This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

MQTT and the NIST Cybersecurity Framework Version 1.0

Committee Note 01

28 May 2014

Specification URIs

This version:

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cn01/mqtt-nist-cybersecurity-v1.0-cn01.html (Authoritative)

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cn01/mqtt-nist-cybersecurity-v1.0-cn01.doc

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cn01/mqtt-nist-cybersecurity-v1.0-cn01.pdf

Previous version:

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cnprd01/mqtt-nist-cybersecurity-v1.0-cnprd01.doc (Authoritative)

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cnprd01/mqtt-nist-cybersecurity-v1.0-cnprd01.html

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cnprd01/mqtt-nist-cybersecurity-v1.0-cnprd01.pdf

Latest version:

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html (Authoritative)

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.doc

http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.pdf

Technical Committee:

OASIS Message Queuing Telemetry Transport (MQTT) TC

Chairs:

Raphael J Cohn (raphael.cohn@stormmq.com), Individual

Richard J Coppen (coppen@uk.ibm.com), IBM

Editors:

Geoff Brown (geoff.brown@m2mi.com), Machine-To-Machine Intelligence (M2Mi) Corporation

Louis-Philippe Lamoureux (louis.lamoureux@m2mi.com) Machine-To-Machine Intelligence (M2Mi) Corporation

Related work:

This document is related to:

- *MQTT Version 3.1.1*. Edited by Andrew Banks and Rahul Gupta. Latest version: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html.

Abstract:

This document provides guidance for organizations wishing to deploy MQTT in a way consistent with the NIST Framework for Improving Critical Infrastructure cybersecurity.

Status:

This document was last revised or approved by the OASIS Message Queuing Telemetry Transport (MQTT) on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this document to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at https://www.oasis-open.org/committees/mqtt/.

Citation format:

When referencing this document the following citation format should be used:

[mqtt-nist-cybersecurity-v1.0]

MQTT and the NIST Cybersecurity Framework Version 1.0. Edited by Geoff Brown and Louis-Philippe Lamoureux. 28 May 2014. OASIS Committee Note 01. http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/cn01/mqtt-nist-cybersecurity-v1.0-cn01.html. Latest version: http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html.

document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1 Introduction

The purpose of this supplemental publication is to introduce implementors and senior executives to the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (herein referred as the NIST Cybersecurity Framework) and its relationship with the MQTT security recommendations. The NIST Cybersecurity Framework provides a common language and mechanism for organizations to: 1) describe current cybersecurity posture; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward the target state; 5) foster communications among internal and external stakeholders.

The NIST Cybersecurity Framework complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program. Rather, the organization can use its current processes and leverage the NIST Cybersecurity Framework to identify opportunities to improve an organization's cybersecurity risk management. It also provides a consensus description of what's needed for a comprehensive cybersecurity program.

This supplemental document focuses solely on the MQTT protocol's integration within the NIST Cybersecurity Framework. Keep in mind that a complete cybersecurity management framework can include a wide variety of topics that must be tailored for specific needs according to the organization's missions, environments of operation, and technologies used. Please refer to the NIST Cybersecurity Framework for more information: http://www.nist.gov/cyberframework/

1.1 References

Useful background reading resources include:

- MQTT version 3.1.1.
  http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/csprd01/mqtt-v3.1.1-csprd01.pdf
- NIST Cybersecurity Framework.
  http://www.nist.gov/cyberframework/
- *Control Objectives for Information and Related Technology (COBIT)*.
  http://www.isaca.org/COBIT/Pages/default.aspx
- *Top 20 Critical Security Controls (CSC*).
  http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf
- *ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program:*
  http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FISA+99.02.01-2009

- *ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels.* http://isa99.isa.org/ISA99%20Wiki/WP-3-3.aspx
- *ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements.* http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- *NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.* April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4
- *OASIS Security Assertion Markup Language (SAML)*. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
- Federal Information Processing Standards (FIPS). http://www.nist.gov/itl/fips.cfm
- Payment Card Industry Data Security Standard (PCI DSS). https://www.pcisecuritystandards.org/security_standards/
- NIST Special publication 800-26 (Security Self-Assessment Guide for Information Technology Systems". http://www.fda.gov/ohrms/dockets/dockets/00d1541/rpt0007.pdf
- ISO 15408:2009 (Evaluation criteria for IT security). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341

1.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts:

1. The Framework Core
2. Framework Implementation Tiers
3. Framework Profiles

Each Framework component reinforces the connection between business drivers and cybersecurity activities.

1.2.1 The Framework Core

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation

and operations level. The Framework Core consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative references such as existing standards, guidelines, and practices for each Subcategory.

1.2.2 Framework Implementation Tiers

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which their cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

1.2.3 Framework Profile

A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a *Current* Profile (the "as is" state) with a *Target* Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

1.3 NIST Cybersecurity Framework for MQTT

In the context of the MQTT protocol, each NIST Cybersecurity component has been reduced to solely reflect security considerations of the protocol and are renamed accordingly: MQTT cybersecurity Framework Core, MQTT cybersecurity Framework Implementation Tiers, and MQTT cybersecurity Framework Profile.

1.3.1 MQTT Cybersecurity Framework Core

The MQTT cybersecurity Framework Core consists of the same five Functions (Identify, Protect, Detect, Respond, Recover) which can provide a high-level, strategic view of an organization's management of MQTT related cybersecurity risk. The MQTT cybersecurity Framework Core then

identifies underlying key Categories and Subcategories for each of these Functions described in Section 2. Because the MQTT cybersecurity Framework is smaller in scope it is unnecessary to provide references for every Category and Subcategory. Instead a non-exhaustive list of informative references is provided in Section 1.1.

1.3.2 MQTT Cybersecurity Framework Implementation Tiers

The MQTT cybersecurity Framework Implementation Tiers demonstrate the implementation of the MQTT cybersecurity Framework Core Functions and Categories and indicate how cybersecurity risk is managed. Organizations should determine the desired Tiers at the Category level, ensuring that the selected levels meet the organizational goals, mitigate cybersecurity risk, and are feasible to implement. External guidance will be helpful, such as information that could be obtained from OASIS Security Assertion Markup Language (SAML), the Federal Information Processing Standards (FIPS), and Payment Card Industry Data Security Standard (PCI DSS).

1.3.2.1 Tier 1: Partial

The organization has not yet implemented a formal, threat-aware MQTT risk management process to determine a prioritized list of cybersecurity activities. The organization might implement some portions of the Framework on an ad hoc basis due to varied experience or information gained from outside sources.

1.3.2.2 Tier 2: Risk-Informed

The organization uses a formal, threat-aware MQTT risk management process to develop an MQTT Profile of the Framework. In addition, risk-informed, management approved processes and procedures are defined and implemented. Staff have adequate resources to perform their cybersecurity duties.

1.3.2.3 Tier 3: Repeatable

The organization updates its Profile based on regular application of its MQTT risk management process to respond to a changing cybersecurity landscape. Risk informed policies, processes, and procedures are defined, implemented as intended, and validated. The organization will also have consistent methods in place to provide updates when a risk change occurs.

1.3.2.4 Tier 4: Adaptive

The organization updates its Profile based on predictive indicators derived from previous and anticipated cybersecurity activities. These updates to the Profile enable the organization to adapt to an evolving cybersecurity landscape and address emerging threats. Risk-informed policies, processes, and procedures are part of the organizational culture and are reviewed regularly - including feedback from lessons learned and information shared from other sources - to predict and address potential cybersecurity events.

1.3.3 MQTT Cybersecurity Framework Profile

An MQTT cybersecurity Framework Profile enables organizations to establish a roadmap for reducing MQTT related cybersecurity risk that is well-aligned with organization and sector goals, considers legal and regulatory requirements, and reflects risk management priorities. An MQTT cybersecurity Framework Profile can be used to describe both the current state and the desired target state of specific MQTT cybersecurity activities, thus revealing gaps that could be addressed to meet MQTT cybersecurity risk management objectives.

The Profile is the selection of the Functions, Categories, and Subcategories that are aligned with the business requirements, risk tolerance, and resources of the organization. The Target Profile should support business requirements and aid in the communication of risk within and between organizations. Identifying the gaps between the Current Profile and the Target Profile allows the creation of a roadmap that organizations could implement to reduce MQTT related cybersecurity risk.

1.3.4 Establishing or Improving a Cybersecurity Program

Together, the three MQTT Cybersecurity Framework components allow organizations to understand and shape their cybersecurity program. The following sub sections illustrate how this can be done.

1.3.4.1 Prioritize and Scope

The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process.

1.3.4.2 Orient

Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and their overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

1.3.4.3 Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

1.3.4.4 Conduct a Risk Assessment

This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

1.3.4.5 Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organization may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

1.3.4.6 Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a "cost benefit" analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

1.3.5 Document Overview

The remainder of this supplemental document contains the following sections:

- Section 2 describes the MQTT cybersecurity Framework Core Functions.
- Appendix A is an Example Implementation of the MQTT cybersecurity Framework.
- Appendix B are Acknowledgements
- Appendix C is the Revision History

2 MQTT Cybersecurity Framework Core Functions

This section describes the five MQTT cybersecurity Framework Core Functions and how they can be used to assess an organization's cybersecurity level where the MQTT protocol is used. The list of components associated with each function presented here is non-exhaustive and provided as a starting point for a cybersecurity Management Framework. Implementors should modify Categories and Subcategories as they see fit such as to tailor the MQTT Cybersecurity Framework functions for their organization. Informative References described in Section 1.1 should also be modified to reflect an organization's regulatory requirements.

2.1 Identify

The purpose of this function is to:

1. Develop the institutional understanding of which MQTT related organizational systems, assets, data, and capabilities need to be protected;
2. determine priority in light of organizational mission;
3. establish processes to achieve risk management goals.

Function	Category	Subcategory
Identify	Asset Management	• List of hardware devices • Software inventory • Network mapping • Lifecycle tracking
	Risk Management	• Defining Risk Tolerance • Risk Identification • Risk Assessment • Authentication of the Server by the Clients • Analysis of Alternatives
	Compliance	• Business Requirements • Legislative and Regulatory • Contractual Requirements • Technology Certification
	Information Sharing and Communications	• Understand Data Flows • Internal Communications • External Communications • Cryptographic suites versioning and implementation how-to
	Environmental Awareness	• Location of (client-side) end-devices • Location of end-to-end communication infrastructures • Location of (server-side) brokers and vicinity

2.2 Protect

The purpose of this function is to develop and implement the appropriate MQTT safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.

Function	Category	Subcategory
Protect	Security Awareness	• User Awareness Training • Formal Training • Exercise and Evaluation
	Identity, Credential and Access Management	• Use of PKI (e.g. TLS, VPN) • Choose a well-known Certificate Authority • Authentication of Clients by the Server • Authentication of the Server by the Clients • Authorization of Clients by the Server
	Information Protection	• Use of cryptographic suites (e.g. TLS, VPN) • Integrity of Application Messages and Control Packets • Privacy of Application Messages and Control Packets • Non-repudiation of message transmission • Secure Random Number Generation for all involved devices
	Server-side Protection	• Compliance with MQTT specification • Automatic Client disconnect mechanisms • Suspicious behavior detection • Dynamic Access Control Listing (e.g. IP address or Client ID) • Rate limiting and/or blocking (e.g. IP address) • Data-at-rest encryption • Frequent session renegotiation to establish new cryptographic parameters (e.g. replace session keys or change cipher suites)
	Client-side Protection	• Tamper proof end-devices • Proper storage of the client certificate (key management considerations) • Two-factor authentication

2.3 Detect

The purpose of this function is to develop and implement the appropriate activities to identify the occurrence of an MQTT related cybersecurity event.

Function	Category	Subcategory
Detect	Network Monitoring	• Repeated connection attempts

		• Abnormal termination of connections
	Physical Monitoring	• Client availability verification • End-devices and their vicinity physical inspection
	Intrusion Detection	• Repeated authentication attempts • Topic scanning (attempts to send or subscribe to many topics) • Sending undeliverable messages (no subscribers to the topics) • Clients that connect but do not send data

2.4 Respond

The purpose of this function is to develop and implement the appropriate activities, prioritized through the organization's risk management process, to take action in response to a detected cybersecurity event.

Function	Category	Subcategory
Respond	Response Planning	• Revoke lost and/or compromised certificates • Revoke lost and/or compromised Client or Server authentication credentials • Disconnect suspicious or compromised end-devices • Block compromised telemetry channels • Increase Firewall policies • Shutdown compromised brokers and servers

2.5 Recover

The purpose of this function is to develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired through a cybersecurity event.

Function	Category	Subcategory
Recover	Recover Planning	• Perform information system recovery (e.g. restart broker, create new telemetry channels, etc.) • Perform reconstitution activities • Provide alternate work site to recover work activities • Review Firewall policies • Reissue certificates and authentication credentials • Inspect end-devices • Review Key Management and cryptographic deployments • Backup systems • Updated contingency plan

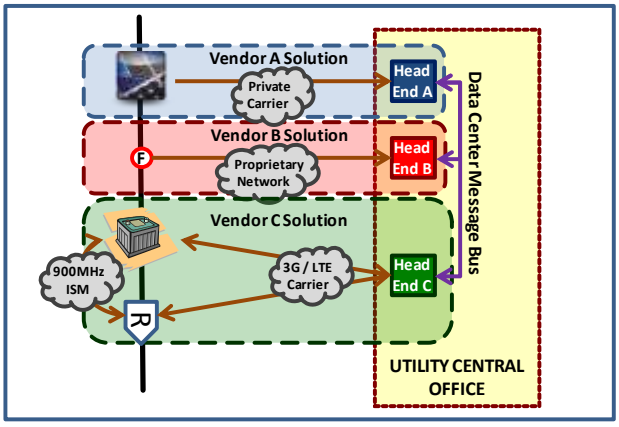
Appendix A. Example Implementation

Large Energy Provider MQTT Bus Architecture

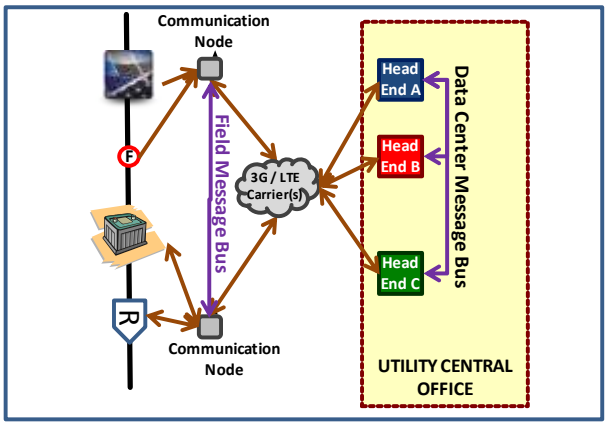
This section provides a worked example to show how the Framework can be applied to help manage MQTT cybersecurity risk. A large energy provider intends to implement an open-source, broker-agnostic, and distributed field message bus architecture based on the MQTT protocol. Protecting the bus architecture is essential because the energy provider is a critical infrastructure.

Context

The organization is looking to build a new architecture around an open-source, broker agnostic 'communication node' concept and is running a pilot project to assess feasibility, and integration within its wider message bus. Its primary role is to facilitate interoperability between the various operational technologies deployed (i.e. SCADA, EMS, DMS, OMS, MDM, etc.) and also augment these technologies by using the MQTT protocol for the efficient sharing and processing of data closer to the asset(s) required for the rapid, reliable, and safe execution of operational functions of all priorities on the electric grid.



Current State – Message Bus at Data Center

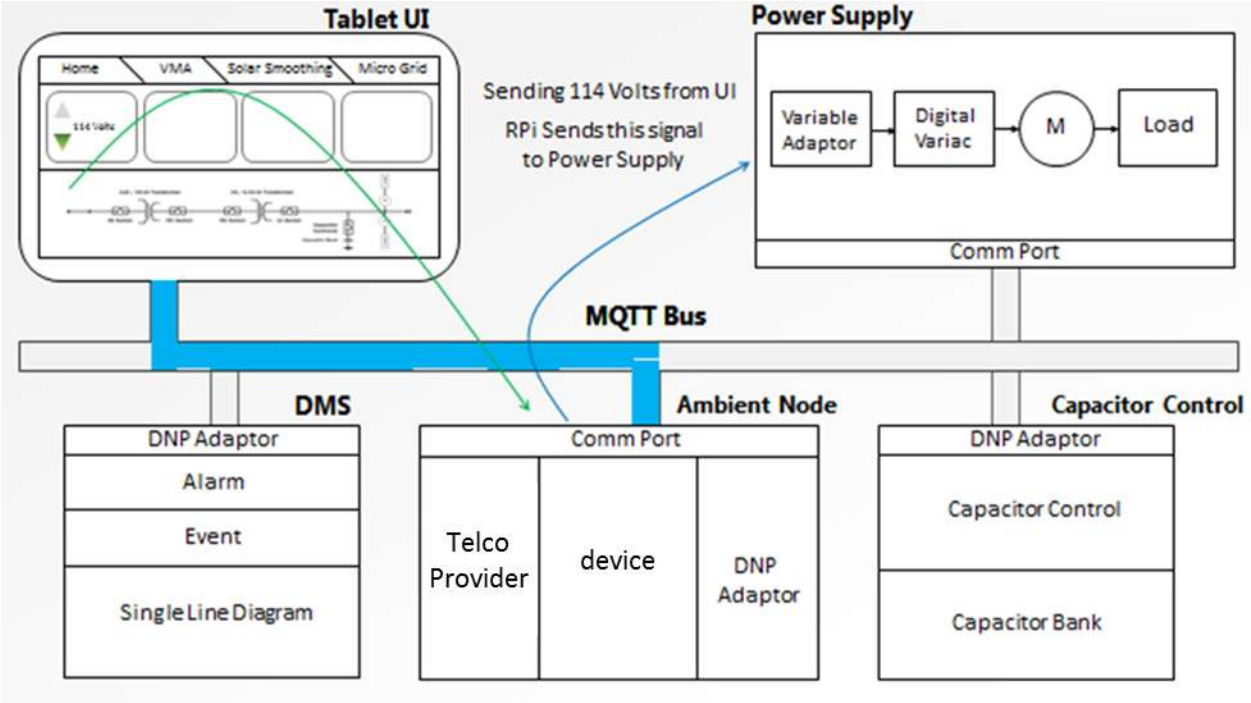


Future State – Message Bus in Field and Data Center

Consequently, using the MQTT protocol will not only improve the simplicity and the integrity of the information exchanges between disparate assets in the field, but also inherently filter a significant amount of unused data overhead and, more importantly, will eliminate the need to backhaul all raw data to a central data center. Fundamentally, these benefits will translate into vast savings in the cost of operating the IT systems and telecommunication networks, but can also achieve further value by enabling deployed control schemes that are not presently feasible without distributed decision-making closer to the electric grid assets.

Test Lab Scenario

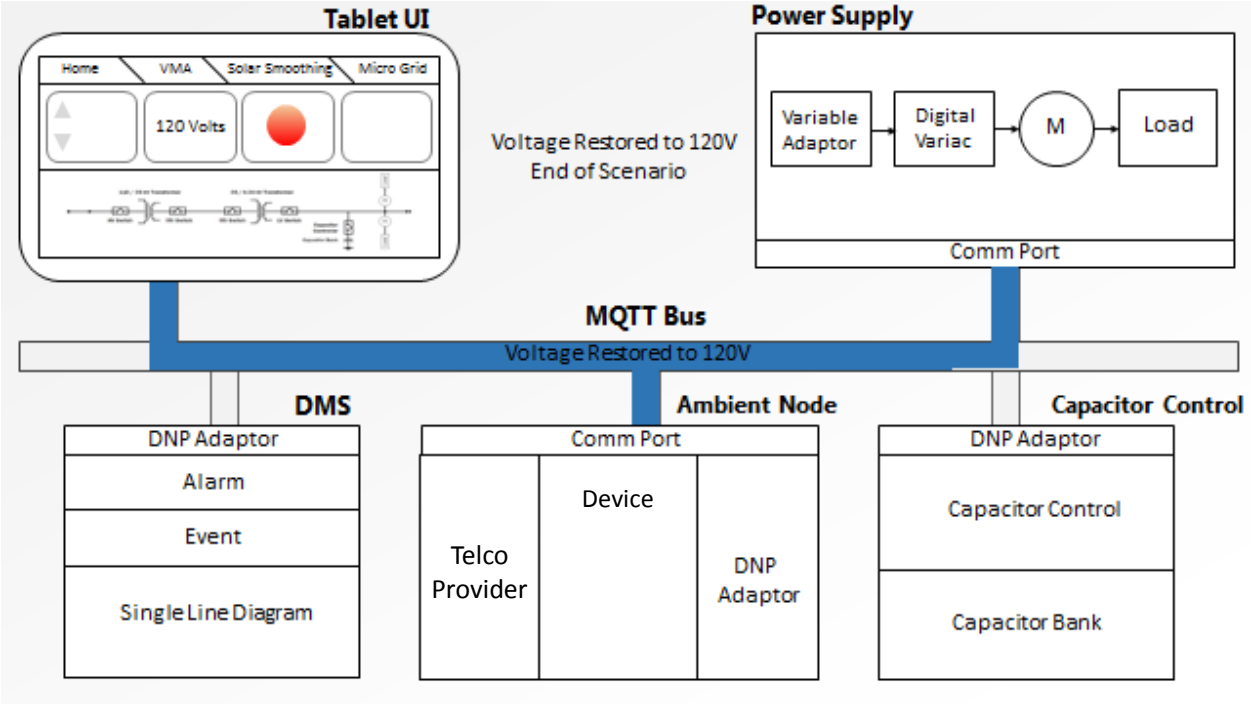
The energy provider is running the following Field Message Bus scenario, based on MQTT. The initial and final state of the system is shown in picture form. The intermediate publish and subscribe steps are described the following paragraph.



Initial State: Scenario starts when the Tablet UI publishes low voltage – 114V.

A Tablet PC is used to control the voltage of a power supply that feeds input voltage to a smart meter. The scenario starts when the Tablet UI publishes low voltage – 114V. The smart meter sees the low voltage and publishes its voltage status change to the distribution management system (DMS). The DMS subscribes and updates its status. The DMS publishes a control command to the cap bank controller to close the cap bank, thus raising the voltage. The cap bank controller publishes its status change – closed – back to the DMS. The DMS subscribes to the cap bank controller status change; it updates its single-line diagram and publishes a raise voltage volt-120 command to the Power Supply who subscribes and makes the change. The meter publishes its voltage status change – 120V. The DMS publishes an updated single-line diagram to the Tablet UI showing the closed cap bank. This scenario is complete when the Tablet UI subscribes to and displays the updated single-line diagram from the DMS.

This simple test scenario reveals the richness, flexibility, and ease of use of publish and subscribe Field Message Bus, MQTT technology. Future plans for the Field Message Bus is to include the necessary security layers: authentication, authorization, encryption, intrusion detection, and quality of trust behavior analytics to the distributed enterprise.



Final State: Scenario ends when the Tablet UI subscribes to raised voltage - 120V and a new single-line diagram from the DMS.

MQTT Cybersecurity Framework

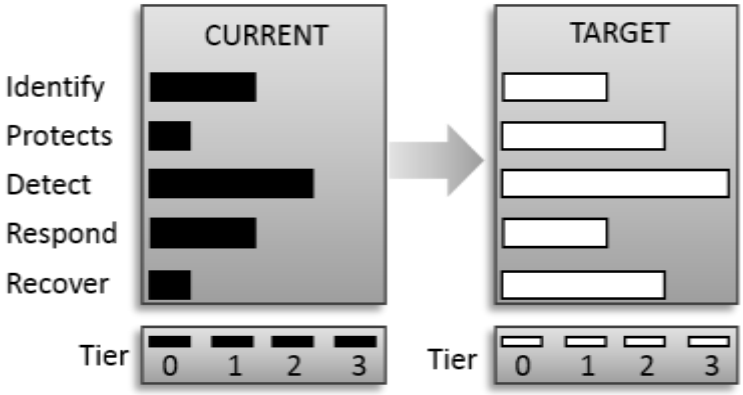
The NIST Cybersecurity Framework document in section 3.2 provides guidance on the steps an organization can take to establish or improve a cybersecurity program.

Following the initial steps the energy provider has developed a Framework Core informed by several recommendation publications such as NIST Special publication 800-26 (Security Self-Assessment Guide for Information Technology Systems" for advice on how to manage IT security and ISO 15408 (Evaluation criteria for IT security) to test the security of the bus architecture. The energy provider has also a list of standards it must comply with imposed by the US government. The Framework Core established for the current MQTT bus architecture is defined below.

Function	Category	Subcategory
Identify	Asset Management	• List of hardware devices • Software inventory • Network mapping
	Risk Management	• Defining Risk Tolerance • Risk Identification • Risk Assessment • Analysis of Alternatives
	Information Sharing and Communications	• Understand Data Flows • Internal Communications • External Communications • Cryptographic suites versioning and implementation how-to
	Environmental Awareness	• Location of (client-side) end-devices • Location of end-to-end communication infrastructures • Location of (server-side) brokers and vicinity
Protect	Information Protection	• User Awareness Training • Identity, Credential and Access Management
Detect	Monitoring	• Network • Physical • Intrusion
Respond	Response Planning	• Revoke lost and/or compromised certificates • Revoke lost and/or compromised Client or Server authentication credentials • Disconnect suspicious or compromised end-devices • Block compromised telemetry channels • Increase Firewall policies • Shutdown compromised brokers and servers
Recover	Recover Planning	• Perform information system recovery (e.g. restart broker, create new telemetry channels, etc.)
	Post Recovery	• Perform reconstitution activities • Provide alternate work site to recover work activities • Review Firewall policies • Backup systems

299

300 Using this Framework Core the energy provider assesses the current Implementation Tier status
301 (in this case at the Function level), conducts a risk assessment of the current operational
302 environment and creates a Target Profile indicating the desired Implementation Tier status for
303 each Function.



The differences between the current and target profiles are analyzed to determine the actions required to bridge the gaps, the results of which are fed into the energy provider's existing cybersecurity program.

Energy Provider Cybersecurity Program

While the majority of the cybersecurity program is concerned with security governance and risk management, there are three distinct sections where MQTT critically interlocks with other compliance processes.

Identify -> Information Sharing and Communications

- Message Flow (internal & external communications)
    - In order to provide resilient global network control, an effective approach is to segregate the organization's data system control plane from the data delivery system. This enables system management processes to analyze control data from message content.
    - It is recommended that the organization's global network QoS levels for the system control plane have a higher priority than the normal data delivery channel. This approach ensures that reconfiguration, partitioning or isolation of internal and external communication channels can be applied without hindrance from the data delivery system.
- Cryptography and versioning
    - Security within MQTT is predominantly TLS. However for the energy provider, there are a number of small form factor/constrained devices such as SCADA control systems that leverage existing light-weight cryptography as well as the prolific AES standard. Thus the energy provider would use TLS, however higher level security process would use PKI management to interoperate with existing Cryptography suites.

Detect -> Monitoring -> Network

- While MQTT is a backbone messaging system, the segregation of the system control plane (with QoS settings) and the message delivery system allows third party monitoring systems easy access to information flow.

Recover-> Post Recovery

- The use, placement and location of persistent and non-persistent MQTT queues has a huge bearing on recovery. For the Energy power provider, MQTT uses non-persistent queues on edge devices and persistent queues for all server side brokers. This approach allows the central services to recover much quicker as the edge devices are always synchronized with the server side MQTT persistent queues.

Appendix B. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Geoff Brown, Machine-To-Machine Intelligence (M2Mi) Corporation
Louis-P. Lamoureux, Machine-To-Machine Intelligence (M2Mi) Corporation
William Bathurst, Machine-To-Machine Intelligence (M2Mi) Corporation
Julien Niset, Machine-To-Machine Intelligence (M2Mi) Corporation
Sarah Cooper, Machine-To-Machine Intelligence (M2Mi) Corporation
Allan Stockdill-Mander, IBM
Richard Coppen, IBM
Andrew Schofield, IBM
Peter Niblett, IBM
Andrew Banks, IBM

Appendix C. Revision History

Revision	Date	Editor	Changes Made
2.0	03/31/2014	Geoff Brown	Incorporated latest JIRAs (200, 206, and 207).

