Single device test requirements for reliable CAN-Based multi-vendor networks

Peter P. Dierauer

By building a system with an open device-level network, the system designer has the option to choose devices from different manufacturers. To minimize the risk that devices will not interoperate correctly in such multi-vendor applications, individual devices need to be tested. This testing must be economical and assure a high confidence level.

Therefore, the industry needs a test concept that allows for clear definition and development of the necessary test sets for individual devices. This document introduces a concept that separates conformance, interoperability, and integrity issues. With this concept and the International Standards Organization (ISO) Open Systems Interface (OSI) 7 Layer Model, the required tests can be developed and performed. This testing concept and its different test strategies are based on Honeywell's Smart Distributed System Test Verification Procedure, which also is explained and discussed.

Introduction

With a very strong trend toward "open" networks, today's system designers have many choices when it comes to selecting devices for their networks. They try to select the manufacturer's products that best suit their application needs. The ability of the selected devices to interoperate as expected in multi-vendor installations is an issue proper testing can address.

When system designers purchase products from a single vendor, the risk that the products will not work together is medium to low. If there is a problem, the designer has a single source of responsibility from which to expect resolution. In this situation, most suppliers provide responsive support because there is no room for debate about where the responsibility lies.

With "open" networks, the situation is different. On one hand, the choice of products is broader. On the other hand, the questions arise: Who takes ownership in case something does not work? To whom do I turn for support?

The device manufacturer has similar problems. How can the company guarantee that its devices will work together with devices from other manufacturers? When a customer calls with a problem, how can the manufacturer determine if the source of the problem lies with its device?

If one set of tests is prescribed for all manufacturers' devices, these risks will be greatly reduced. While this sounds like a simple solution, there remains the questions of which test sets are appropriate and to what degree individual devices need to be tested. Ideally, customers would like testing assurance to reduce the risk of operating problems as much as possible. However, they also recognize that the entire testing procedure must be economical. Therefore, the industry needs to develop a test procedure that guarantees minimal risk at the lowest possible price.

Basic test requirements

To analyze the situation, testing borders must first be defined. At first glance, it seems to make sense to limit testing to the communication channel as this is the interface between different devices. How and how broadly device manufacturers tests their devices to work in the applications of their target markets is generally considered proprietary. These conditions lead to a situation where even if a solid network specification is adopted, manufacturers would only have to assure the correct behavior of their devices' communication channel and only under test conditions.

Another problem is that devices usually provide specific information and data related to their functionality. It is very important that the device's documentation and its implementation is consistent. System designers need to be able to select the right products, based on documentation, to design appropriate information flows.

A device-level network is only an information transport mechanism. The network specification only defines the mechanism for how data is transported. In other words, a network provides a data container or envelope and guarantees the fault-free delivery of this envelope. How the data in the envelope has to be interpreted and in which language the data is presented, is not defined in a network specification. Two different devices are only able to talk to each other when they communicate in the same language.

To structure these possible problems for a discussion of test sets and procedures, it helps to group them into three major areas:

- conformance,
- interoperability, and
- integrity.

Conformance, as it pertains to device-level networks, is the compliance of a device or a system with a network specification.

Interoperability is the fault-free, cooperative communication of different devices on a single network.

Integrity is the fully functional, cooperative interaction of devices in a specific application.

Conformance issues are a subset of interoperability; and interoperability is a subset of integrity. This is because two devices will never work together at all if they do not follow the basic rules of a communication system.

End users are seeking integrity. With that in mind, the appropriate test set has to test on the level of integrity. Manufacturers who are trying to define a test set for single devices face limitations when it comes to testing beyond the network interface. They do not know what kind of network configuration will be implemented in the device application or under what kind of environmental conditions the device will operate. Further, the manufacturer has no idea what the device configuration will be or which data will be transferred to which node in the network.

Such unanswered questions, the fact that nothing can be tested 100 percent, and the economic requirements of testing indicate that a sound testing strategy is imperative.

Conformance testing

Conformance is the basis for reliable communication. Therefore, it makes sense to go far in this area of testing. Manufacturers should try to test everything related to the protocol stack.

The protocol stack defines all the necessary functionality required to communicate between two devices. The network protocol stacks are usually defined according to the ISO OSI 7 Layer Model with implementations of the Physical Layer, Data Link Layer, and the Application Layer.

The Physical Layer describes how data is physically transported over a medium. Signal forms, sample points, switch levels, signal decoding rules, connectors, etc. are defined in this section.

Different market segments often ask for different Physical Layers because the various Layers are often optimized to work in specific environments. Also, the installation praxis can influence which mechanical interface (connector) is preferred. It is important to recognize that this variety represents products intended for different applications.

Usually there are different transceivers defined for specific physical transfer media, such as twisted pair or fiber optic. To define the electrical behavior of these transceiver and receiver circuits is complex, and to design a circuit according to these specifications is expensive. As a result, very often Physical Layer specifications define circuits and provide part lists, or they refer to a standard for which integrated circuits are available for purchase.

If a designer uses the appropriate parts and implements the right schematic, the risk that the transceivers and receivers will not conform is low. This presents the opportunity to use passive testing to verify conformance of this segment.

In passive testing, conformance is verified visually. Circuit schematics are compared with specified circuits. Part lists are compared to critical part lists, etc. Consequently, the manufacturer must be trusted to deliver accurate product documentation. Confidence levels can be increased by running some active tests, such as trying to communicate with the device in worst-case topology conditions (maximum bus length, maximum load, etc.). Active conformance testing involves stimulating a device and comparing the device response to a defined behavior correlated to a defined stimulus.

Another problem that is encountered, especially with Physical Layer testing, involves the fact that the only connection that can be used for active testing is the interface on the Physical Layer to the medium (device connector). This means there is no opportunity to test the different layers independently or to check sub-parts of a layer. As a result, only the entire communication stack can be tested as one piece. A similar problem is encountered with passive testing. Visual verification does not guarantee that the correct parts are used in the actual product.

Therefore, a combination of active and passive testing is the appropriate test strategy for the Physical Layer. Active Physical Layer testing should always be performed under worst-case conditions. About 80 percent of conformance problems in the field are found to be related to the Physical Layer. This reinforces the importance of testing this area carefully.

The Data Link Layer mainly defines the media access and the error handling functionality on the transmission level. These are complex logical functions, and chip sets are commonly available for the different networks.

A static test is used to verify conformance at the Data Link Layer. This is because the chip manufacturer performs extensive testing, making the risk for nonconformance at this level quite low.

The Application Layer (ALP) defines the different services a network stack provides for the application. Usually a device does not support all specified services because some services are not necessary to provide device functionality on the network. However, the device still needs to behave in a specific way if a non-supported service is requested over the network. Therefore, tests still need to be performed on the non-implemented service set. In these test series, one expects to observe the correct behaviors (error messages, device not responding, etc.).

To verify the conformance of an ALP, the dynamic test method is predestined because testing of an ALP requires exchanging all possible messages. This can be automated to enable extensive testing at low cost.

Usually, an ALP can be split into several different sub-groups. The heart of an ALP is the service convention or the protocol engine. This is where the basic services are defined. Intensive testing of this area is very important because the other function blocks in a ALP, such as Layer Management and Node Management, use those basic services.

Special attention must be paid to device-level networks that implement the Physical, Data Link and Application Layer as the Lower Layer Interface (part of the Application Layer). Due to the fact that Levels 3 through 6 are not implemented and defined in those networks, the implementation and presentation of the basic ALP services in the Data Link Layer Protocol Unit must be specified (Lower Layer Interface). This is critical for correct operation of a network.

Conformance testing of an Application Layer usually consists of an extensive message exchange between the device under test and the test host. Consequently, the ALP conformance test is a dynamic test.

Thus far, the test process has established that the data transmission mechanisms are working. Next comes assurance that the device is delivering the correct data. Imagine the problems control engineers would encounter if a system controller asked for a temperature reading and received pressure data in response. Tests must be performed to verify that the device responds as described in the product data sheet.

This need to verify that devices deliver correct data brings up a philosophical question: Is this testing requirement a conformance or an interoperability test? For communication purists, it is definitely an interoperability question because the network is only a mail system. The mail system is not concerned with what is in the envelope. However, to address the market driver of "ease of use," it becomes important for networks to begin to define at least a structure or a language that allows for common descriptions of network accessible data and device functions. This will ensure that all devices that interface to a certain network can be described in the same way. Several different names exist for such a description system (object models, profiles, etc.) There is no consistent definition of those expressions, and each network defines them a little bit differently based on the overall philosophy the manufacturer follows.

In the case of a network that defines such a descriptive language, testing is still in the conformance arena because, as a first step, the conformance of the device description must be verified according to the defined rules. This can be done only with static testing.

In a second step, conformance of the device implementation to the device description must be verified, so that the system designer can design his network information flow based on data sheets. Therefore, a complete test for all defined data and function access options in the different configurations of a device must be run. This testing is dynamic and can be automated very easily. It is a message exchange between the device under test and the test equipment.

The prescribed conformance testing process enables verification of an implementation against existing specifications. It attempts to test as much as possible.

Interoperability testing
The situation is different in the area of interoperability. There is no way to test all the different existing devices in all possible combinations together or to anticipate in which configuration a network will be implemented in a application.
Extensive interoperability tests are meaningful during a system design, where a network can be built up in the required configuration. For a generic test of single devices, two interoperability tests appear to be accurate. Experience shows when using both a non-participative system test and a participative system test more than 80 percent of interoperability problems can be detected.

The non-participative test consists of a defined network where topology, message traffic, and participating devices are defined. The device under test is included in the network but does not participate in the communication. The test is focused on potential network behavior changes caused by connecting and disconnecting the device under test.

In the participative test, the device under test is included in the information exchange. In this case, the test and analysis focus is again on the influence of the device under test according to the totality of network traffic. As a second point, the behavior of the device as it relates to its own messaging activity is analyzed.

Integrity testing
Integrity testing includes even more application-specific unknowns than the interoperability test. However, networks are usually designed for certain market segments, and the solutions for the different application segments reflect only those application requirements. It is obvious that the requirements for a network used in a airplane could be different from a network that connects office PCs. However, we can identify a common requirement and problem area for all networks.

A network has to transport data in a reliable way and, at least today's networks, are built from electrical components. Those electrical components can be influenced by electro magnetic interference, which destroys messages, causes extensive messaging delays, etc. Communication networks are expected to be resistant to such interference or have the ability to recover from it automatically. The problem is that EMI not only effects the network, it effects the devices, too.

Since interference is mainly introduced in the communication system, it makes sense to focus testing on the device's communication system. The most preferred and most common way to implement such device integrity tests for different networks today is to use fast-burst transient tests. Fast transient bursts are introduced in the communication media, and the device's communication-related reactions and recovery behavior on the communication channel are analyzed.

An example of a Verification Test Procedure Specification

Honeywell's Smart Distributed System has a very detailed Verification Test Procedure Specification. The different tests are defined in detail and are tool-independent. All test descriptions include:

- test purpose description,
- definition of the test setup,
- procedure instruction list to execute the test,
- criteria definition for passing the test,
- test checklists, and
- test protocol forms.

The test specification is public, and device manufacturers are able to test their devices prior to official testing at a certified independent test lab.

Different tests are executed and documented based on the exact implementation. For instance, the Smart Distributed System test specification defines several possible connectors or transceivers for which different tests are used.

The Smart Distributed System Conformance Test consists of static and dynamic tests for the Physical Layer. Based on the fact that the Smart Distributed System uses CAN (Controller Area Network) as a Data Link Layer, and the CAN chip supplier (Bosch) tests its variety of available chips according to the CAN specification for conformance, the Data Link Layer tests are only static.

The Application Layer tests are extensive and dynamic. The same is true for the Smart Distributed System's object model implementation testing. The verification of the description is a static test.

The Smart Distributed System's interoperability test set consists of both a non-participative test and a participative system test. In these tests, devices are exchanged, and the device under test is tested under several different network configurations. The tests are designed so that the same tests can be used for system-specific interoperability tests. Therefore, the Smart Distributed System test procedure provides help and guidance for system designers as well as other device manufacturers.

The integrity test consists of a fast transient burst test according to the IEC 801-4 standard test. Test setup and procedure is defined in detail.

The Smart Distributed System Verification Test Procedure is designed to detect failures as soon as possible and to recognize problems to avoid large-scale retesting. The Smart Distributed System goes so far as to verify that the object model (device description) conforms even prior to implementation. This ensures that device developers start with a correct base.

Summary

The test strategies used in the area of single device testing according to device-level network specifications are strongly influenced by the OSI ISO 7 Layer Model. Late implementations are guided by a concept that differentiates between conformance, interoperability, and integrity.

More work is ahead to define and enforce procedures to describe the rules of retesting after product production related changes are made to guarantee ongoing conformance, interoperability, and the integrity of products.

Peter P. Dierauer
Honeywell
11 West Spring Street
Freeport, IL 61032 USA
Phone (815) 266 3176
Fax (815) 235 5623
Pdieraue@micro.honeywell.com