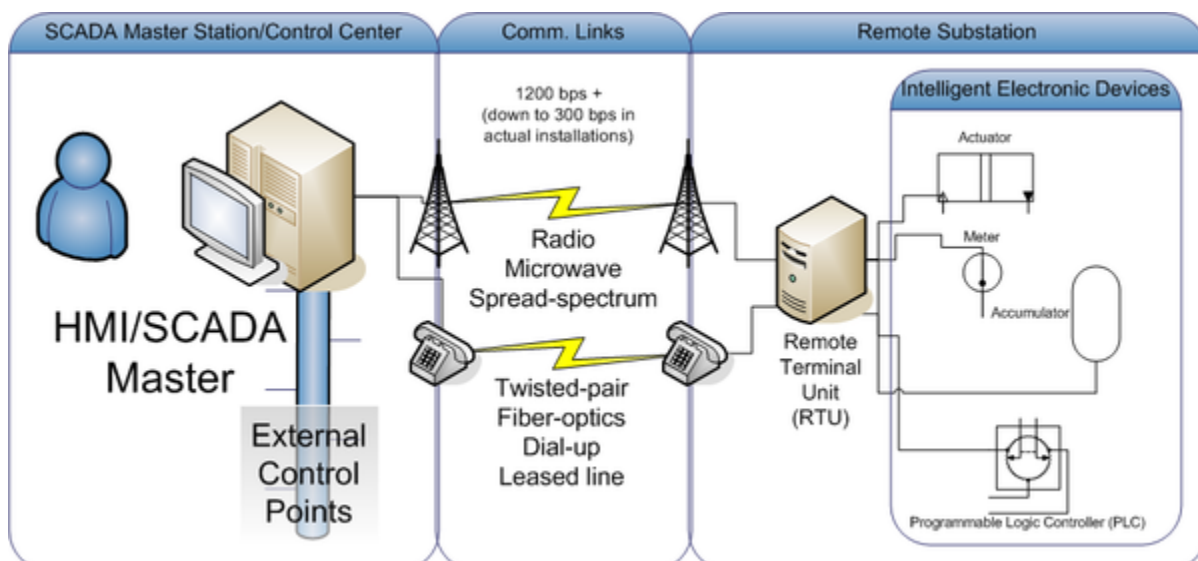


DNP3

Distributed Network Protocol 3 (DNP3) is a set of [communications protocols](#) used between components in [process automation](#) systems. Its main use is in utilities such as electric and water companies. Usage in other industries is not common. It was developed for communications between various types of [data acquisition](#) and control equipment. It plays a crucial role in [SCADA](#) systems, where it is used by SCADA Master Stations (a.k.a. Control Centers), [Remote Terminal Units \(RTUs\)](#), and [Intelligent Electronic Devices \(IEDs\)](#). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter-Control Center Communications Protocol (a part of [IEC 60870-6](#)), is used for inter-master station communications. Competing standards include the older [Modbus](#) protocol and the newer [IEC 61850](#) protocol.



History

While [IEC 60870-5](#) was still under development and had not been standardized, there was a need to create a standard that would allow interoperability between various vendors' [SCADA](#) components for the electrical grid. Thus, in 1993, GE-Harris Canada (formerly known as Westronic) used the partially completed [IEC 60870-5](#) protocol specifications as the basis for an open and immediately implementable protocol that specifically catered to North American requirements. The protocol is designed to allow reliable communications in the adverse environments that electric utility automation systems are subjected to, being specifically designed to overcome distortion induced by [electromagnetic interference](#) (EMI), aging components (their expected lifetimes may stretch into decades), and poor transmission media.

Security

Because [smart grid](#) applications generally assume access by third parties to the same physical networks and underlying IP infrastructure of the grid, much work has been done to add Secure Authentication features to the DNP3 protocol. The DNP3 protocol is compliant with [IEC 62351-5](#). Some vendors support encryption via [bump-in-the-wire](#) for serial communications or virtual private networks for Internet Protocol-based communications. One of the most popular bump-in-the-wire methods began originally as AGA-12 (American Gas Association) in 2003, later becoming IEEE Std. 1711-2010. This standard was subsequently withdrawn March 27, 2014.

The DNP3 protocol is also referenced in [IEEE Std. IEEE 1379-2000](#), which recommends a set of best practices for implementing modern SCADA Master-RTU/IED communication links. These include not just encryption but other practices that enhance security against well known intrusion methods.

It is recommended to use DNP3 with TLS, Transport Layer Security, in accordance with [IEC 62351-3](#).

Technical details

The DNP3 protocol has significant features that make it more robust, efficient, and interoperable than older protocols such as Modbus, at the cost of higher complexity.

In terms of the [OSI model](#) for networks, DNP3 specifies a [layer 2](#) protocol. It provides multiplexing, data fragmentation, error checking, link control, prioritization, and layer 2 addressing services for user data. It also defines a Transport function (somewhat similar to the

function of [layer 4](#)) and an Application Layer ([layer 7](#)) that defines functions and generic data types suitable for common SCADA applications. The DNP3 [frame](#) strongly resembles, but is not identical to the [IEC 60870-5 FT3](#) frame. It makes heavy use of [cyclic redundancy check](#) codes to detect errors.

The improved bandwidth efficiency is accomplished through event oriented [data reporting](#). The Remote Terminal Unit monitors data points and generates events when it determines that the data should be reported (for example, when it changes value). These events are each placed in one of three buffers, associated with "Classes" 1, 2 and 3. In addition to these, Class 0 is defined as the "static" or current status of the monitored data.

The Remote Terminal Unit is initially interrogated with what DNP3 terms an "Integrity Poll" (a combined Read of Class 1, 2, 3 and 0 data). This causes the Remote Terminal Unit to send all buffered events and also all static point data to the Master station. Following this, the Master polls for the event data by reading Class 1, Class 2 or Class 3. The reading of the classes can all be performed together or each class can be read at a different rate, providing a mechanism to create different reporting priorities for the different classes. After an Integrity Poll, only significant data changes are sent. This can result in significantly more responsive data retrieval than polling everything, all the time, irrespective of whether it has changed significantly.

The Remote Terminal Unit can also be configured to spontaneously report Class 1, 2, or 3 data, when it becomes available.

The DNP3 protocol supports time synchronization with an RTU. The DNP Protocol has time stamped variants of all point data objects so that even with infrequent RTU polling, it is still possible to receive enough data to reconstruct a sequence of events of what happened in between the polls.

The DNP3 protocol has a substantial library of common point-oriented objects. The focus of this extensive library was to eliminate the need for bit-mapping data over other objects, as is often done in many Modbus installations. For example, floating point number variants are available, so there is no need to map the number on to a pair of 16 bit registers. This improves compatibility and eliminates problems such as [endianness](#).

A Remote Terminal Unit for the DNP3 protocol can be a small, simple embedded device, or it can be a large, complex rack filled with equipment. The DNP User Group has established four levels of subsets of the protocol for RTU compliance. The DNP Users Group has published test procedures for Levels 1 and 2, the simplest implementations.

The protocol is robust, efficient, and compatible with a wide range of equipment, but has become more complex and subtle over time. Increasingly demanding industrial applications are part of the challenge. Also, SCADA concepts are technically simple but field applications that integrate several types of equipment can become complex to set up or troubleshoot due to variances in vendor implementations.

IEEE Standardization

The IEEE adopted DNP3 as IEEE Std 1815-2010 (<https://dx.doi.org/10.1109/IEEESTD.2010.5518537>) on July 23, 2010.^[1] IEEE Std 1815 was co-sponsored by the Transmission and Distribution Committee and Substations Committee of the IEEE Power & Energy Society, with additional input from the DNP Users Group (<http://www.dnp.org/Pages/AboutUsersGroup.aspx>) .

In April 2012, the IEEE approved Std 1815-2012 (<http://standards.ieee.org/findstds/standard/1815-2012.html>) for publication. IEEE Std 1815-2010 (<http://standards.ieee.org/findstds/standard/1815-2010.html>) has been deprecated. The 2012 version of the standard includes features for Secure Authentication Version 5. The previous version of secure authentication in IEEE 1815-2010 used [pre-shared keys](#) only. The new version is capable of using [Public Key Infrastructure](#), and it facilitates remote key changes.

References

- *1379-2000 – IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation*. 2001. doi:10.1109/IEEESTD.2001.92412 (<https://doi.org/10.1109%2FIEEESTD.2001.92412>) . ISBN 978-0-7381-2639-5.
- *1815-2010 – IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)*. 2010. doi:10.1109/IEEESTD.2010.5518537 (<https://doi.org/10.1109%2FIEEESTD.2010.5518537>) . ISBN 978-0-7381-6312-3.
- *1815-2012 – IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*. 2012. doi:10.1109/IEEESTD.2012.6327578 (<https://doi.org/10.1109%2FIEEESTD.2012.6327578>) . ISBN 978-0-7381-7292-7.
 1. "[Communicate, Collaborate, Cooperate - IEEE Smart Grid](https://web.archive.org/web/20100706091347/http://smartgrid.ieee.org/ieee-smartgrid-news/89-ieee-delivers-critical-1815-dnp3-standard-in-record-)" (<https://web.archive.org/web/20100706091347/http://smartgrid.ieee.org/ieee-smartgrid-news/89-ieee-delivers-critical-1815-dnp3-standard-in-record->

time) . Archived from the original (<http://smartgrid.ieee.org/ieee-smartgrid-news/89-ieee-delivers-critical-1815-dnp3-standard-in-record-time>) on 2010-07-06. Retrieved 2010-08-28.

External links

- [Official website \(https://www.dnp.org/\)](https://www.dnp.org/) 

Retrieved from

["https://en.wikipedia.org/w/index.php?title=DNP3&oldid=1078136308"](https://en.wikipedia.org/w/index.php?title=DNP3&oldid=1078136308)

Last edited 4 months ago by Fffrr