# Lab 2: Introduction to Modbus TCP

**Christos Dalamagkas, PPC SA**
**Marios Siganos, K3Y Ltd**

**23/8/2023**

**Sofia, Bulgaria**

**c.Dalamagkas@dei.gr**

Co-funded by the
Erasmus+ Programme
of the European Union

Course material developed in collaboration with Technical University of Sofia, University of Western Macedonia, International Hellenic University, University of Cyprus, Public Power Corporation S.A., K3Y Ltd and Software Company EOOD with support from Erasmus +

# Agenda

1. Discussion on Industrial IoT protocols
2. Background of Modbus TCP
3. Remote Labs setup
4. Lab 2: Introduction to Modbus TCP

# Application Layer Protocols

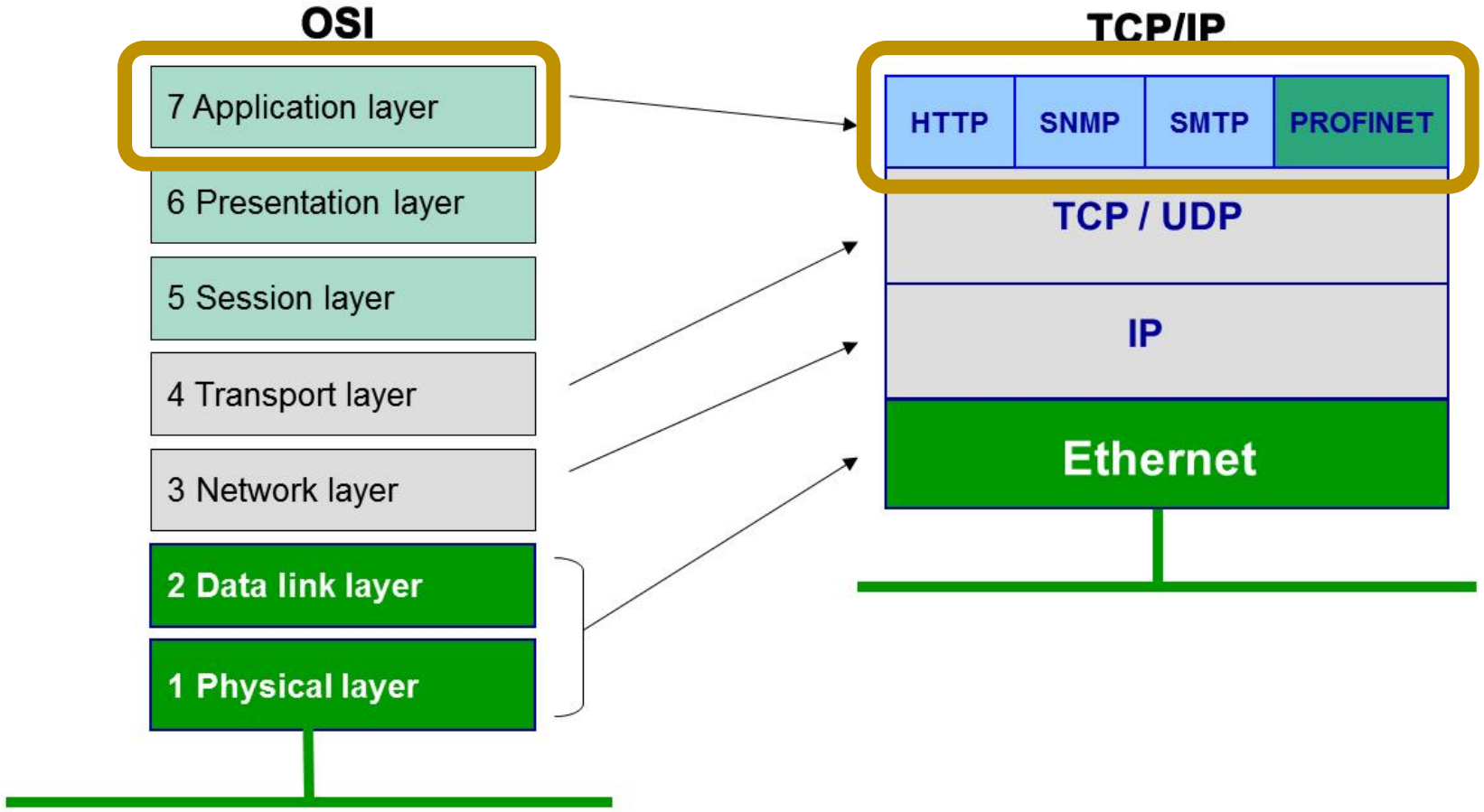



Fig. 2: https://www.motioncontroltips.com/what-is-the-application-layer-in-an-industrial-network/

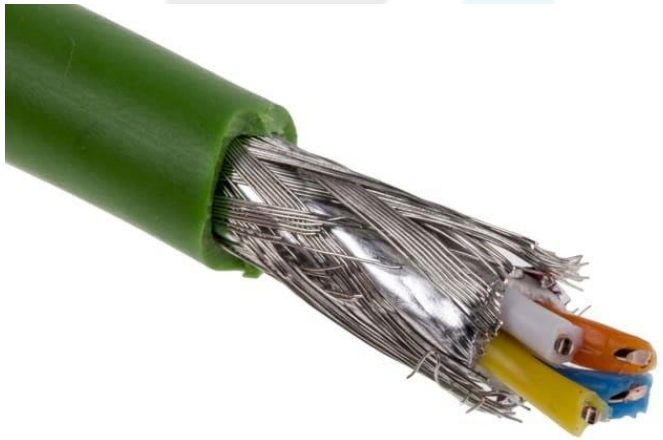
# Industrial Communications

- Historically, data communications in industrial context have been carried out through serial fieldbus protocols (e.g., PROFIBUS, CAN, Modbus)
- Limitations of fieldbus protocols:
  - Low bit-rate / Low transmission speed
  - High cost – need for dedicated infrastructure
- Industrial Ethernet tends to replace fieldbus technologies:
  - Greater bit-rate
  - Integration with IT infrastructure
  - More topology options
  - Easier to expand
  - Easier to get technical support
  - Multiple protocols over the same infrastructure
  - Integration with wireless and optical fibre networks

# Industrial Ethernet

Based on the IEEE 802.3 standard – Its Ethernet applied in industrial context:

- Communication protocols for specialized use cases
- Quality of Service
- Improved medium – Resistance to interference, endurance



JAUNTY Erasmus+

# Industrial IoT Communication Protocols















# Modbus

- Developed in 1979 by Modicon (now Schneider Electric).
- Very simple protocol for industrial environments.
- Allows to remotely read and write the contents of memory addresses.
- Can run over TCP/IP – Originally the protocol run over a serial cable (Modbus RTU).
- Follows the client/server model (formerly master/slave)
  - The client sends a reading request to a Modbus server (e.g., a metering device) about the value of a specific address.
  - The Modbus server responds with the requested value.

# Modbus

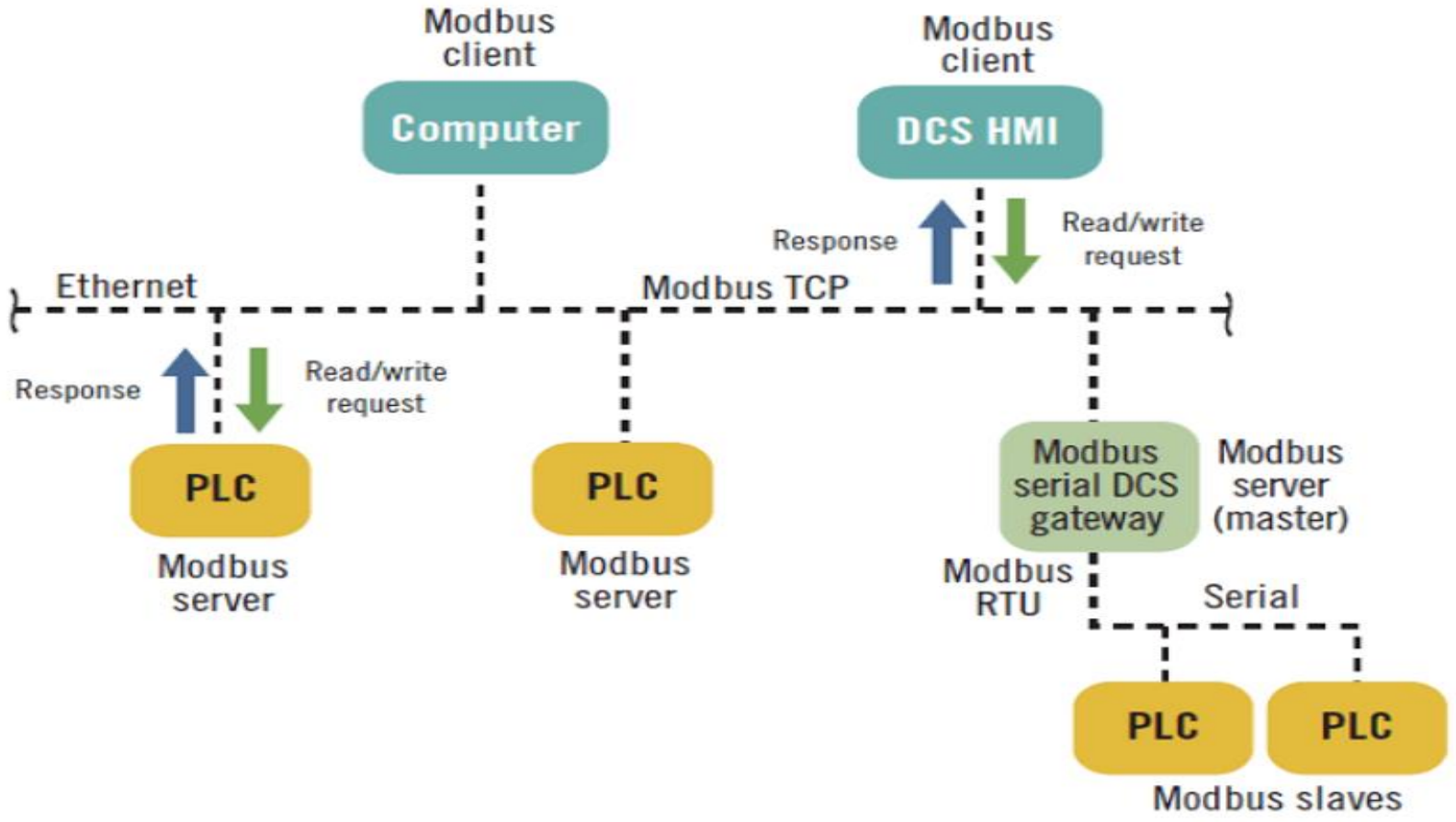



Fig. 21: https://www.controlglobal.com/articles/2019/introduction-to-modbus/

# Modbus Terminology

**Unit ID** (or slave ID): Inherited by the Modbus RTU variant, indicates the unique address of the device on the bus (1-254). On Modbus TCP, this may be ignored.

**Function code**: The Modbus operation that takes place (e.g., discrete input, diagnostic, etc)

**Modbus address**: A “location” inside the device memory, where a specific metric/value is stored.

**Modbus register map**: A document that specifies the Modbus addresses and the supported function code for each address

# Most common function codes in Modbus TCP

| Function name | Function code (decimal) | Memory type |
|---|---|---|
| **Read Discrete Inputs** | 2 | Discrete input (read-only memory type) |
| **Read Coils** | 1 | Coil (read/write memory type) |
| **Write Single Coil** | 5 | |
| **Write Multiple Coils** | 15 | |
| **Read Input Registers** | 4 | Input register (read-only memory type) |
| **Read Multiple Holding Registers** | 3 | Holding register (read/write memory type) |
| **Write Single Holding Register** | 6 | |
| **Write Multiple Holding Registers** | 16 | |

# Modbus

```
15.266493     10.0.0.57          10.0.0.3          Modbus…    66    Query: Trans:     0; Unit:  10, Func:   8/  1: Force Listen Only Mode
```

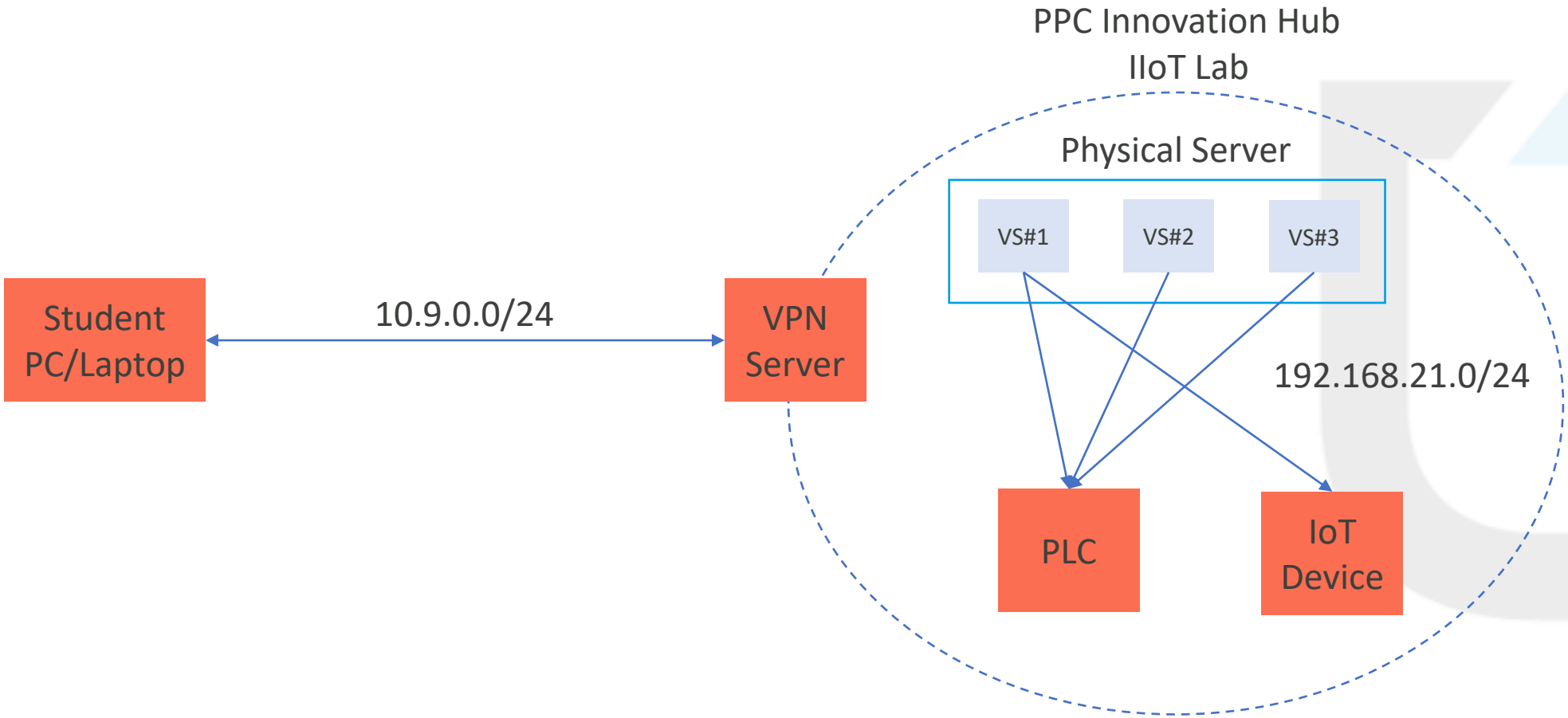
```
▾ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 10
▾ Modbus
    .000 1000 = Function Code: Diagnostics (8)
    Diagnostic Code: Force Listen Only Mode (4)
    Data: 0000
```

```
15.268405     10.0.0.3           10.0.0.57         Modbus…    63 Response: Trans:     0; Unit:  10, Func:   8: Diagnostics. Exception returned
```

```
▾ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 3
    Unit Identifier: 10
▾ Function 8:  Diagnostics.  Exception: Gateway target device failed to respond
    .000 1000 = Function Code: Diagnostics (8)
    Exception Code: Gateway target device failed to respond (11)
```

# Remote Labs Setup

# Remote Labs Setup



# Thank you for your attention!