ADVANCED SMART METER TESTING – TEST-SYSTEM WITH INTEGRATED AMI INTERFACE

Marcel Schönknecht, Florian Becker, Frank Gonzalez
ZERYCON GmbH, ZERA GmbH

Abstract

This publication reports the need for smart meter testing, a test system approach with an integrated AMI interface. The first part of this article pinpoints the general need for testing and how it can be accomplished. The second part is about which details of an AMI interface are important for successful integration. At last, some experiences we have made in the past with different systems are shown.

This paper discusses tools for asserting the proper operation of the AMI from the smart meters to the Meter Data Management (MDM) system. It also considers the data security implications of smart meter testing. For that purpose, End to End (E2E) tests and negative tests are discussed. Furthermore, it outlines the necessities for an Application Programming Interface (API) to be successfully integrated into a test system.

1 Introduction

The build-up process of an AMI is a lot of work and needs to be meticulously prepared. Most important points are the interoperability and the interchangeability. These are the most important subjects for the infrastructure, which allows to integrate components from different manufacturers without losing functionality or even operational readiness. Also, reducing the dependency on suppliers of meters and infrastructure is a massive advantage.

To ensure interoperability, interchangeability, and conformity it is mandatory to test the implementation of the AMI devices. While interoperability and interchangeability serve primarily to cut down on operational and procurement costs, conformity can ensure other requirements, like data security. In turn, data security ensures resilience against cyber-attacks and therefore the reliability of the AMI.

With metrological tests and communication tests the first steps are done. To ensure the proper operation of smart meters with the AMI, E2E tests are commonly used.

2 Interoperability, Interchangeability And Conformity

2.1 Interoperability

Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, in present or future, in either implementation or access, without any restrictions [1].

2.2 Interchangeability

Interchangeability is given as soon as a device can be exchanged for a device from another manufacturer, without compromising functionality or quality [2].

2.3 Conformity

Conformity is the adherence of a product to a standard. It does not necessarily correlate with interoperability and interchangeability.

E.g., a product can adhere to a standard, but if it leaves room for interpretation, the product may be neither interoperable nor interchangeable. This problem is especially prevalent with Device Language Message Specification (DLMS) / Companion Specification for Energy Metering (COSEM) meters.

3 Responsibilities And Dependencies

There are different concepts to operate an AMI and MDMS. From the utilities point of view the major criteria are:

1. Initial costs
2. Operational costs
3. Need to have know-how
4. Dependence on the supplier
5. Responsibility in case of error

The most important criteria should be the independence from supplier and manufacturer. To achieve this goal, the utility should test the meters themselves and operate their own MDMS, or at least carry out quality assurance independently. For this, the utility needs access to the essential information and an interface to the system. This increases the initial costs and raises the need of know-how but will reduce operational costs. The improvement of know-how allows the utility to prevent failures with the infrastructure and the quality will raise.

If the utility gives up sovereignty over the meter, the Data Concentrator (DC), and the MDMS, it is difficult to take responsibility for the proper functionality.

If the supplier hands over the operation of certain parts of the AMI to service providers or the manufacturer, it is very important for the utility to ensure the best quality themselves. For this the systems needs interfaces to enable end-to-end tests.

4 Benefits Of Integrated Ami Interface In The Meter Test System

4.1 Fully Automatic Tests

With focus on metrological tests in combination with communication tests or encrypted meter communication the MDMS interface is the best solution. The test can read all needed information from the MDMS database and use it directly in the test sequence. No manual steps are needed. This also increases the data security and avoids manual failures. Some examples for useful data from the MDMS interface are:

4.1.1 Keys For Encrypted Communication With The Meter

All communication with the meter will be encrypted in the future. In Europe, the smart meter does not provide any information without authentication and encryption. To test the communication interface of the meter or to operate automatic tests, the test system must have access to the cryptographic keys.

To provide the keys via CSV or other plain text file is technically possible, but a worst-case scenario regarding data security.

To use default passwords or keys within the meter to avoid a key or password management is also a very bad idea. One security breach could lead to a security issue for all meters within the infrastructure.

4.1.2 Comparison Of Meter Identification Information

Identification data is printed on the meter case and included in the meter software. An important test is to compare this information. This is common for smart meter testing and showed massive mismatches in the past. To compare this ID with the MDMS data is equally important and can contain mismatches. The “meter id” is one example for more data to compare.

Meters must not be delivered and tested with standard passwords or standard cryptographic parameters for testing purposes. This eliminates the need to change the default settings after the verification. In addition, there is no longer any need to differentiate between test meters and productive meters. This decreases the workload and increases quality.

4.2 End-To-End Tests

With in a test sequence, E2E tests can be combined with metrological tests and communication tests. For this, the meter mounted on the test system is also connected to the AMI. The test system requests the MDMS to operate a particular function with the meter. The MDMS operates the function through the complete communication infrastructure to the meter. It is a test of all components involved.

5 Test Facilities For End-To-End-Tests

E2E testing refers to a software testing method that involves testing an application’s workflow from beginning to end. This method basically aims to replicate real user scenarios so that the system can be validated for integration and data integrity.

Essentially, the test goes through every operation the application can perform to test if the application communicates with hardware, network connectivity, external dependencies, databases, and other applications [3].

An end-to-end test takes care of a chain of functionalities within the whole system. In the context of smart meters, this means that the entire communication path between the meter and the MDMS tested. This test is particularly useful before many potentially faulty meters are installed in the infrastructure. Not only important for type tests, but also for sample tests. The focus is twofold. On the one hand, the meter and the MDMS are addressed directly. This allows detailed tests to be carried out at these interfaces. On the other hand, all components between the meter and the MDMS are tested. However, it is not possible to make a detailed statement about the causes in the event of an error.

In times of material shortages, there are occasional design changes to the hardware of the meters without the manufacturer proactively communicating this. These changes can have qualitative effects on the smart meters and have been uncovered with sample tests in the past. For this purpose, the test system can be used, which is used for the metrological tests and the communication test anyway. There are a few conditions regarding the test facilities that need to be met for this.

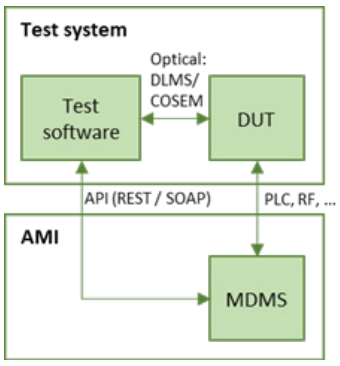

Fig-1: Test facility logical interfaces

To perform end-to-end tests with the whole AMI, the test facility must have a communication interface. There are several specific possible interfaces and protocols. Fig-1 shows a few of them:

1. Interface to the meter on the test bench, e.g., an optical interface.
2. Web based interface to the MDMS or AMI. E.g., via REST or SOAP.
3. Interface between the meter and the MDMS by using power line communication (PLC) or radio frequency (RF) communication.

6 Examples Of End-To-End Tests

There are many possibilities to perform tests from end to end. In this scenario, the meter is mounted on the test bench and is connected to the AMI at the same time. E.g., the test system can perform functionalities by using a web-based interface to the MDMS. Therefore, the test system sends a command to the MDMS to perform one or more functions at the same time.

6.1 Function Tests

In the field, there are several functions an MDMS can perform with the meter. All these functions can be operated by the test system if the interface is implemented. Some examples are:

1. Open or close the load switch
2. Enable or disable customer information on display
3. Read event log / get tempering status
4. Create new billing period (new customer)
5. Read any register, e.g. 1.8.0, 2.8.0, etc.

6.2 Data Mismatch / Open And Close The Load Switch

Opening and closing the load switch is an obvious operation for the AMI. If the database of the MDMS indicates the load switch is closed, how can we be sure? For this, it is very common to perform a load switch opening or closure via the AMI interface and perform a burden measurement of the load switch on the test system. With this combination, we can be sure the command was executed and performed well. In addition, it is also possible to perform a negative test. Disconnect the meter from the AMI and perform the load switch command again. Such a test scenario can also be used for other functionalities.

By now, we have seen different behaviours of different MDMS. One system gives the actual status from the database. The other gives a response with the error message, “meter not connected”. All of this is good. A third system we saw, gives the new status as the response status. But in this case the MDMS was not able to execute the action with the disconnected meter and saved the new status in the database before trying to execute the action. This results in data inconsistency and holds a lot of potential for future errors in the system. To operate this system properly and to trust the information from the MDMS is not possible.

6.3 Timestamp Difficulties

Register values are mostly linked to timestamps and log and temper information. What part of the AMI is responsible for these timestamps? By performing E2E tests, the operator is also able to perform negative tests.

7 Testing Data Security And Negative Testing

A cyber-attack is the malicious presentation of invalid data for the purpose of collecting, disrupting, degrading, or destroying systems or information.

While E2E tests can assert the functionality of a chain of systems in positive cases, they cannot test a single system's reaction to invalid input data. This is what negative tests are for.

With negative tests, a system is fed invalid data to ensure the proper handling of such errors (or attacks). This is especially relevant for security-sensitive areas, such as encryption.

Negative testing does not serve to assert interoperability or interchangeability, but conformity. Nonetheless, it is especially valuable for data security concerns, as the purpose of encryption is, that systems should only be interoperable if authorised.

Most of the time, for the actual encryption a programming library will be used. But this library must be properly parameterised by the system, which is a more likely source of error than the encryption library itself.

Such parameters will rather be used during the establishment of a channel than its usage. Therefore, the test should focus on the establishment phase.

E.g., it is advisable to check the parameters for the Transport Layer Security (TLS) handshake. These parameters can be cipher suites or elliptic curves that have known security issues and should not be used, invalid certificates (e.g., with invalid structures, or invalid signatures), wrong frame-counters (to simulate replay-attacks), or wrong length information (to cause buffer overflows).

To have a basis to test these parameters, standardisation bodies should restrict the usage cipher suites and elliptic curves and only include cryptographic methods that are state-of-the-art. This should be revaluated on an ongoing basis. The US National Institute for Standards and Technology (NIST) publishes guidelines on how to implement TLS, which can be used for orientation [4].

8 Best Practice Mdm System Interface

From our point of view there are features the AMI interface must provide. To give clear and understandable descriptions, this section focuses a web-based AMI Representational State Transfer (REST) JavaScipt Object Notation (JSON) interface with suitable examples.

It is uncertain that the design and the number of calls will match with the mission objective, but there could be errors or gaps. For this reason, the following criteria should be critically examined for each functionality.

8.1 Documentation

The best interface and data format is useless if there is a bad or missing documentation. The documentation must contain every single API call with verb, URL, path parameters, query attributes, request body structure, request body attributes, request examples, response body structure, response body attributes, response examples and valid HTTP response codes.

The documentation should be machine-readable. Typically, an OpenAPI specification can be easily exported based on the interface implemented on the server. At best, the test system has the option to automatically import the interface description as a file.

With this, communication with the MDMS can be performed via the interface without much configuration effort.

In the case of an interface update, the resulting new documentation of the interface can simply be imported into the test system without the need for implementation. This feature helps to be independent from the test system service department and is a massive improvement for the customer.

8.2 Quality Of Response Data

There are different ways to design a response. The easiest way is: "HTTP 200 OK" without any more information. In this case the result of a bad response could be "HTTP 400 Bad Request" or "HTTP 500 Internal server error"

If the interface just provides a standard response without any more information, the automatic validation on the test system is much more difficult and could lead to manual verification of the results. E.g., if the interface provides "HTTP 400 Bad Request – The mandatory attribute1 is empty" the cause of error is clear.

In some cases, there were interfaces that did not even differentiate between HTTP 400 and HTTP 500 errors. That does not allow for any useful conclusions about the cause. Finding such an error is directly associated with a lot of effort.

It should always be possible to distinguish between errors in the communication caused by a component of the MDMS by the meter being unreachable. Restarting an MDMS component remotely is usually easier than driving to the metering point on-site [3].

8.3 Possibility To Query A Status

Status information may be useful for different operations. The best way to ensure that an operation has been carried out properly is to request the status before and after the action is carried out. The change of the status will show the result and is a good basis for the evaluation. If the MDMS claims to have taken an action, the policy should always be independent verification. This can be done by requesting a new status or through another independent interface, such as the optical interface on the meter.

There was a system which was not able to provide status information of the meter. The information was available in the database of the MDMS, but there was no way to request it. Furthermore, this system also had a data inconsistency. When operating the load switch, the new status was not written to the database after the switching was carried out, but before. This status was not corrected in case of failed communication with the meter. At the same time, a response was generated that the action was not carried out successfully leading to a mismatch between the data returned and stored in the MDMS.

8.4 Basic And Advanced Security

The place where the test system is located should not be accessible to unauthorized persons. However, this cannot always be guaranteed. For this reason, IT security should complement physical security.

Encrypted communication between the test system and the MDMS interface must be seen as a minimum level of security. Also, authentication between the communication instances is a security basic. Therefore, the test system must provide TLS encrypted communication for the interface. The certificates and encryption specifications depend on the customer.

To avoid security issues, the data payload,

e.g., encryption keys, can additionally be protected with application layer encryption. This means, the data inside the TLS channel is additionally encrypted. If an unauthorized person gets access to the test system, the data is not accessible in plain text. For this the test system must operate a decryption and encryption software service integrated into the test sequence.

After reading data from the MDMS the test system should neither show nor log security information as plain text. Therefore, specific information can be made incomprehensible for the user but will be decrypted to use within the test sequence.

8.5 Availability And Response Time

Availability and response times are always an issue. The transmission technology with MDMS and the meter already plays a role here. The communication via RF communication may have different reaction times than via PLC. This must be kept in mind while designing the tests.

We have seen a system that polled an RF meter in seconds, while polling PLC meters sometimes took over 30 minutes. In this case, the test sequence may time out and interrupt the test unintentionally.

The PLC communication from more than one meter on the test system may lead to another error. Since PLC uses a shared medium, collisions may occur when meters communicate at the same time. This can be avoided by techniques in the protocol and should therefore be seen as a matter of urgency [5].

To get information of the AMI scalability, load tests can be performed with the test system. If the AMI and MDMS is not able to handle 20 meters on the test system at the same time, it is improbable that it can operate under field conditions.

9 Conclusions

Conducting E2E tests brings an important statement about the quality of the entire AMI and allows utilities to keep independence. It promotes the approach of interoperability and interchangeability to a particularly high level and represents a tool for verification.

To also ensure conformity (and therefore a basic level of data security), E2E testing should be complemented by negative testing. For encrypted communication, tests should focus on cryptographic parameters. For this reason, standards should restrict the usage of cryptographic parameters, such as cipher suites, and elliptic curves.

Regardless of whether the AMI or parts of it are operated by the utility itself or a service provider, the responsibility belongs to the utility. For this, the E2E tests should be conducted by the utility itself. The best way to test a smart meter is the combination of metrological tests, communication tests and E2E tests. It saves time and brings all benefits. Therefore, an interface to the MDMS is required for the test system. There are several ways to establish a secure and well-functioning web-based API, but it also requires know-how.

A test bench with an integrated MDMS interface brings a lot of functionalities in addition to the standard metrological and communication tests and avoids unpleasant surprises in the future. Fully automatic test sequences with highly secured devices under test are the benefit. No more manual steps and, more importantly, no more errors due to manual intermediate steps.

The integration of an MDMS interface into a smart meter test system is feasible and can

be established with a high level of security.

10 References

[1] H. van der Veer and A. Wiles, "Achieving Technical Interoperability - the ETSI Approach," ETSI, 04 2008. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf. [Accessed 08 08 2022].

[2] Y. S. Chow und H. Teicher, Probability Theory, Springer, 1997.

[3] S. Bose, „BrowserStack," 19 05 2021. [Online]. Available: https://www.browserstack.com/guide/end-to-end-testing. [Zugriff am 12 08 2022].

[4] K. A. McKay und D. A. Cooper, „Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations: NIST SP 800-52 Rev. 2," National Institute for Standards and Technology, 29 08 2019. [Online]. Available: https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2. [Zugriff am 12 09 2022].

[5] G3-PLC, "g3-plc.com," 01 03 2022. [Online]. Available: https://g3-plc.com/download/111/user-guidelines/3089/g3-plc-alliance_plc-introduction-for-non-experts_1-2_pub_march2022.pdf.

Author's Biodata

Author:	Marcel Schönknecht
Organization:	ZERYCON GmbH
Contact Details:	+49 2244 9277-245
E-mail id:	mas@zerycon.de
Brief Experience:	Marcel Schönknecht is head of project development at ZERYCON GmbH, Königswinter, Germany. He graduated Ruhr West University of Applied Sciences in Bottrop, Germany with a master's degree in informatics in 2016. He has five years of experiences in Smart Meter testing. In 2019 he already was a speaker at IEEMA Metering India 8th International Seminar of Energy Meters.

Author's Biodata

Author:	Florian Becker
Organization:	ZERYCON GmbH
Contact Details:	+49 2244 9277-246
E-mail id:	fbe@zerycon.de
Brief Experience:	Florian Becker, B.Sc., is a project developer at ZERYCON, Königswinter, Germany. He graduated Ruhr West University of Applied Sciences in Bottrop, Germany in 2018 and has since specialised on secure meter communications, e.g., as a consulting technical expert for the German Federal Office for Information Security for the QA and test development for the relevant German regulation.

Author's Biodata

Author:	Frank Gonzalez
Organization:	ZERA GmbH
Contact Details:	+49 2244 9277-163
E-mail id:	f.gonzalez@zera.de
Brief Experience:	Frank Gonzalez is Project Manager at ZERA GmbH. He has two decades of experience in leading complex meter test system projects worldwide. He is a graduate in Electronics Engineering from University Simon Bolivar in Venezuela.