Device & Datapoint Onboarding

Sebastian Käbisch

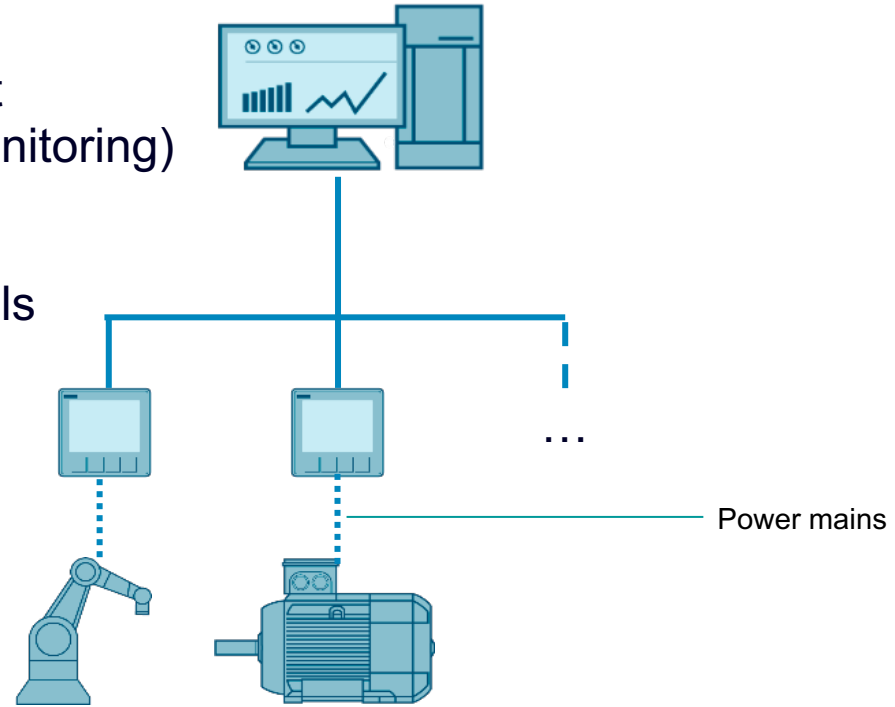
SIEMENS

Siemens-Volkswagen Energy Management Show Case
(will be presented at HMI 2022 @IDTA_Booth)

High integration effort
(e.g., energy data monitoring)

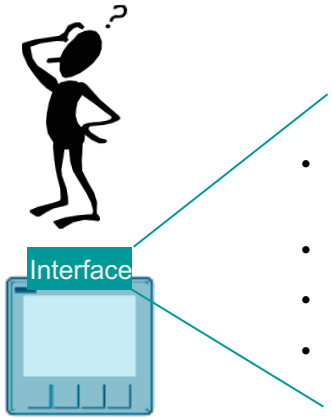
Multiple com. protocols
(e.g., Modbus)

Multiple vendors



SIEMENS

How to get Communication / Datapoint Metadata of the Assets Today?



- Electronic device / interface descriptions (e.g., EDDL, FDI, nodeset, …)
- Manuel (PDF, HTML,…)
- CVS, Excel, …
- Source Code

What kind of data do you serve?

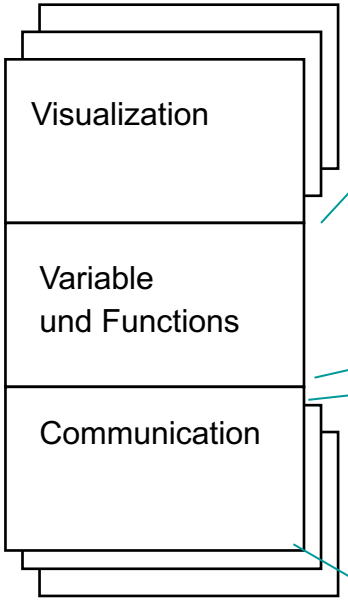
What kind of functions do you have?

How can I access the data/function?

…

SIEMENS

Example I / III
Electronic device / interface description: EDDL




```
VARIABLE Measured_value
{
 LABEL    "Temperature";
 HELP     "Measured process value";
 CLASS    INPUT;
 TYPE                    FLOATING_POINT
                         {
                                 DEFAULT_VALUE=0;
                         }
}
VARIABLE hi_lim
{
 LABEL"Upper range limit";
 HELP  "This parameter is a hint to the operator, i.e. a low prior alarm"

 CLASS          INPUT;
 HANDLING READ & WRITE;
 TYPE  FLOAT
   {
         MIN_VALUE     0.0;
         MAX_VALUE     100.0;
   }
}
...
COMMAND read_device_status
{
 NUMBER                  137;
 OPERATION               READ;
 TRANSACTION
         {
                 REQUEST {}
                 REPLAY          {
                                   response_code, device_status,
                                   parameter_errors
                                 }
         }
 RESPONSE_CODES
         {
           0,    SUCCESS,                    [no_command_specific_error];
           6,    MODE_ERROR,                 "Module Device Link Broken";
         }
}
...
```

Source:
Prof. Christian Diedrich, Lecture “Automatisierungssysteme”,
University Magdeburg

SIEMENS

Example II / III
Manuel (Web): Siemens SENTRON PAC Energy Meter

Content | Search | Index

- PAC4200
  - Introduction
  - Description
  - Installation
  - Connection
  - Commissioning
  - Operation
  - Parameterizing
  - Service and maintenance
  - Technical data
  - Dimensional drawings
  - Appendix
    - Load profile
    - Modbus
      - Modbus
      - **Measured variables without a time stamp with the function codes 0x03 and 0x04**
      - Structure – Digital inputs status and digital outputs status with the function codes 0x01 and 0x02
      - Structure – Limit values with the function codes 0x01 and 0x02
      - Structure – PMD diagnostics and status with the function codes 0x03 and 0x04
      - Measured variables for the load profile with the function codes 0x03 and 0x04
      - Tariff-specific energy values in double format with the function codes 0x03, 0x04, and 0x10
      - Tariff-specific energy values in float format with the function codes 0x03 and 0x04
      - Maximum values with a time stamp and the function codes 0x03 and 0x04
      - Minimum values with a time stamp and the function codes 0x03 and 0x04
      - Odd harmonics without a time stamp with the function codes 0x03 and 0x04
      - Odd harmonics with a time stamp with the function codes 0x03 and 0x04
      - Readout of harmonic components of all harmonics with function codes 0x03, 0x04 and 0x14
      - Readout of averages (aggregation) with function codes 0x03, 0x04 and 0x14
      - Configuration settings with the function codes 0x03, 0x04, and 0x10
      - Value range for limit source
      - Communication settings with the function codes 0x03, 0x04, and 0x10

Entry type: **Manual**, Entry ID: **34261595**, Entry date: **05/27/2019** ★★★★½ (7) › Rate

System Manual SENTRON PAC4200 Power Monitoring Device

Document: PAC4200 (05/2019, English)
Type of topic: Fact

Measured variables without a time stamp with the function codes 0x03 and 0x04

Addressing the measured variables without a time stamp

The SENTRON PAC4200 Power Monitoring Device provides measured variables with or without a time stamp.

Note

Error in the case of inconsistent access to measured values

Please ensure the start offset of the register is correct when making **read accesses**.

Please ensure the start offset and the number of registers are correct when making **write accesses**.

If a value consists of two registers, a read command applied in the second register, for example, will generate an error code. The SENTRON PAC4200 will also output an error code if, for example, a write operation ends in the middle of a multi-register value.

Table: Measured variables available without a time stamp

Offset	Number of registers	Name	Format	Unit	Value range	Access
1	2	Voltage L1-N	Float	V	-	R
3	2	Voltage L2-N	Float	V	-	R
5	2	Voltage L3-N	Float	V	-	R
7	2	Voltage L1-L2	Float	V	-	R
9	2	Voltage L2-L3	Float	V	-	R

Modbus TCP port, configurable

Ports are communication channels which make it possible to access a Modbus-capable device via a network.

Standard IP ports like port 502 are often tested by port scanners. If an open port is discovered by an attacker, the device can be attacked via this port.

Definition "Advanced Data Identifier"

The "advanced data identifier" has a length of 5 bytes. It consists of an object ID (4 bytes, format "unsigned long" big endian) and the number (1 byte) of data records required in the response frame.

Details for protocol binding:

- Function Codes:
  - 0x03 → readHoldingRegisters
  - 0x04 → readInputRegisters
- Port: 502
- Offset & No. Register (pro Datenpunkt verschieden)
- Byte Order: Big Endian
- Byte Länge: 4

Datapoint metadata:

- Name
- Type
- Unit
- Ranges
- lese-/schreibbar

SIEMENS

Example III / III
Excel: PHOENIX CONTACT Energy Meter

CH	Dec	Hex	Count	Unit	Divider	R/W	Datatype	Default	Name (DE)
H2	**32768**	**8000**	**88**	**46**					**Messwerte**
R	32768	8000	2	V	1	R	FI32		Außenleiterspannung U12
R	32770	8002	2	V	1	R	FI32		Außenleiterspannung U23
R	32772	8004	2	V	1	R	FI32		Außenleiterspannung U31
R	32774	8006	2	V	1	R	FI32		Leiterspannung U1
R	32776	8008	2	V	1	R	FI32		Leiterspannung U2
R	32778	800A	2	V	1	R	FI32		Leiterspannung U3
R	32780	800C	2	Hz	1	R	FI32		Frequenz
R	32782	800E	2	A	1	R	FI32		Strom I1
R	32784	8010	2	A	1	R	FI32		Strom I2
R	32786	8012	2	A	1	R	FI32		Strom I3
R	32788	8014	2	A	1	R	FI32		Strom IN
R	32790	8016	2	W	1	R	FI32		Gesamtwirkleistung
R	32792	8018	2	var	1	R	FI32		Gesamtblindleistung vektoriell

SIEMENS

Problem Statement

- Vendors uses different sources or technologies to describe datapoint / communication metadata
  - Electronic device / interface descriptions (depends on industry sector and specific communication protocols)
  - PDF, Web pages, …
  - Excel, CSV,…
  - …

- In manuals, different vendors describe identical datapoints in a different way, e.g.,
  - Datapoint naming:
    - “Voltage L1-N” vs “Leiterspannung U1”
  - Addressing:
    - offset vs hex
    - count vs number of registers
  - Datatype system:
    - Float vs FI32
  - …

- Typically, semantic context is missing such as known from
  - ECLASS IRDIs
  - semanticIDs (from AAS)
  - …

Impact

- → If no electronic device / interface description exist, onboarding typically results to an expensive process
  - e.g., SENTRON PAC offers up to 87 different datapoints
  - c&p the metadata in engineering tools or application source code
  - …
- → Risk of error proneness
  - wrong calculation or interpretation (e.g., offset vs hex)
  - number twister
  - …
- → Errors are usually detected late and are sometimes difficult to fix
  - Debugging is usually time-consuming and resource-intensive
  - …