RightPlug Digital Plug Encoding

Introduction

The RightPlug Standard defines requirements for digital encoding of electrical plugs. The types of information stored in encoded plugs and applications that make use of encoded information are virtually unlimited.

This document is intended to provide an introduction to the features and benefits of digital plug encoding according to the RightPlug Standard.

RightPlug Alliance

Background

In the past, new technologies were frequently developed and protected as proprietary to their creators. Some of these technologies achieved widespread adoption as "controlled open" standards where control of the specification remained with the original creator, but use of the standard was permitted to selected third parties under license.

In many cases, several standards competed for one application resulting in wasted resources and significant delay in acceptance of any standard as the market waited for the "winner" to emerge.
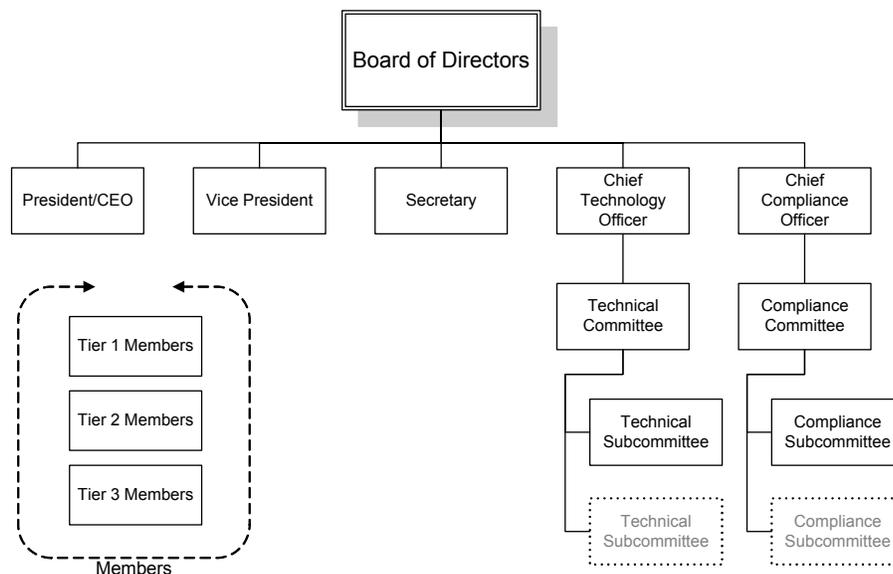
More recently, open standards have become more common with development and extension of the standard controlled by a group of organizations with common interest. In most cases the cooperating organizations are competitors in the market, yet benefit from mutual cooperation in the development of uniform standards.

RightPlug Alliance

Recognizing that digital plug encoding has a variety of applications, it follows that the standard should be developed, extended and maintained in the open environment of an independent organization.

The RightPlug Alliance is a not-for-profit Illinois corporation that develops, maintains and publishes the RightPlug Standard. Membership is open to any organization or individual that is involved in the design or manufacture of electrical products or of ancillary products related to digital encoding of electrical plugs.

As new applications for digital plug encoding are discovered, extensions to the RightPlug standard will become necessary. The RightPlug standard has been designed to facilitate extensions and revisions while maintaining backward compatibility.

Digital Plug Encoding

Key Requirements

- 100% compatible with existing plug standards and test requirements
- International, supports all plug types, not tied to a particular plug form-factor or region
- Data encoding is independent of plug form-factor, open, extensible, and supports manufacturer-specific extensions
- Support for product authentication and immune to duplication using off the shelf components
- Data encoding supports audit trail of a single encoded plug back to source components
- Incorporate existing IEC/ISO standards where practical

Encoding Technology

RightPlug digital encoding is based on the IEC/ISO 14443 Standard for Proximity Identification Cards. The primary application for ISO14443, along with other similar standards, is RFID which primarily relates to identification and tracking of freight and has also found applications in digital payment cards and electronic ticketing.

ISO14443 is one of the shorter range passive technologies, is designed for a maximum read range of 10cm, and is intended for electronic ticketing, electronic payment and identification card applications.
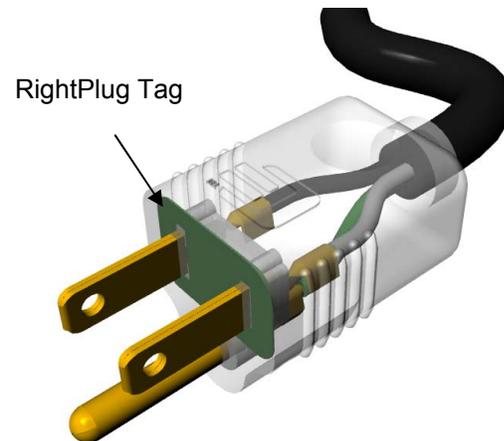
A RightPlug encoding tag incorporates anISO14443B contactless transponder chip with an antenna in a form-factor compatible with an existing plug standard.
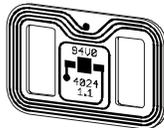
RightPlug Encoding Tag
for NEMA 1-15 & NEMA 5-15 Plugs
(approximately actual size)
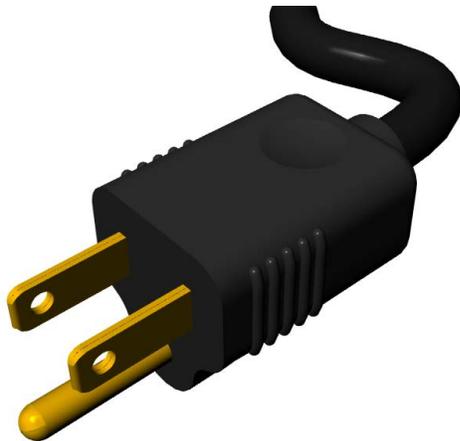
RightPlug Tag

Molded NEMA 5-15 Plug   Embedded RightPlug Tag

Identification

Transponder Chip Identification

Each transponder chip has a 64-bit factory-programmed Unique ID (UID) code. Not only is this code assured to be globally unique, it is assured to be distinguishable from ID codes used by other ISO14443 transponders. It is not possible to use a commercial off-the-shelf transponder to mimic a RightPlug Encoding Tag, although they are compatible in all other ways.

Product Identification

Each manufacturer of RightPlug compliant products is assigned a unique 24-bit Manufacturer ID code (MID). Each product is assigned a 16-bit Product ID code (PID) that is unique within the scope of each MID. The combination of MID and PID is a unique identifier for a particular product.

Additional Product Identification

Manufacturers may optionally assign a 24-bit Lot ID (LID) to each product, in addition to a 16-bit Version/Variant ID (VID) to fully document a particular product.

Privacy

The RightPlug Alliance and its members do not collect or use information linking an individual or individuals to information contained within encoding transponders, except when an individual has specifically granted prior permission for such information to be gathered and used for specific and limited purposes.

For example: an owner of a product may opt to provide personally identifiable information to the RightPlug Alliance in order to receive notification of future product recalls for an encoded product they own.

Application-Specific Extensions

Data Encoding

RightPlug data encoding rules are designed to permit the storage of a wide variety of application-specific data. It is a certainty that certain reader devices will not understand at least some of the application-specific data in a particular tag. RightPlug data encoding is designed to allow a reader to find relevant data and ignore unrelated data in a tag.

Data Type ID

Each data item stored within an encoding tag has a data type ID. Reader devices determine which data items they "understand" by examining the data type IDs. Data Type IDs are assigned by the RightPlug Alliance as new application-specific extensions to the standard are incorporated into the standard.

Original Designer-Manufacturer (ODM) Extensions

Although ODM-specific extensions tend to reduce interoperability and compatibility in an open standard, there are certain product test and configuration applications that are best-supported by such a mechanism. The RightPlug standard has limited support for ODM-specific extensions intended for configuration, test, diagnostic and similar purposes only.
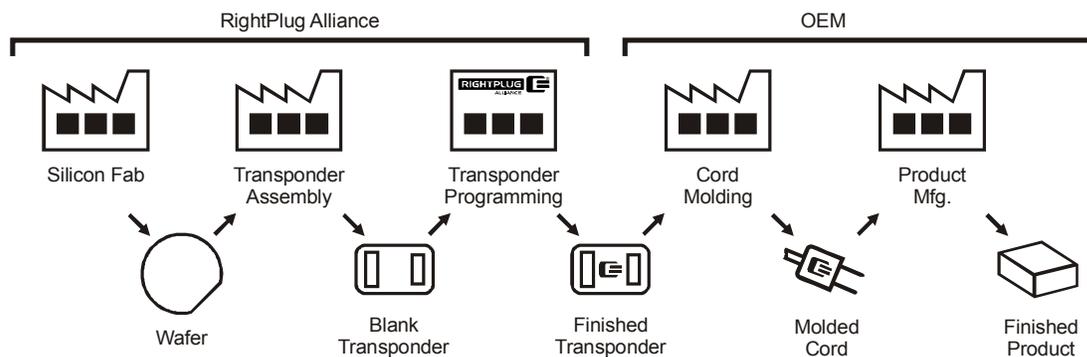
End-Product Authentication

Counterfeit and diverted products are a significant loss for manufacturers worldwide. A means to detect product that has not passed though the legitimate manufacturing and distribution process is a significant tool to help reduce this problem.

Product Authentication Objectives

- Prevent the use of commercially available components to create "cloned" RightPlug Encoding Tags
- Track RightPlug Encoding Tags from silicon wafer to finished goods
- Provide automated means to rapidly validate an individual end-product confirming that it has passed though the legitimate manufacturing process and distribution channel.

Encoding Transponder Process

Authentication Audit Trail

At each step of manufacturing an electronic audit trail is maintained for each individual encoding tag. The RightPlug Alliance maintains the audit trail from silicon wafer to finished programmed product-specific transponder. Manufacturers optionally maintain an audit trail through their own processes including distribution channel and point of sale.

Product Authentication

Stand-alone Authentication

Certain types of devices are unlikely to have external communication capabilities. Basic authentication is possible using just the information present in the encoded plug.

Example: An electrical outlet is designed to operate safely with authentic RightPlug encoded plugs, but may not provide the level of safety expected by the user if a counterfeit (possibly improperly encoded) plug is used. It is desirable for the receptacle to have a high level of confidence that an encoded plug is authentic before delivering power.

On-line Authentication

Some devices are likely to have external communication capabilities either though a direct internet connection or though indirect means via other equipment. Authentication takes full advantage of the audit trail to confirm that the encoding tag in question has passed though the legitimate manufacturing and distribution process.

Example: A hand-held authentication device is used by customs inspection personnel to rapidly validate incoming merchandise while still in its packaging

Forensic Analysis

In addition to product authentication, the audit trail enables detection of product or component diversion. If diverted encoding tags are detected by the authentication process, the audit trail provides evidence that can identify the likely point of diversion to help guide investigating authorities and support any subsequent prosecution.