (or at home). Their differences against other types of consumers can be summarized as follows:

   a. Mobility. EVs are not continuously connected to the power grid; their point of attachment to the power grid may change.

   b. Volume. A large number of EVs is expected to emerge in the future (e.g., 1,000,000 EVs within the area of an average size distribution grid), considerably larger than the corresponding number of other types of prosumers.

   c. Authority. Typically, each EV is expected to be operated and controlled by a different entity.

   The consumer aspects of a prosumer shall be denoted with **pro-c**, while the provider aspects with **pro-d**.

3. **Stand-Alone DER (sader):** These establishments are in the business of generation large amount of electricity for selling it to the grid. They differ from the bulk energy suppliers in their choice of energy sources and volume of energy produced. Wind turbines or wind farms, photovoltaics, small-hydro turbines and heat pumps are examples of stand-alone DERs.

4. **The Grid:** The grid itself must participate – through its Energy Supply Manager (**esm**) – in the REM. The utility is responsible for energy transfer. The grid also participates through its Distribution Manager (**dm)** entity, responsible for the management of the grid e.g., delivering power to a certain location.

5. **Aggregator (aggr):** A central entity for the support of RETs. Its role is to mediate between energy providers and consumers in order to facilitate the matching of demand and supply. This may include functions such as the aggregation of requests and/or offers, over a certain area and/or time (we elaborate on this in the following). We will assume that the Aggregator is an independent authority, though it may be possible that the Aggregator function is established by the utility.

6. **Regulator (reg):** An independent authority that determines or approves the electricity market rule, monitors retail transactions so as to ensure compliance with regulations and rules e.g., investigates the suspect cases of abuse (market power), and sets or controls the prices of products and services in the case of monopolies.

Figure 8 illustrates the concept of the REM.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

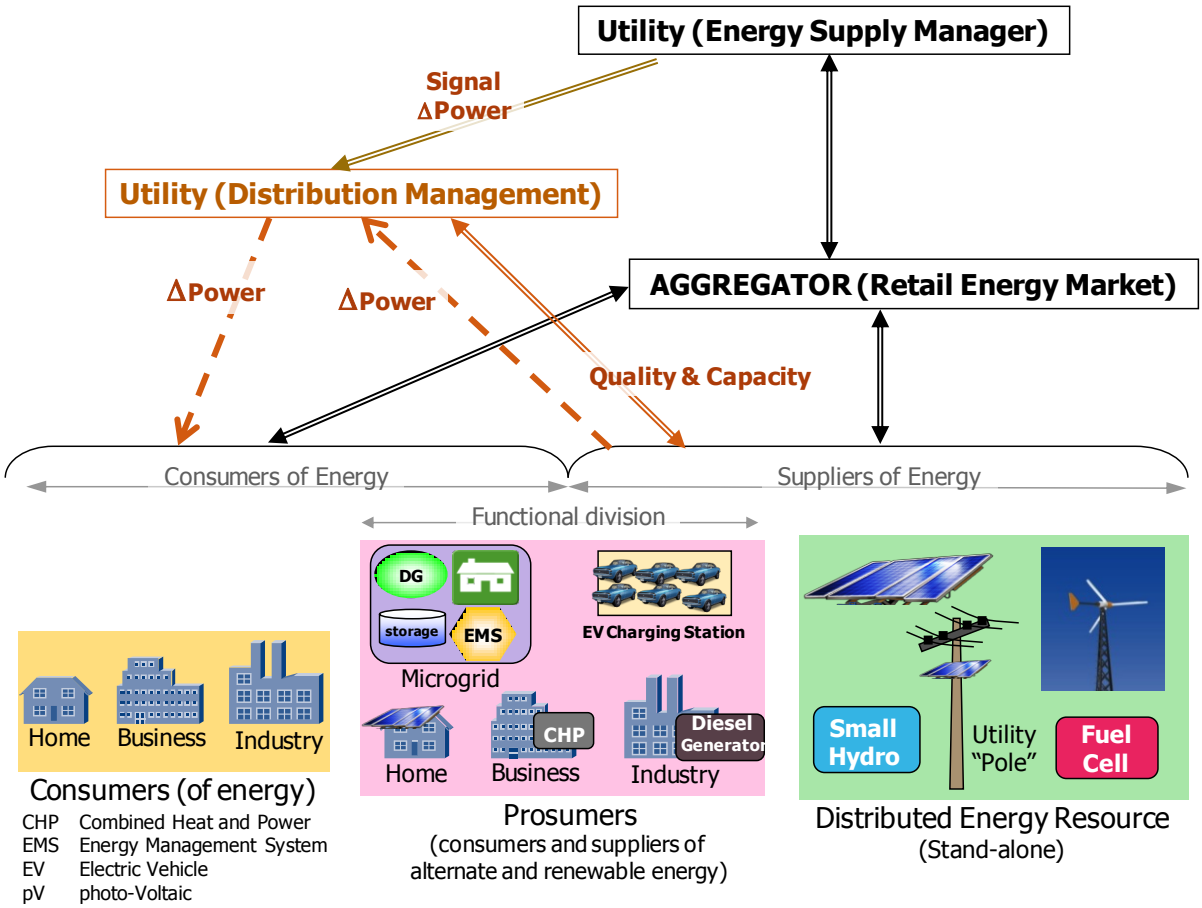

Figure 8: *An Illustration of a Retail Energy Market*

7.2. Application scenarios

A series of application scenarios can be identified in the broad context of REMs. However, C-DAX shall only provide support for a well-defined subset of these scenarios. Namely, the application scenarios described in the following sub-sections.

Note: in all the following scenarios, established agreements for the provision of energy are realized through control plane signaling in the power grid domain (e.g., control signals sent to actuators such as breakers) between **cnsmr**, **proc-c/d**, **esm** and **sader** entities and the **dm**.

7.2.1. Demand Response (Application Scenario I)

In this application scenario, focus is on the support of the communication needs for the realization of *Demand Response*.

7.2.1.1 Actors

The participating entities in this application scenario are the *Consumers* (along with the consumer functionality of *prosumers)*, the ESM and the Regulator.

7.2.1.2 Scope and Objectives

As demand may vary significantly through time, due, for example, to weather conditions, DNOs often face excessive costs in their effort to accommodate particularly high (peak) demands. This is because these peaks are usually served by stand-by energy providers with high operating costs. In the case of Demand Response, DNOs utilize pricing as a mechanism for shaping peak energy demand, giving incentives to consumers to reduce (or even increase in cases of excessive energy supply) their

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

consumption. In some cases, this mechanism can also be used to deploy grid ancillary services (e.g., voltage support, frequency regulation, load shedding in case of grid operation in emergency conditions etc.). In the opposite direction, consumers may also communicate their demand along with the price they are willing to pay in order to be accommodated. As a result, a negotiation mechanism is established between the DNO (the ESM in particular) and the consumers.

7.2.1.3 Communication scenario

We consider the following simple communication scenario for the realization of DR:

a. The ESM collects information regarding the energy consumption across the distribution network. This information is provided by devices at the consumer premises. Based on the collected information, the ESM anticipates the energy demand in the distribution network and can reason on the energy levels it shall be able to support.

b. Utilizing the collected information, the ESM provides the consumers with *supply offers* containing pricing information, with the purpose of shaping their demand for energy.

c. Consumers may reply with *demand requests* denoting their requirements possibly along with pricing information, thus engaging in a negotiation process with the ESM. The entire process may take several forms i.e., the ESM may provide offers that consumers either accept or reject, (large) consumers may provide demand requests denoting the reduction in the requested load and the corresponding requested value, which the ESM may accept of reject, or both parties may exchange supply/demand offers/requests.

d. The negotiation process continues until an agreement is reached or the maximum number of bids has been reached (i.e., no agreement was reached).

e. The Regulator supervises the entire process in order to ensure that pricing policies comply with energy market rules. To this end the Regulator is informed about the outcome of each negotiation process (*Power Transaction Plan*) by both parties (ESM and consumers) and provides a *response* validating (or not) the negotiation outcome. The Power Transaction Plan provides information about the amount of energy to be transferred, the location of the producer(s) and the consumer(s) and the duration of the transfer.

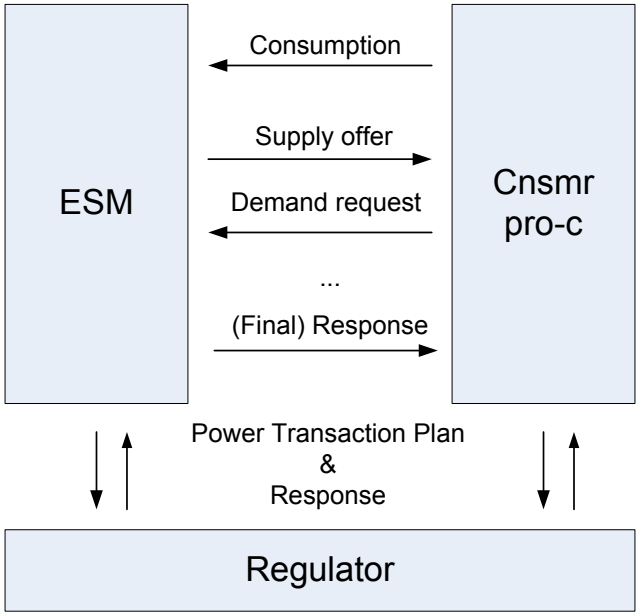

Figure 9: *Demand Response communication overview*

7.2.1.4 Relation to UCM document

This application scenario reflects some of the use cases in the UCM document and in particular those under the Generic High Level Use Case: *Receiving consumption, price or environmental information*

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

for further action by consumer or a local energy management system (WGSP-2110). More specifically, it covers the following use cases:

- Exchange information regarding power consumption or generation (WG-SP-2111)
- Exchange price and/or environmental information (WG-SP-2112)

7.2.2. Flexibility offerings (Application Scenario II)

In this application scenario, focus is on the support for matching energy demand with supply.

7.2.2.1 Actors

The participating entities in this application scenario are the *Consumers* (along with the consumer functionality of *prosumers* and possibly the ESM), Stand-Alone DERs (along with the provider functionality of *prosumers)* and the Aggregator.

7.2.2.2 Scope and Objectives

Our focus in this scenario is on the impact of the expected explosive growth of Distributed Energy Resources (DER) connected into the grid. Often located at the consumer locations, there may be thousands, even hundreds of thousands of energy providers connected into the grid as compared to the much smaller number of bulk generation providers. The owners of these DER facilities shall sell this energy to consumers. In cases of renewable resources, the actual availability of energy may significantly vary through time, due to external conditions (e.g., weather). Note that in addition to the *stand-alone DER* establishments, DERs may also be located and operated by consumers who may want to sell excess energy (i.e., prosumers). Since a prosumer may sell energy in excess of its needs; the availability of energy may vary subject to consumption.

Our target in this application scenario is to enable the matching of power demand and supply, while taking into account this highly dynamic, inherently distributed and large scale communication environment.

7.2.2.3 Communication scenario

Consumers and SADERS denote their demand and supply. On the consumer side, requests are submitted denoting the required amount of energy. On the SADER side, offers are submitted denoting the available amount of energy. Both requests and offers further contain information regarding the duration of the described energy demand/supply, the location of the corresponding entity in the distribution grid and possibly some pricing information[10].

The role of the Aggregator is to mediate between the two parties with the purpose of matching the expressed demand and supply. This matching refers to the amount of energy offered and requested taking into account the timing, location and pricing restrictions. In this process, the Aggregator may appear to consumers as an energy provider, and to SADERs as a consumer, resulting in the formation of a two-sided market. In order to facilitate matching of demand and supply, the Aggregator may combine demand requests and/or supply offers by multiple consumers and/or providers, respectively e.g., the total amount of energy requested by a set of consumers is aggregated so as to be served by a single supply offer.

We consider the following simple communication scenario between the clients for buying and selling the energy:

a. A buyer (consumer, prosumer, or the Energy Supply Manager – ESM) sends an energy *demand request* to the Aggregator. Each demand request is independent of another demand request as well as it is independent of any energy bids (offers) received from the sellers (prosumers or stand-alone DERs).

[10] This information may express the price ranges acceptable by consumers and the offered prices by the SADERs, and may enable negotiations similar to that of Application Scenario I. However, we defer this aspect for the hybrid Application Scenario III.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

i. In cases of sudden energy availability (e.g., following sudden wind strength peaks), the Aggregator may explicitly *poll* energy demand requests from consumers possibly offering lower prices in order to allow for this energy to be consumed.

b. A seller (prosumer of the stand-alone DER) sends a *supply offer* for available power for sale to the Aggregator. Each offer is independent of each other as well as independent of any demands received from the buyers (consumer, prosumer, or the ESM).

   i. In cases of sudden demand peaks, the Aggregator may explicitly *poll* energy offers from providers to accommodate the corresponding urgent demand requests of the ESM.

c. The Aggregator responds to the buyer with a *supply offer*, accepting the demand request, possibly with changed parameter values from the ones in the demand request, or rejects the demand. For example, the Aggregator may offer less power than requested and/or for less duration than requested.

   a. For every offer made to a buyer, the Aggregator must verify that it can be implemented by the DNO i.e., the offered energy can be transferred to the buyer premises without overloading the distribution network. For this purpose the Aggregator verifies the feasibility of a *power transaction plan* which describes the transaction to be completed in the context of a specific supply offer.

d. The Aggregator responds to the seller with a *demand offer*, accepting the bid to sell, but possibly with changes in parameter values from the ones in the demand request, or rejects the bid. For example, the Aggregator may reduce the power level or the duration for which it will be used.

e. The buyer either accepts the counter offer from the Aggregator or rejects it.

f. The seller either accepts the counter offer from the Aggregator or rejects it.

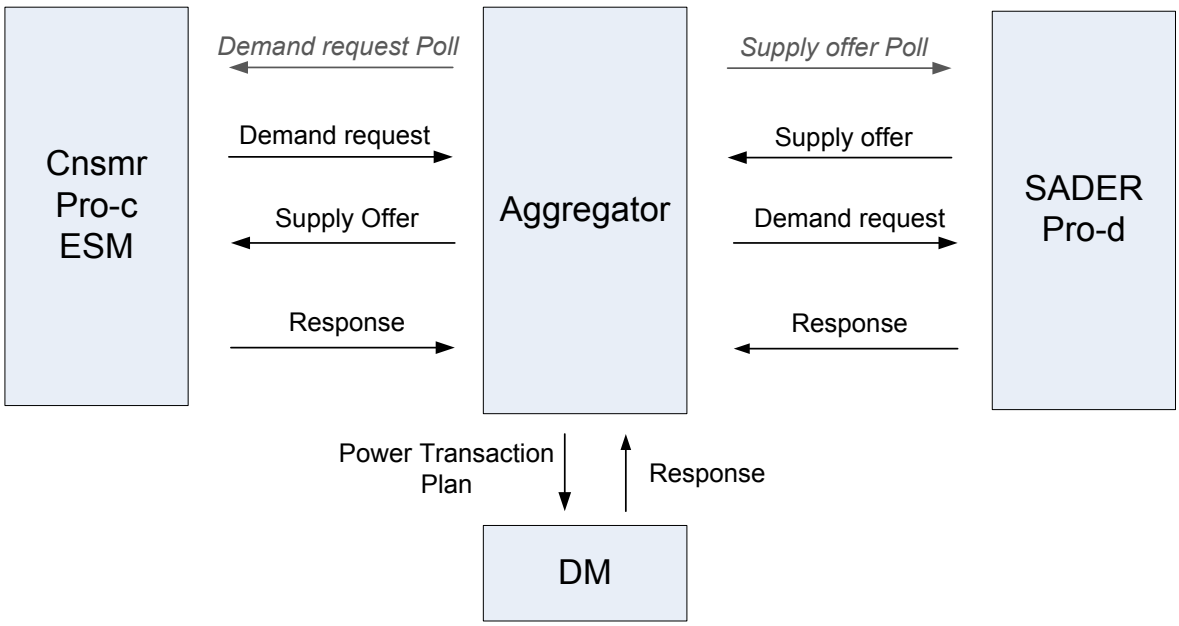

Figure 10: *Flexibility offering communication overview*

7.2.2.4 Relation to UCM document

This application scenario reflects the use cases described in the Generic High Level Use Case: *Flexibility offerings – WGSP-2128*. According to the UCM document:

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

"*The objectives of this use case are the exchange of offerings of the use of flexibility in supply and demand with another party, negotiation of these offerings and activation. This use case describes how two market roles offer, accept and assign demand or generation flexibility. Flexibility offerings are sent from flexibility providers to one or more (potential) users of flexibility. The offerings state the available flexibility in the dimensions of time (when can production / consumption take place) power and/or energy (what can be produced / consumed) and finance (in return for what compensation). These offerings are negotiated by a process of offering, accepting or rejecting, possibly followed by providing a different offering.*"

Obviously Application Scenario II reflects the objectives of offerings exchange for the use of flexibility in supply and demand. Nevertheless, here we do not consider the actual activation of the service. The negotiation process is supported by the following Application Scenario III.

7.2.3. Electric Vehicle support (Application Scenario III)

Given the substantially different characteristics of EVs when compared to other types of prosumers (i.e., mobility, volume, multiple authorities, see Section 7.1), we further consider a separate application scenario for the support of EVs. The aimed functionality remains the same as with Application Scenarios I, and II, however the focus in this case shall be on the implications introduced by these characteristics.

7.2.3.1 Relation to UCM document

This application scenario reflects the use cases described in the Generic High Level Use Case: *Smart Charging – WGSP-1003*. According to the UCM document:

"*Smart charging makes it possible that even with limited network capacity; multiple electric vehicles can simultaneously be charged if the charging is done in a "smart" way. Smart charging enables peak shaving, demand side management for all purposes and can postpone or even prevent network expansion."*

This fourth application scenario covers several aspects of WGSP 1003 including:

- WGSP-1100 Uncontrolled charging
- WGSP-1200 Charging with demand response
- WGSP-1300 Smart (re- / de) charging

7.2.4. Hybrid scenarios (Application Scenario IV)

The above-described scenarios provide concrete examples of interactions that are expected to emerge in active distribution networks. Though referring to specific functionality these scenarios can also be foreseen to co-exist in more complex scenarios. For example:

- Consumers and/or SADERs engage in a negotiation process with the Aggregator for the establishment of the final price, i.e., the communication mechanisms of Application Scenario II are employed for the matching of existing requests and offers, while mechanisms of Application Scenario I are further used for the negotiation of the price. Note that Application Scenario II only foresees a binary decision of whether to accept or reject an offer/request.
- The ESM places a demand request for additional power supply (Application Scenario II), but also engages in a negotiation with the Aggregator for the price (Application Scenario I).

7.3. Additional features

Apart from the basic functionality presented above, we further consider a set of functional features whose support is expected to enhance the capabilities on an application level. This refers to functionality placed on C-DAX nodes. The rationale behind the definition of these features is to

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

enhance the information-centric character of the C-DAX architecture. The purpose here is to realize a set of functional primitives that can support a range of applications, while at the same time avoiding the introduction of application-logic into the network.

In the following we present these features on a functional primitive level, presenting the relation to Use Case 3 and each application scenario.

7.3.1. Data aggregation

The purpose of the data aggregation primitive function is to apply aggregation functions on the reported values in the messages exchanged by the different actors. Such functions include: AVG, SUM, MIN/MAX, MEDIAN. The following table provides an overview of the applicability of these functions to the different types of information exchanged in the context of Use Case 3. The Domain column denotes the domain across which the aggregation function is applied e.g., applying the SUM function across the Location domain results in summing the values published across an area of the network. The Actor column denotes the entity that is expected to use the outcome of this function.

Table VIII: *Example scenarios for data aggregation*

No	Information	Domain	Function	Scenario	Actor
1	Residual energy (EVs)	Location/time	ALL	Forecasting demand/supply	ESM
2	Demand request	Location	SUM	Facilitating demand/supply matching	AGG
3		Time	SUM	Statistics for infrastructure development	ESM
4	Bid requests (offers)	Location	SUM	Facilitating demand/supply matching	AGG
5	Power consumption	Location/time	ALL	Forecasting demand	ESM

- In scenario No 1 the reports on the residual energy of EVs are aggregated on both the Location and Time domains in order to enable forecasting of energy demand and/or supply at certain areas of the network and/or certain time periods. This is considered as useful input for the ESM in the case of Application Scenarios I, III and IV.
- In scenario No 2 the denoted demand of energy in certain areas of the network can be aggregated so as to facilitate the matching of requests and offers i.e., aggregating the demand in a certain area of the distribution network so as to satisfy it with an offer presenting the desirable characteristics i.e., the amount of energy offered. This functionality can be supported by the Aggregator entity on a centralized manner. However, we consider the support of this functionality on a C-DAX node level so as to address the associated scalability concerns of a centralized approach. This is considered as useful input for the Aggregator in the case of Application Scenarios II, III and IV.
- In scenario No 3, the denoted demand or supply can be aggregated across the time domain in order to provide useful input for the DNO, related to the load in the network and the potential need for new infrastructure deployment. This scenario does not fall in the context of Use Case 3 and as such it will not be investigated further.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

- Scenario No 4 is similar to Scenario No 2 but refers to the aggregation of information describing the supply of energy. Again, the target in this case is to facilitate matching of requests and offers. This is considered as useful input for the Aggregator in the case of Application Scenarios II, III and IV.
- In scenario No5 power consumption reports are aggregated across location and/or time so as to facilitate the forecasting of demand and support the scheduling of power supply. This is considered as useful input for the ESM for both Application Scenario I, where it may use it for shaping pricing, and Application Scenario II, where it may use it to anticipate the need for publishing a Demand Request (as well as scenarios III and IV).

7.3.2. Data filtering

The purpose of the data filtering function is to provide the recipients of exchanged information with specific subsets of the globally available information. In the context of use case 3, we consider a set of filter function operators such as <, >, = to be applied by C-DAX nodes on the payload values of incoming publications. The following Table provides an overview of the considered application scenarios in the context of Use Case 3.

Table IX: *Example scenarios for data filtering*

No	Information	Operator	Scenario	Actor
6	Residual energy (EVs)	>,<	EV critical conditions	ESM
7	Power consumption	>	Trigger Demand request (additional supply)	ESM

- In scenario No 6, the C-DAX cloud may filter published information on critical residual energy levels of EVs, so as to enable an ESM to make an estimation of the expected demand. This is similar to the demand forecasting case in scenario No 5, however it is tailored for the more dynamic conditions applying in the case of EVs.
- In scenario No 7, unexpected levels of power consumption can be anticipated so as to trigger the publication of a Demand Request by the ESM in the context of the Application Scenario II.

7.4. Assumptions

In the following we list a series of assumptions made in the context of Use Case 3 and the described application scenarios.

1. It is assumed that there is only one Energy Service Manager (ESM) and only one Aggregator. This is a simplifying assumption to limit the complexity of the use case and it may be revisited in the course of the project. Additionally, this assumption does not preclude the realization of their functionality in a distributed manner.
2. It is assumed that all consumers, prosumers, and SADER participants of the REM are connected to the grid. EVs constitute the only exception as they can be disconnected from the grid when moving.
3. Transactions with the Bulk Energy Markets (BEM) are not taken into account.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

4. Any signalling between the Demand Response function of the utility and the ESM are outside of the C-DAX.

7.5. Requirements

In this section, C-DAX requirements for RETs are specified. These are primarily related to the delay requirements that must be fulfilled. However, as already argued, a major challenge to be addressed in this use case, relates to the scale of the (power and communication) network.

7.5.1. Network Scale

As already mentioned, Use Case 3 aims at the support of the functionality presented in Section 7.2 in the context of a large number of communicating entities. The exact set of participating entities i.e., C-DAX clients, were presented in Section 7.1. Table X further presents the expected volumes of C-DAX clients, for each type of communicating entity.

Table X: *Supported numbers of C-DAX Clients for RETs*

Client	Client Abbreviation	Number*	Description and Comments
Consumer	**cnsmr**	100,000	Those utility customers that participate in the REM only as a consumers. Examples: home, business, Industrial complex
Consumer function of a prosumer	**pro-c**	10,000	A prosumer is made of two different clients: one as a consumer and the other as a DER. Examples: Electric Vehicles, Home with a solar panel, business with CHP, industrial complex with generators, microgrids
DER function of a prosumer	**pro-d**	10,000	
Stand-Alone DER	**sader**	1000	Examples: solar panel on utility pole, wind farm, fuel cells, small hydro
Aggregator	**aggr**	1	
Energy Supply Manager	**esm**	1	
Distribution Manager	**dm**	1	
Regulator	**reg**	1	

* Numbers yet to be finalized

Note: We will model distributed storage as a prosumer, since it receives (charging) power from the grid and delivers (discharging) power into the grid.

7.5.2. Message priorities and delay requirements

The delay requirements for the information exchanges in Use Case 3 vary, subject to the importance/criticality of the information carried by the corresponding messages. These priorities are specified as High, Medium, and Low and are presented, along with the related delay requirements in Table XI below.

Table XI: *Message priorities and delay objectives*

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Message	Priority	Client-Client Delay Objective (minimum)
Demand request	Low (>70)	1000 ms
Supply offer	Low (>70)	1000 ms
Accept/ Reject demand request/supply offer	Low (>70)	1000 ms
Residual energy (EVs)	Low (>70)	1000 ms
Power transaction plan	Low (>70)	1000 ms
Power consumption	Low (>70)	1000 ms
Bid/request polling	High (25-35)	100 ms

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

8. Concluding Remarks

Requirements for developing the C-DAX system were provided in this document. Since this will be the first realization of the C-DAX platform, the document includes both platform and functional requirements for C-DAX so that it will be able to support three different sets of scenarios exemplified by the three use cases included in this document:

- Use Case 1: This use case considers the communication between RTUs and IEDs in distribution substations with SCADA master control and other systems in the utility DCC;
- Use Case 2: This use case mainly considers the communication between the PMUs deployed along the MV distribution lines and PMU Data Concentrators (PDCs) located at the distribution substations and other communication required for distribution management implementation based on state estimation using the PMU measurements. It also covers the communication between the PDC and the DCC side, including PMU maintenance instructions etc.
- Use Case 3: This use case considers RETs between the consumers of energy and owners of distributed generation including those owned and located at consumer premises. These transactions facilitate the matching of demand with supply and/or the operation of demand-response mechanisms.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Appendix A

An example of distribution grid

To set context for the Use Case descriptions and C-DAX requirements, and to understand the terminology, throughout this document, the Alliander distribution grid is used as an example, as illustrated in Figure 11.

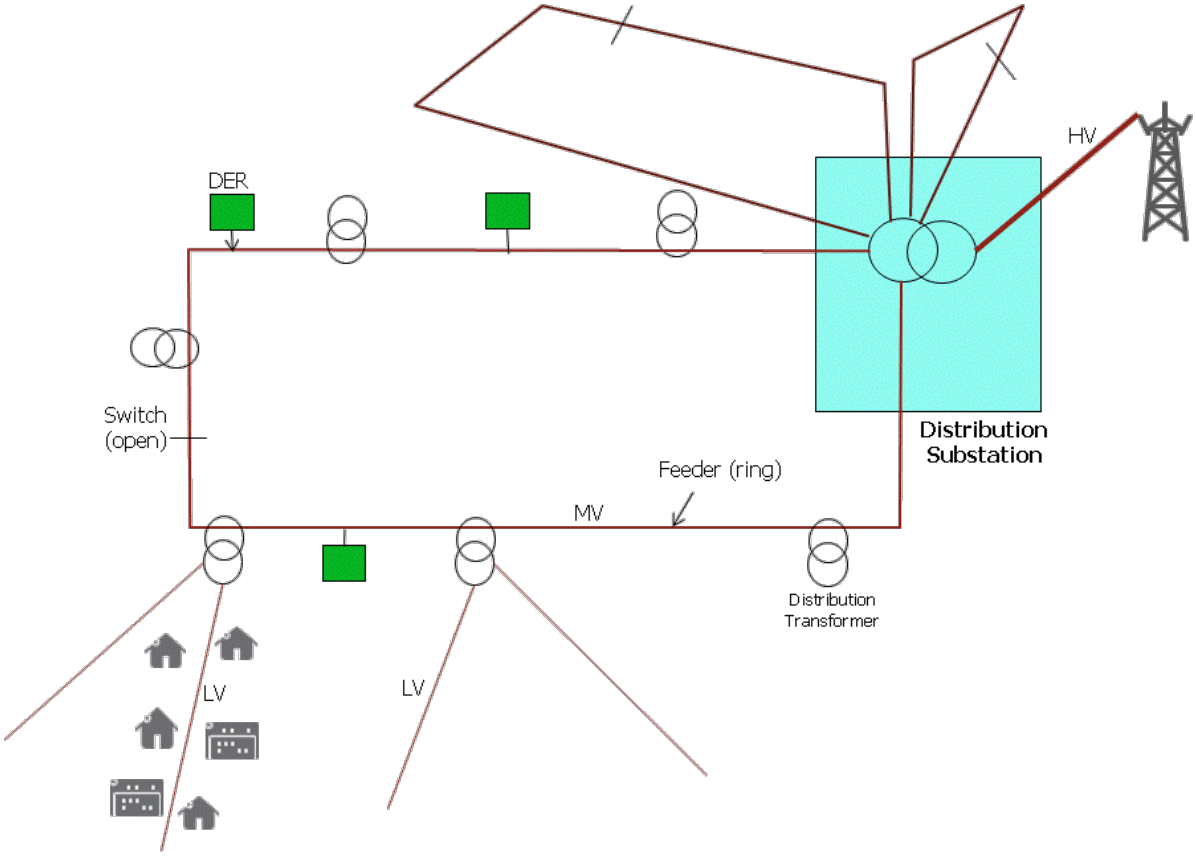

Figure 11: *An Illustration of Distribution Grid*

A *distribution substation* provides for HV/MV transformation from a 150kV transmission system to a 10 or 20 KV distribution grid. One or more *feeders* (composed by distribution lines) deliver power to most consumers connected to the secondary of the MV/LV *distribution transformers*. Based on about 350 substations and about 40,000 distribution transformers in the Alliander distribution grid, there are an average of about 115 distribution transformers supported by a distribution substations over one or more feeders from the substation. Note that a few large industrial and business customers may be supported directly at the MV level.

A feeder is deployed as a ring for grid reliability. In most normal operation scenario, the ring is open in two segments with dedicated switches. This operation mode allows dividing the ring in two spurs from the substation. If there is a fault on the feeder, the fault section is isolated from the ring and the switch closed to support the customers connected to the rest of the feeder.

Many DER units connect to the grid to the feeders at MV level injecting power in the grid at that voltage level. DERs (often collocated with consumer locations) also connect to the grid at the LV level (not shown in Figure 11).

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

APPENDIX B

A Framework for Communication Network Architectures

A communication network architecture framework for the smart grid [20] is shown in Figure 12.

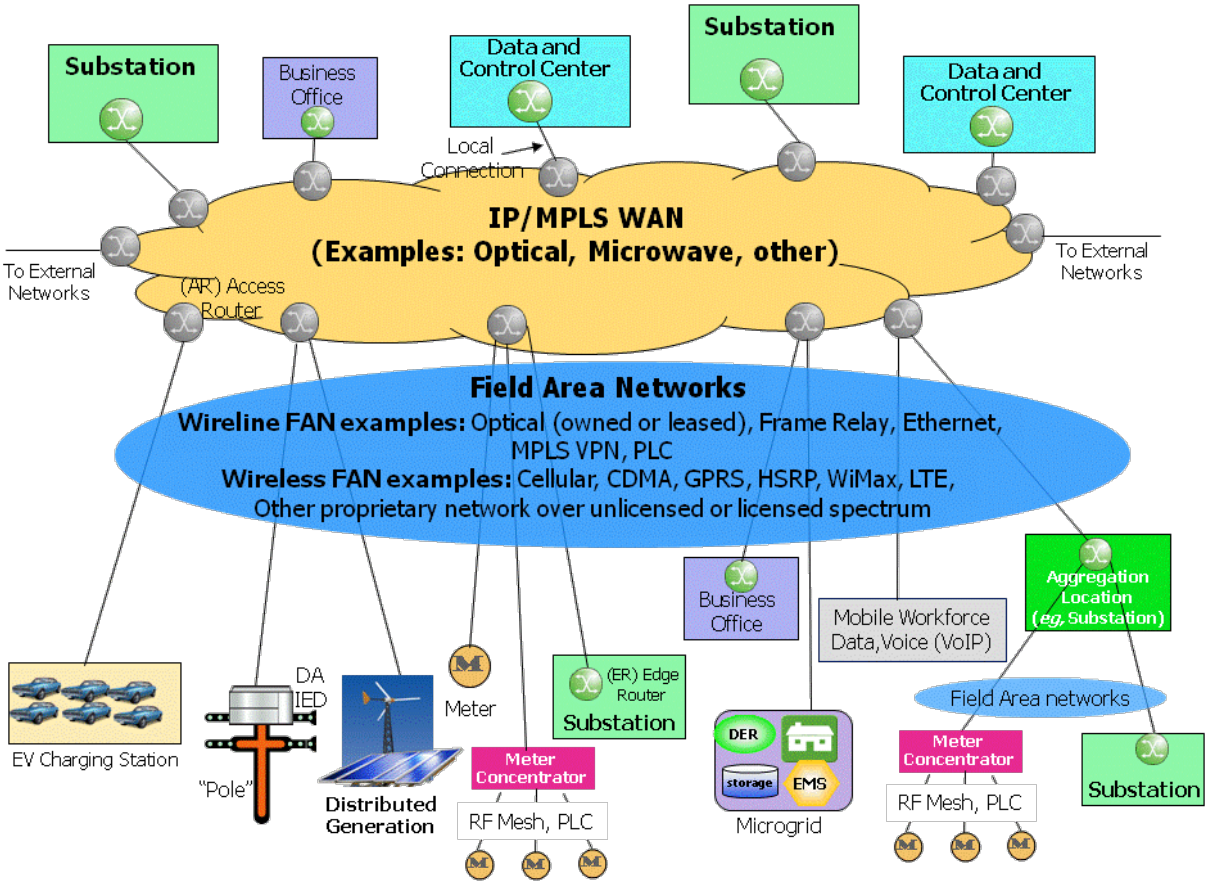

Figure 12: *Reference Architecture for the Target Communication Network for the Smart Grid*

The core network is called Wide Area Network (WAN) by the utility community which interconnects the Access Routers (AR). Many utilities have existing fiber to the plant infrastructure. Some utilities may additionally have a microwave network infrastructure. The utility may also lease a WAN infrastructure from service providers if necessary. In the case of smaller utilities, the WAN may be just an interconnection of a few Ars.

Utility endpoints that are collocated with Ars connect to the WAN directly over LANs at those locations. All remote endpoints connect to the Ars over the access networks called Field Area Networks (FAN). There may be one or more wireless and/or wire line FANs connecting to the endpoints. Example FAN technologies are listed in Figure 12.

Some of the smart grid elements (and by implications the corresponding applications) are shown in Figure 12. But note that other types of endpoints (current and future) can be easily accommodated in the architecture.

In Figure 13, a substation architecture based on IEC 61850 is shown.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

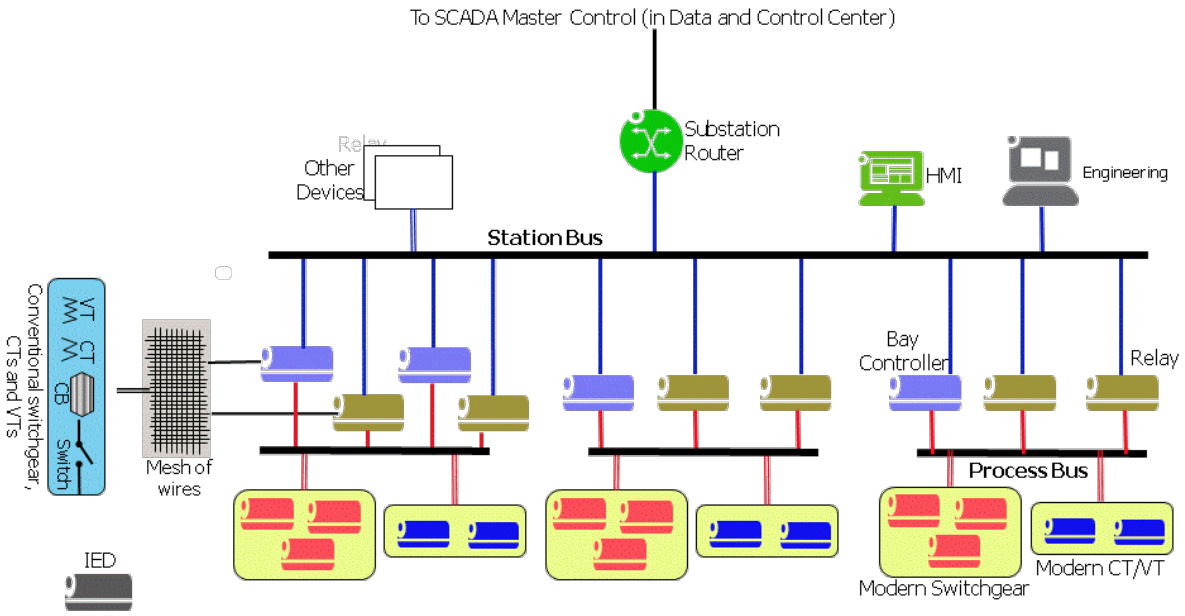

Figure 13: *Substation Architecture based on IEC 61850: An Example*

IEDs perform one of more of the many functions that are performed by the conventional switchgear and measurement devices such as the relays, bay controllers, voltage transformers (VT) and current transformers (CT). Some of the IEDs also support interfaces to the conventional elements before they are phased out from the substation. The IEDs are connected over an interconnection of process busses and a station bus for internal communication. They may also connect to an IP router for connecting to an IP network for communication with the systems in utility control center.

In a traditional substation, (before migration to IEC 61850), the conventional switchgear, VTs, CTs, relays and bay controllers are connection to an RTU that is responsible for all communication with the systems in the control center.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

APPENDIX C

Priority and Delay Objectives for Traffic of Smart Grid and Other Utility Applications

One way end-to-end delay objectives and priorities for traffic from many Smart Grid and Other applications over an integrated network are provided in Table XII which is a modified version of the table in [16].

Table XII: *Delay and Priority Requirements for Smart Grid Applications*

Application Function	Delay Allowance (minimum)	Priority	Application Type
	ms	0-max 100-min	
Delay ≤ 10 ms			
(High speed) Protection Information	8, 10	2	Teleprotection (for 60 Hz, 50 Hz)
Load shedding for underfrequency	10	20	SCADA
10 ms < Delay ≤ 20 ms			
Breaker reclosures	16	15	Teleprotection
Lockout functions	16	12	Teleprotection
Many Transformer Protection and control applications*	16	12	Teleprotection
System Protection (PMU)	20	12	Synchrophasors
20 ms < Delay ≤ 100 ms			
Synchrophasor Measurements, Status (Class A), Events, Control	60	10	Synchrophasors
SCADA periodic Measurement+status, Events Control	100	25	SCADA
DA periodic Measurement+status, Events Control	100	26	Distribution Automation
DG/DS Measurement+status, Events Control	100	27	Distributed Generation / Distributed Storage
PTT signaling – critical	100	30	
PMU clock synchronization	100	20	Synchrophasors
100 ms < Delay ≤ 250 ms			
VoIP bearer (inc. PTT)	175	50	MWF, Business Voice
VoIP signaling	200	60	Business Voice
DLR Measurements, Status, Events Control	200	28	Dynamic Line Rating
Real-time video (MWF)	200	55	MWF
On demand CCTV video	200	55	CCTV
Critical Operation Data (*eg,* DMS, TMS)	200	45	SCADA, DA, DG/DS, DLR, *etc*
Critical Business Data	250	70	Business Data
Most distribution and SCADA apps	250	65	SCADA
AMI – Critical (*eg* VVWC)	250	40	AMI
250 ms < Delay < 1 s			
AMI – Priority (*eg,* ADR, Black Start)	300	70	AMI
CCTV stream – normal	400	75	
PMU (Other than Class A)	500	80	Synchrophasors

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

Application Function	Delay Allowance (minimum)	Priority	Application Type
	ms	0-max 100-min	
Some Transformer Protection and Control Applications	500	80	Protection
Non-Critical Operations Data	500	80	SCADA, DA, DG/DS, DLR, *etc*
Non-Critical Business Data	500	80	Business data
1 s ≤ Delay			
Image files	1000	90	SCADA
Fault recorders	1000	90	SCADA
(Medium speed) monitoring and control information	1000	90	SCADA
(Low speed) O and M information	1000	90	SCADA
Fault isolation and Service restoration	1000	90	Protection
Distribution applications	1000	90	Some Distribution automation, Some Demand Response
AMI –Measurements, Status, Events, Control	1000	85	AMI
Text strings	1000	90	SCADA
Audio and video data streams	1000	78	SCADA
Fault Recorders	1000	90	SCADA
Best effort, Default	2000	100	Many

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

References

[1] US NIST, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[2] US NIST "Special Publication 800-67 Revision 1 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," (Revised January 2012).

[3] Stéphane Manuel, "Classification and generation of disturbance vectors for collision attacks against SHA-1," Designs, Codes and Cryptography, v.59 n.1-3, April 2011.

[4] E. Rescorla, "Diffie-Hellman Key Agreement Method," IETF RFC 2631, June, 1999.

[5] US NIST, "Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," March, 2006.

[6] Y-J. Kim, V. Kolesnikov, and M. Thottan, "Resilient End-to-End Message Protection for Large-scale Cyber-Physical System Communications," IEEE Smart Grid Communications, Nov. 2012.

[7] S. C. Bono, M. Green, A. Stubbleeld, A. Juels, A. D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in Proceedings of USENIX Security Symposium, Aug. 2005.

[8] K. Nohl and D. Evans, "Reverse-engineering a cryptographic RFID tag," in Proceedings of USENIX Security Symposium, Aug. 2008.

[9] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, "Biclique Cryptanalysis of the Full AES", 2011.

[10] B. Gassend, D. Clarke, M. van Dijk and S. Devadas, "Silicon Physical Random Functions," Proceedings of the Computer and Communications Security Conference, November 2002.

[11] IEC, *Communication Networks and Systems in Substations Parts 1-10,* Technical Report, 2002-2005.

[12] IEC, *Transmission protocols –Network access for IEC 60870-5-101using standard transport profiles*, CEI/IEC 60870-5-104:2006, June 2006.

[13] IEEE, IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems, IEEE Std C37.111-1999, March 1999.

[14] BSI, *Voltage characteristics of electricity supplied by public distribution systems*, British Standard, BS EN 50160:2000, May 2004.

[15] IEEE standard 1159-2009 (revision of IEEE Std 1159-1995), Recommended Practice for Monitoring Electric Power Quality.

[16] J. G. Deshpande, E. Kim, and M. Thottan, *Differentiated Services QoS in Smart Grid Communication Networks*, Bell Labs Technical Journal special issue on Vertical Markets, December, 2011.

[17] IEEE, IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Std C37.118.1™-2011, December 2011.

[18] IEEE, IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Std C37.118.2™-2011, December 2011.

[19] Information and Communication Technologies for Smart Distributed Generation (ICT4SMARTDG), *Key Messages and Recommendations on Solution Implementation of Four Important and Essential Scenarios,* Deliverable 4 of the European Commission Project – Grant Agreement No. 23888. Project titled "Steps Forward for Promotion of Large scale Implementation", December 2011.

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

[20] K. Budka, J. Deshpande, M. Thottan, "Communication Network Transformation for Smart Grid Evolution", UTC Journal, May 2012.

[21] CEN, CENELEC and ETSI, "Use Case Collection, Management, Repository, Analysis and Harmonization," DRAFT Report of the Working Group Sustainable Processes to the Smart Grid Coordination Group / Mandate M/490, Draft version 0.65, 2012.

List of Acronyms

AES	Advanced Encryption Standard
AR	Access Router
BEM	Bulk Energy Market
CA	Certification Authority
C-DAX	Cyber-secure Data And Control Cloud
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation en Electronique et en électrotechnique
CML	Cumulative Lost Minutes
COMTRADE	Common Format for Transient Data Exchange
DCC	Distribution Control Center
DdoS	Distributed Denial of Service
DER	Distributed Energy Resource
DES	Data Encryption Standard
DHKE	Diffie-Hellman Key Exchange
DM	Distribution Manager
DMS	Distribution Management System
DoS	Denial of Service
DR	Demand Response
DSO	Distribution Service Operator
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
EMS	Energy Management System
ESM	Energy Supply Manager
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FAN	Field Area Network
FLIR	Fault Location, Isolation and Restoration
HAN	Home Area Network
HSM	Hardware Security Modules
ICN	Information Centric Networking
IDS	Intrusion Detection System
IEC	International Electro-technical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
LTE	Long Term Evolution

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED

LV	Low Voltage
MAC	Message Authentication Code
MV	Medium Voltage
NIST	National Institute of Standards and Technology
PDC	Phasor Data Concentrator
PHY	Physical (layer)
PKI	Public Key Infrastructure
PLC	Power Line Communication
PMU	Phasor Measurement Unit
PUF	Physically Un-clonable Function
PV	Photovoltaic
REM	Retail Energy Market
REMP	Resilient End-to-end Message Protection
RET	Retail Energy Transductions
RFID	Radio-Frequency Identification
RSA	Rivest, Shamir, Adleman
RT-SE	Real Time State Estimator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG-CG	Smart Grid – Coordination Group
SE	State Estimation or State Estimator
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
TS	Technical Specification
UCG	Use Case Group
UCM	Use Case Management
VVO	Volt and Var control and Optimization
WAN	Wide Area Network
WGSP	Work Group Sustainable Processes
WM	Wholesale Market

COPYRIGHT © 2013 C-DAX Consortium. ALL RIGHTS RESERVED