Profinet and Profibus

S.Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Introduction

- PROFIBUS (1989) is based on RS-485 and Profinet (Process Field Network) Introduced in 2003 [IEC 61158].

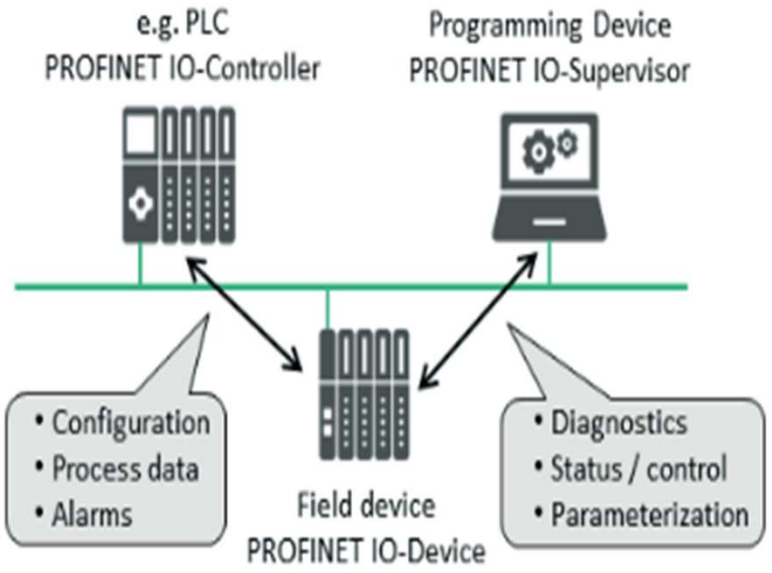
- Profinet (Process Field Network) is an industry technical standard for data communication over Industrial Ethernet, designed
  - for collecting data from,
  - controlling equipment in industrial systems, with a particular strength in delivering data under tight time constraints.

- Profinet defines the entire data exchange between controllers (called "IO-Controllers") and the devices (called "IO-Devices"), as well as parameter setting and diagnosis.

- The Profinet protocol is designed for the fast data exchange between Ethernet-based field devices and follows the provider-consumer model.

Device types

- The **IO-Controller**, which controls the automation task.
  - a PLC, DCS, or IPC; [Master]
- The **IO-Device**, which is a field device, monitored and controlled by an IO-Controller. An IO-Device may consist of several modules and sub-modules.
  - IO-Devices can be varied: I/O blocks, drives, sensors, or actuators. [Slave]
- The **IO-Supervisor** is software typically based on a PC for setting parameters and diagnosing individual IO-Devices.



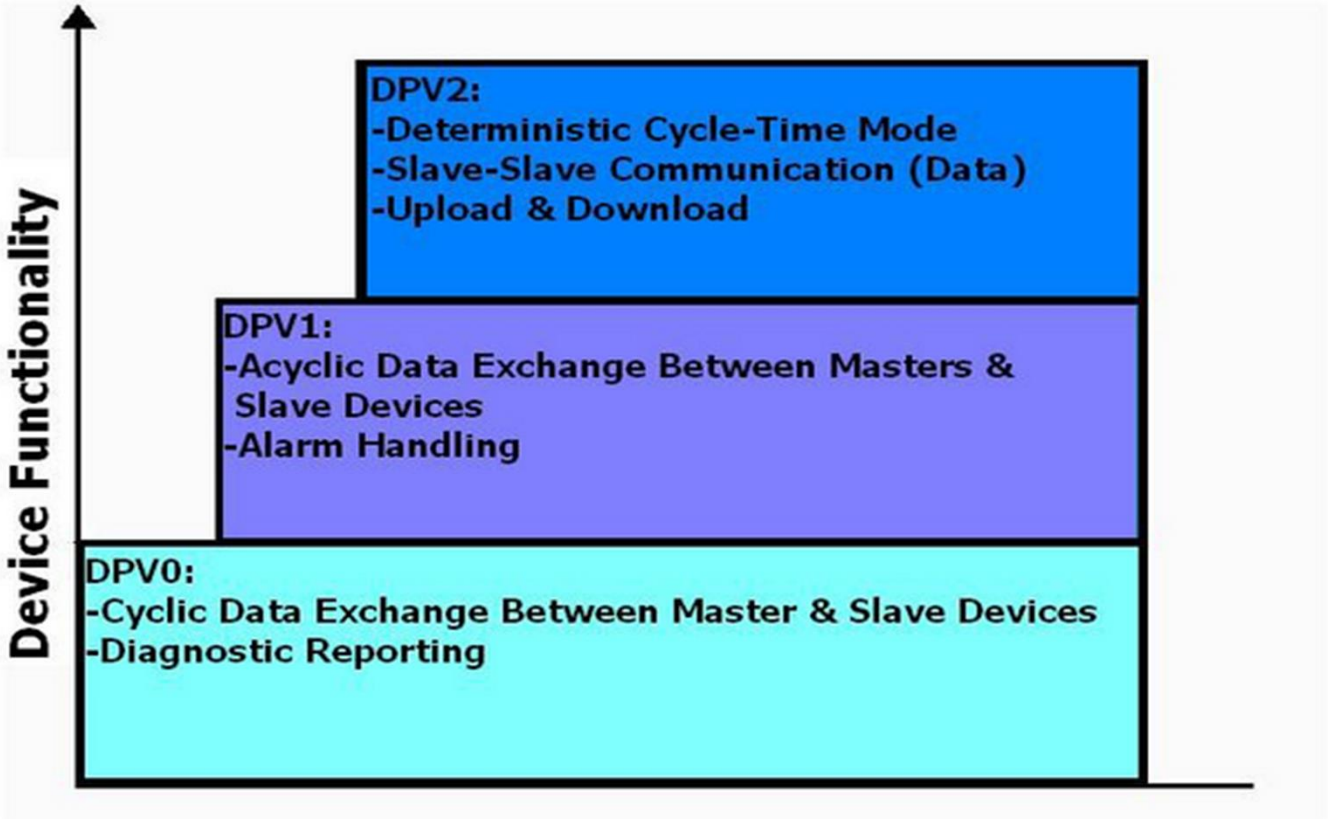
ProfiBUS

- Profibus was designed in the 1990s [contradiction with the first slide] to meet all industrial communication needs for both factory and process automation.

- Profibus is also a master-slave type protocol like Modbus but with an additional token ring protocol to allow for multiple masters.

- All devices go through a startup sequence during which they “join” the network.
  - Each slave maintains a failsafe timer.
  - If the master does not talk to it within a certain time limit, the slave goes into a safe state;
  - the master must then go through the startup sequence again before further data exchange can occur.
  - This, in combination with a watchdog timer in the master, ensures that all communication occurs every bus cycle with a certain time value.

Device Functionality



Communication

- PROFIBUS Master controls the bus in
  - Operate mode, the PLC/DCS sends output data and receives Input data to/from each slave device it is controlling.
  - Data exchanges mode, master exchange data with each slave, does a small amount of bus maintenance and then starts over again.

- Diagnostics - When a slave device detects a change that needs to be reported to the PLC/DCS, it sets a bit that goes to the master along with the input data from that slave's inputs.
  - The next time that the slave with the diagnostic has its' turn in the I/O cycle, the master sends a "get diagnostic" telegram to the slave instead of outputs and the slave responds with the diagnosis instead of inputs.

- When the master reads the diagnosis, the slave turns off the bit that says it has a new diagnosis.

- The master then continues with data exchange to all the other slave devices. The next time through, the master performs data exchange with the slave, just like before.

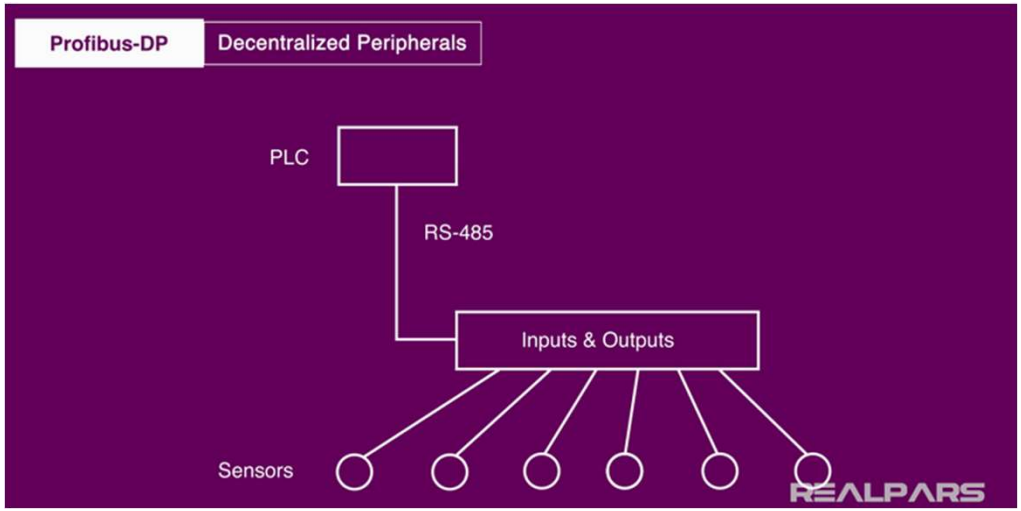
PROFIBUS Decentralized Peripherals (DP)

- The user can select transmission speeds between 9.6 kbps and 12 Mbps.
- It can use wireless, fiber optic and copper
- It works based multi-master token. If there is more than one master than the field devices can be accessed based on master possessing the token.
- Two category of masters
  - 01 – for the process control
  - 02 – for diagnosis, generate alarms and device configuration

PROFIBUS Process Automation (PA)

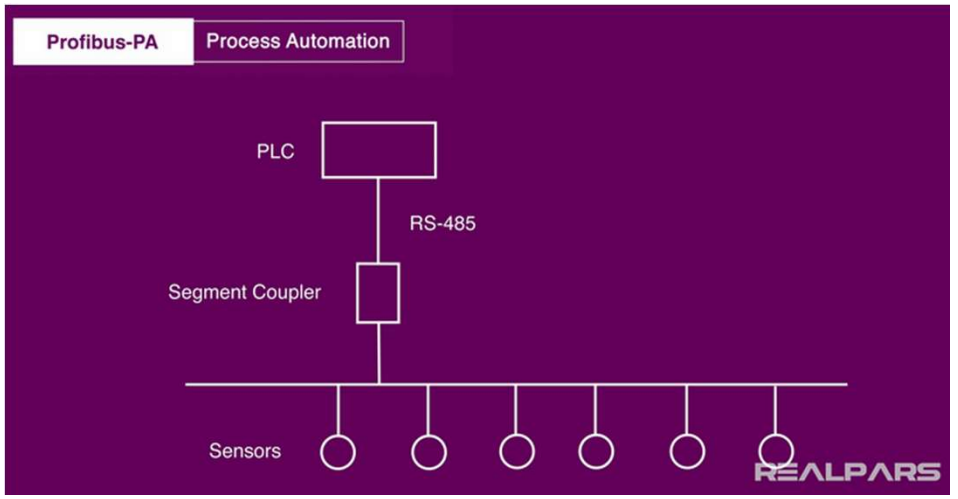
- Uses twisted pair
- Like a Bus Topology
- Uses coupler to convert from PA to DP.
- PLCs do not support PA directly hence we need a coupler

DP and PA



PROFIBUS DP (Decentralised Peripherals)[6] is used to operate sensors and actuators via a centralised controller in production (factory) automation applications.

PROFIBUS PA (Process Automation) is used to monitor measuring equipment via a process control system in process automation applications. This variant is designed for use in explosion/hazardous areas (Ex-zone 0 and 1).



DP Vs DA

Type	**Purpose**	**Technology**	**Baudrate**	**Cable**	**Cable length and restriction**	**Topology**
PROFIBUS DP	Fast	RS-485	Up to 12Mbps	Shielded twisted pair. Data only.	Up to 1200m.	Bus
PROFIBUS PA	Explosion safety (Ex)	MBP-IS	31.25kbps only	Shielded twisted pair. Data and Power supply.	Up to 1900m. Ex-zone.	Bus, star, tree

Physical Layer

- The physical layer for Profibus DP is based on RS-485, which Modbus uses.
- For example, the output from all Profibus PA transmitters is five bytes long.
- The first four bytes are the IEEE floating point value of the process variable.
- The fifth byte is the status byte that indicates whether or not the process variable can be trusted.
- *The major status codes are all standardized in the specification. For example 0x80 indicates everything okay.*

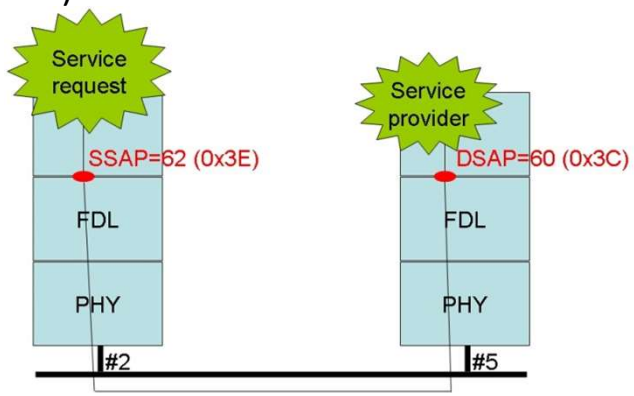
Data Format

Maximum size 244 Bytes in case of variable length

Types:

- Variable Length
- Fixed Length
- Null
- Token

SD	Start Delimiter
LE	Length of protocol data unit
LEr	Repetition of length of protocol data unit, (Hamming distance = 4)
FC	Function Code
DA	Destination Address
SA	Source Address
DSAP	Destination Service Access Point
SSAP	Source Service Access Point
PDU	Protocol Data Unit (protocol data)
FCS	Frame Checking Sequence, calculated by simply adding up the bytes within the specified length. An overflow is ignored here.
ED	End Delimiter (= 0x16)



Clock Synchronization

- In the PROFIBUS DP-V2 version clocks in a PROFIBUS network can also be synchronized.
- For this purpose, a station is defined as the time master which then distributes the time within its network.
- This time master must be a master and is designated as a class 3 master. Other masters are
  - Class-1 master (DPM1) is the central control unit of a system, e.g. a PLC
  - Class-2 masters (DPM2) are used for operation and monitoring purposes as well as during start-up.

Profinet

- A minimal Profinet **IO-System** consists of
  - at least one IO-Controller that controls
  - one or more IO-Devices.

- In addition, one or more IO-Supervisors can optionally be switched on temporarily for the engineering of the IO-Devices if required.

- If two IO-Systems are in the same IP network, the **IO-Controllers can also share an input signal as shared input**, in which they have read access to the same submodule in an IO-Device.

- This simplifies the combination of a PLC with a separate safety controller or motion control. Likewise, an entire IO-Device can be shared as a shared device.

- UDP port number: 34964/49153

Provision for the Critical Infrastructure

- **Safety:** Ensuring functional safety. The system should go into a safe state in the event of a fault.
- **Availability:** Increasing the availability. In the event of a fault, the system should still be able to perform the minimum required function.
- **Security:** Information security is to ensure the integrity of the system.

Data Exchange

- In a master-slave interaction, the master has unidirectional control over all its slave devices and processes.
- The controller will always be the master, and the IO devices will always be slaves.
- The consumer provider model is more flexible. In PROFINET networks, controllers and IO devices can both assume consumer and provider roles, leveraging the full duplex nature of Ethernet.
- The controller provides output data to the configured IO devices in its role as provider and is the consumer of input data from IO devices.
- The IO device is the provider of input data and the consumer of output data.

Addressing

- Ethernet devices always communicate using their unique MAC address.
- In a PROFINET IO system, each field device receives a symbolic name that uniquely identifies the field device within this IO system.
- This name is used for relating the IP address to the MAC address of the field device.
- The DCP (Discovery and basic Configuration Protocol) is used for this.

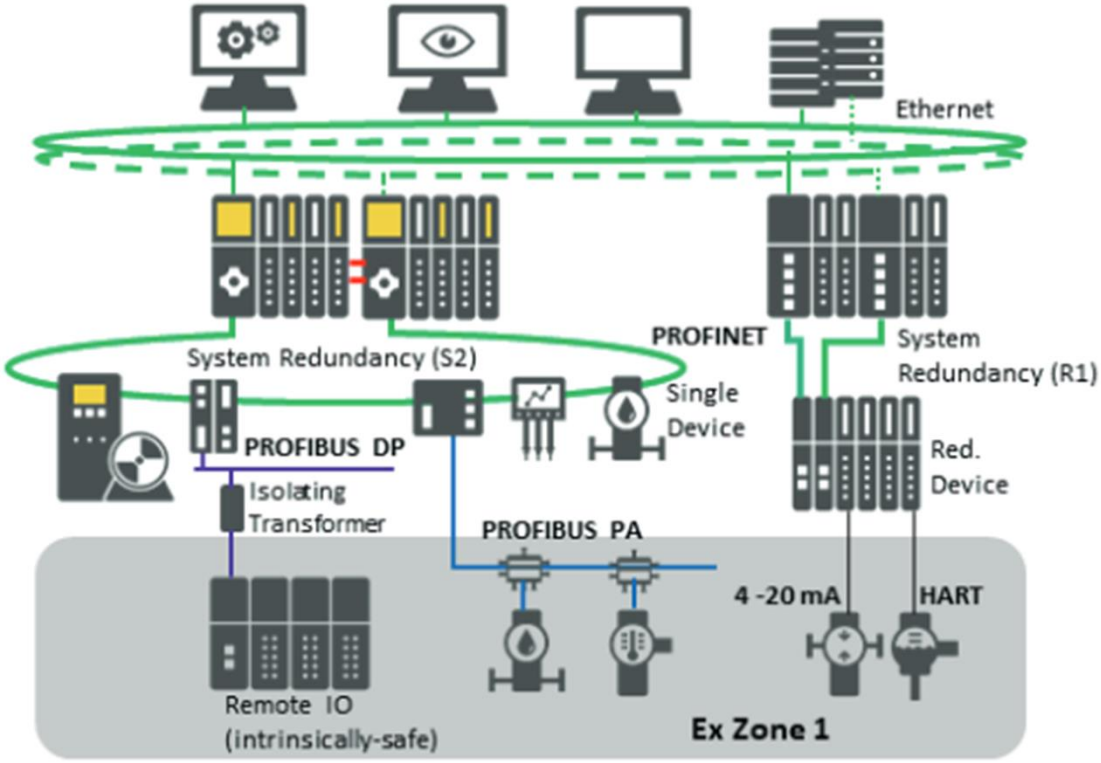
ProfiNet Vs ProfiBus

Parameters	Profibus	Profinet
Data channels	One exactly defined data channel between Master and Slave.	Several data channels between Controller/Supervisor and Device
Number of devices	126 devices maximum	Arbitrary, depends on network
Data transfer rate	Max. 12 Mbit/s	100 Mbit/s with full duplex
Topology	Standard: star and tree Possible: bus and ring	Standard: line Possible: tree and ring
Wired transmission technology	PROFIBUS over copper or fiber-optic cable	Industrial Ethernet over copper or fiber-optic cable
Wireless transmission technology	Infrared transmission is possible	Industrial WLAN (Wireless Local Area Network) is possible

Fail-safe (F)

- It is the ability to reliably protect a system from hazards or to reduce the risk to an acceptable level with corresponding technical and organizational measures.
  - a consecutive numbering of F-messages ("sign-of-life"),
  - a time expectation with acknowledgment ("watchdog"),
  - an identifier between sender and recipient ("F-address")
  - a data integrity check (Cyclic Redundancy Check, or CRC).

PROFINET in process automation



https://www.profibus.com/index.php?eID=dumpFile&t=f&f=207029&token=5ec409c02dbe77dedc621d2b7c7b6eee73c7c275

Security Classes

- Class 1 is where we tighten up security for the Discovery and basic Configuration Protocol (DCP) (making it read only) & SNMP protocols (Community String - Password), and protect General Station Description (GSD) files (Certificate).

- Class 2 is where we use authenticity between a controller and a device to ensure a device is allowed to be on the network. This helps prevent man-in-the-middle attacks.

- Class 3 is where we are actually encrypting the real-time I/O data in case you are concerned it contains sensitive information like recipes, formulas, or other trade secrets.

References

- PROFINET System Description: Technology and Application [https://www.profibus.com/index.php?eID=dumpFile&t=f&f=51714&token=4ea5554cbb80a066e805a879116ead2a759c23c3]
- https://en.wikipedia.org/wiki/Profinet
- https://netilion.endress.com/blog/profibus-network-iiot-services/
- https://realpars.com/profibus/
- https://instrumentationtools.com/how-profibus-communication-works/
- https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/profibus-overview.html
- https://profinews.com/2023/01/profinet-security-classes-1-2-3/
- https://www.felser.ch/profibus-manual/service_access_point.html