Pacific Northwest NATIONAL LABORATORY

MultiSpeak Landscape Assessment

MS-SPEAK Project

March 2018

TE McDermott
WJ Hutton

Prepared for the U.S. Department of Energy under **Contract DE-AC05-76RL01830**

U.S. DEPARTMENT OF ENERGY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

1.0 Current State of MultiSpeak

MultiSpeak is an interface specification for electric power distribution software functions, implemented and maintained by NRECA via www.multispeak.org. Compared to the IEC Common Information Model (CIM) standards 61968 and 61970, MultiSpeak has followed a less-formal development process, and has been more pragmatic in application. It was adopted much faster than distribution CIM, with currently 96 vendor members and 153 interoperable product pairs tested. The most widely used version is still version 3, adopted in 2005. There are some vendors using version 4, adopted in 2009, or version 5, adopted in 2015. However, the first version 5 interoperability tests won't be performed by NRECA until later in March 2018.
There was a partially-completed effort to harmonize MultiSpeak with distribution CIM, embodied in IEC 61968-14, which focused on harmonization for metering. NRECA stopped supporting this harmonization due to funding limitations, but would still like to finish the work, as it can help ensure MultiSpeak's longevity and has expressed interest in collaborating with PNNL on this work. In version 5, optional support has been added for CIM naming conventions. This need could be partly addressed in the GridAPPS-D GMLC project, which focuses on interoperability, rather than MS-SPEAK, which focuses on cyber security.

2.0 Role for Cybersecurity Research

PNNL brings a unique perspective to this problem space. Our understanding of the MultiSpeak lifecycle and the development of the ESB (Enterprise Service Bus) in phase 1 of this project, along with our work with key MultiSpeak experts will allow us to bring groups together to ensure a robust and adoptable solution by industry. The bulk of the MultiSpeak users are smaller sites, who do not have the resources or capabilities to ensure their vendors provide the level of cyber security needed to for secure transmissions. By working with NRECA, industry, MultiSpeak working group, and vendors to develop a secure and consistent approach in version 5 we can bridge the gap between these groups. PNNL would provide a verification and validation approach for vendors to test their implementations via a "Plug Fest" event at PNNL. Results would be shared with all along with a framework for implementation which could become the basis for a standard.

3.0 Background

In 2005, the first MultiSpeak Security Specification addressed confidentiality, authentication and integrity of messages through optional use of Secure Sockets Layer (SSL), shown at the middle of Figure 1. This could be grafted on to MultiSpeak version 3 messages with little effort, and many users actually did so. The 2005 document stated that non-repudiation is not required for electric utilities, and it left access control to the utility IT department. The 2013 version of MultiSpeak Security Specification updated the referenced Web standards and referenced the NIST specifications for smart grid cyber security. It also added WS-Security for deep packet inspection, per-message and per-session security, shown at the bottom of Figure 1.

Although MultiSpeak Security Specification can be implemented on versions 3, 4 and 5 of MultiSpeak, only version 5 is practical for supporting packet inspection and WS-Security. However, most vendors are at version 3. There are a few vendors working with versions 4 and 5 internally, but not yet through formal interoperability testing that would "give teeth" to the

standard. The MultiSpeak versions are not backward compatible in their method signatures, as illustrated in Appendix B for the meter connect/disconnect function. This has been a barrier for established vendors moving beyond version 3, although a vendor new to MultiSpeak would probably start with version 4 or 5.

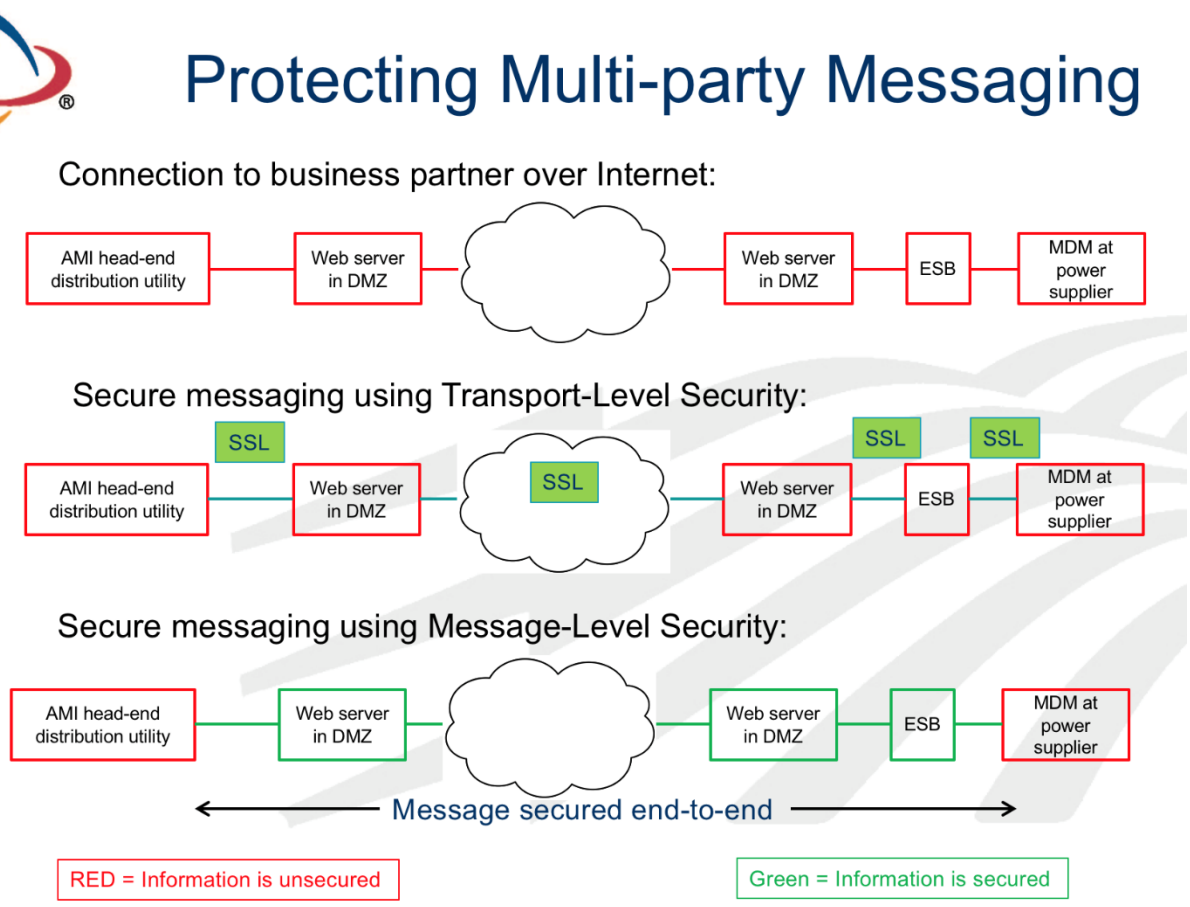

Figure 1 Messaging Security Overview from the MultiSpeak Integrator Training Slides

4.0 PNNL's Outreach

Through contacts made by phone and in person at the TechAdvantage conference (Appendix A), we've identified at least three vendors who would participate in a demonstration of MultiSpeak cyber security per the 2013 specification. NRECA and NRTC would also participate. The rural electric cooperatives are still assessing their vulnerabilities, but they would adopt a more secure version of MultiSpeak if their vendors and integrators could provide it. This demonstration would involve one MultiSpeak interface (CD – Connect/Disconnect) out of the thirty-eight shown in Figure 2. It would then be left to the vendor community to implement the remaining thirty-seven functions in a cyber-secure fashion, possibly incorporating the open-source software to be developed and published in the MS-SPEAK project.

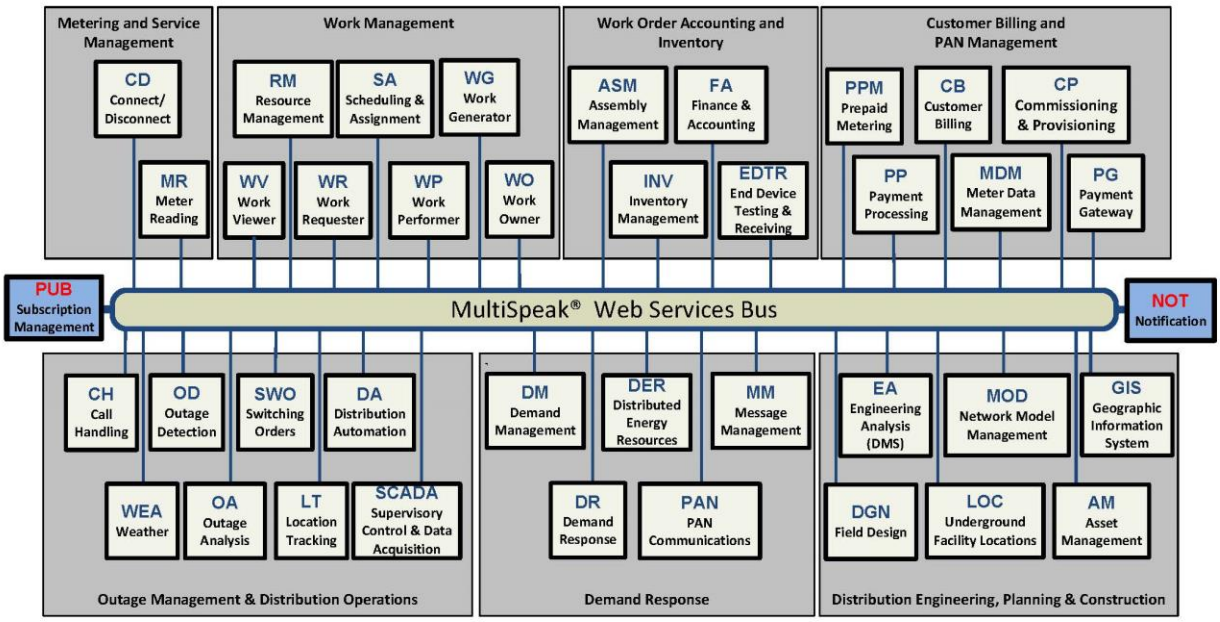

Figure 2 MultiSpeak Version 5 Functions. MS-SPEAK aims to develop and demonstrate cyber security for one of these, CD.

Appendix A – TechAdvantage 2018 Trip Report

Two PNNL staff attended the 2018 TechAdvantage Conference in Nashville, February 26-28, for meeting and information gathering to help develop this Phase 2 plan. Some key findings:

1. Doug Lambert: NRTC remains interested in the project and wants to participate in Phase 2 even if unfunded. CIM harmonization efforts were halted by NRECA due to funding, but NRTC would like to see this carried through (i.e. after MS-SPEAK).
2. Gary McNaughton provided a billing rate of $195/hour, with a strong preference to contract through NRTC. Gary is “retiring” from NRECA involvement in June 2018 but is interested in helping out with MS-SPEAK. By observation, Gary has essential subject matter expertise that NRECA and NRTC both rely on.
3. Alvin Razon: NRECA would like to collaborate on MS-SPEAK and would like NRTC to remain in the picture. MultiSpeak funding is only at the $300K-400K level, and they think $1.0-1.5M is needed. Alvin would like for PNNL to join MultiSpeak as a dues-paying member, would help with vendor outreach, and would help coordinating with NRECA subcontractors currently working on new interoperability test procedures. NRECA has implemented “digital badging” for vendors who pass the new tests; the first of these is scheduled for later in March 2018.
    a. Increase Technologies – Jeremy Westbrook
    b. KLM Technologies – Marlon Umali, for the test harness
4. Conference Sessions: several cooperatives are using MultiSpeak actively for new integration projects; some of these cooperatives are in North Carolina and work closely with Doug Lambert, in fact his office is physically located at Wake Electric Membership Corporation. In the cyber security arena, most cooperatives are still in the self-assessment phase. There was also a session on cyber insurance.
5. Vendors: on the floor, several vendors claim to be working with MultiSpeak versions 4 and 5, but they are using internal development labs to implement point-to-point interfaces with other vendor products according to customer demand. These are not widely published, and without formal testing, there is no guarantee that they are conforming to MultiSpeak rigidly.
6. Vendor participants: there are three who expressed strong interest in this project:
    a. Milsoft (Steve Collier) has been a strong proponent of MultiSpeak from its beginnings. They don’t have a metering connect/disconnect product but would participate in other ways.
    b. Eaton (Michael Sharp) asked skeptical questions about the value (to Eaton) of formal testing, but a followup call has been scheduled for March 9.
    c. Aclara (Tom Mickus) asked for a followup, still to be scheduled.
7. Other vendors: none of them said “no”. There are several to follow up on:
    a. NISC – Jeremy Lang and Todd Eisenhauer, need to follow up
    b. Survalent – John McKinney, need to follow up
    c. ABB – John Barnick, they use a NC-based integrator, need to follow up
    d. Itron – Malcolm Green and Doug Sorenson, need to follow up

e. SEDC – need to contact Sarat Yellapetti, saraty@sedata.com, (770) 414-8400 ext 2331 when he's back in the office.

f. Landis & Gyr – left message for Carol Meyer, need to follow up

g. OSI International – extended conversation, we left cards with them

h. Siemens – extended conversation, we left cards with them

8. Contact Umatilla Electric Cooperative in Hermiston about participating. Have they worked with PNNL before?

9. Other utility members of MultiSpeak in the Pacific Northwest include Cowlitz County PUD, Peninsula Light Co, Inland Power & Light, and Kootenai Electric Cooperative.

10. In a follow-up phone call, Eaton confirmed their interest if the project moves forward. David Sutton, Yukon Software Product Manager, joined Michael Sharp on this call. They implemented v5 during 2017 for expected future use, but all current customers and enquiries have been for v3. They skipped v4. Traffic is often encrypted (i.e. the 2005 MultiSpeak Security Specification) but no other cyber security has been requested.

Appendix B – Connect/Disconnect Version Differences

The connect/disconnect (CD) function is part of the meter reading (MR) module in versions 3 and 4, but has its own module called remote connect/disconnect (RCD) in version 5. The main purpose is to disconnect and reconnect customer service remotely, based on payment or non-payment of their bills. It also includes load limiting, typically for pre-pay customers. However, CD operations may occur for other reasons, and we've heard anecdotes of utilities (improperly) using CD to switch primary feeder equipment, such as capacitor banks. This is an important function to protect, as hackers could use CD to disconnect customers, and in some cases, cause other switching operations to occur on the distribution system. There are also many vendors, including practically all of the metering and customer billing vendors, interested in this function. Those factors make CD a good candidate for the first MultiSpeak interoperability test of cyber security.

CD implementation also appears to be relatively simple, compared to some other functions like GIS and engineering analysis (EA) feeder models; see Figure 1. Even so, a CD test would have to include some other functions and use cases in versions 3, 4 or 5:

- Network management; the PingURL method implemented in MS-SPEAK Phase 1.
- Discovery; does a product support CD and if so, which features? 9 use cases in version 5.
- ErrorHandling; common to all functions. 3 use cases in version 5.
- Subscription Management; what other functions need to be notified about CD events? 4 use cases in version 5.
- Perform a meter reading on demand just before disconnecting. This is handled differently in versions 3, 4 and 5.
- Notify customer account management of the disconnect or reconnect, so that billing data and service dates can be updated. This is handled differently in versions 3, 4 and 5.
- Notify the outage management system that the customer has been disconnected or reconnected with cause, so if that customer calls, it won't be handled as an outage. This is handled differently in versions 3, 4 and 5.

The MultiSpeak use cases, methods and data structures are well-documented with UML in Enterprise Architect software files. Some of the use cases are "modular" and implemented with one or two methods. Other user cases are "composite" and reference other use cases. To implement the CD interface, one starts by enumerating all of the methods referenced in the CD modular or composite use cases. Second, the core functions like subscription management and error handling should be added. Third, the set of method signatures will reference various data structures and types that must be supported. Fourth, use case activity diagrams will specify which messages are part of each use case; these are important inputs for test scripts. For example, in version 4.1 there are 11 methods to implement for CD, and in various combinations, those will support 11 use cases for CD. See Table B.1.

Table B.1. Summary of CD Use Cases and Methods in MultiSpeak Version 4.1

Use Cases (Root MSP.MR:20)	Required Method Implementations
100 Disconnect for non-payment (composite)	InitiateConnectDisconnect
110 Reconnect after payment (composite)	CDStatesChangedNotification
120 Initiate power limit	GetCDMeterState
130 Cancel power limit	InitiateCDMeterStateRequest
140 Connect (composite)	InitiateMeterReadingsByMeterID
142 Connect without arming	GetReadingsByMeterID
143 Arm	GetLatestReadingsByMeterIDList
145 Connect with arming	ReadingChangedNotification
147 Disconnect	FormattedBlockNotification
150 Last known state	IntervalDataNotification
160 Verify state	ConnectDisconnectChangedNotification
Referenced Use Cases for meter reading and outage management	
MR:10.110 Meter reading on demand	
OM:70.170 Service disconnection for non-outage cause	
OM:70.180 Service reconnection for non-outage cause	

In version 3, the CD functions were localized to interface 2B, between customer billing (CB) and CD. There was also a link between CB and call handling (CH), but no other apparent interface to outage management. The data structures may also differ, but this has not been explored yet. Between versions 4.1 and 5, the differences appear to be more significant than between 3.0 and 4.1. As enumerated above, there are 16 total use cases in version 5 for discovery, error handling and subscription management. Rather than send explicit messages for use cases OM:70.170 and 180 to the outage management system, it's expected that an outage management system would subscribe to notifications of CD events, and the CD function provider must then publish those events when appropriate. While the functionality is very similar, it's apparent that use cases and methods have been substantially reorganized in version 5. For example, there is a widespread pattern of pairing notification and response messages. See Table B.2 for a summary.

Table B.2. Version 5 RCD Use Cases and Messages

Composite Use Cases (MSP.RCD:)	Messages (each has a matching Response message)
10.C.10 Synchronize CD devices	CDDevicesChangedNotification
10.C.20 Synchronize CD capable	CDDevicesCreatedNotification
20.C.10 Disconnect customer	CDDevicesDeletedNotification
30.C.10 Establish load limit	CDDevicesExchangedNotification
30.C.20 Cancel load limit	CDDevicesInstalledNotification
Modular Use Cases (MSP.RCD:)	CDDevicesUninstalledNotification
10.M.10 Request CD capable meters	CDStatesChangedNotification
10.M.20 Request collection changes	CDStatesNotification
10.M.25 Request CD devices	ConnectDisconnectEventsNotification
10.M.30 Subscribe CD device changes	GetAllCDDevices
10.M.40 Subscribe CD state changes	GetCDDeviceStates
10.M.50 Subscribe CD events	GetCDEnabledMeters
10.M.60 Subscribe collection changes	GetCDMeterCollectionChanges
20.M.10 Request RCD switch action	GetCDMeterStates
20.M.100 Publish CD status changes	GetCDSupportedMeters
20.M.105 Publish new CD events	GetConnectDisconnectEventsByReasonCode
20.M.110 CD events by reason/date	InitiateCDDeviceExchanges
20.M.120 Publish CD collection change	InitiateCDDeviceInstallations
20.M.130 Obtain CD collection change	InitiateCDDeviceUninstallations
20.M.20 Publish RCD switch action	InitiateCDStateRequest
20.M.30 Obtain CD meter status	InitiateConnectDisconnect
20.M.40 Request RCD status check	IsCDSupported
20.M.50 Publish RCD switch status	SetCDDevicesDisabled
20.M.60 Disable a CD device	SetCDDevicesEnabled
20.M.70 Enable a CD device	
20.M.80 Get CD device capability	
20.M.90 Publish collection changes	

In order to support CD message translation between versions 3, 4 and 5, it will be necessary to review and compare all of the available use case sequence diagrams in detail. This process will identify all of the methods, data structures and data types that must be supported. For version 3, use cases were not used and only the schema (XSD) and WSDL files are available. Assertion documents were used for version 3 testing, and it's likely that equivalent use cases can be derived from the assertion documents, along with the version 3 specification documents in PDF. From this cursory review, it seems unlikely that message-level translation would be successful. Instead, the approach should be based on "use case translation", which is going to require subject matter expertise and will also complicate the implementation. For example, we might require supplemental "begin use case" and "end use case" messages to the translator, which would then be able to analyze and translate groups of messages to fulfill the specified use case.

Pacific Northest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov