SIU Southern Illinois University CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 8: Industrial Network Protocols

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Industrial Network Protocols

- Modbus
- DNP3

Recall: ICS vs SCADA vs Enterprise

Function	Industrial Control	SCADA	Enterprise
Real-time operation	Critical	High	Best Effort
Reliability Req.	Critical	High	Best Effort
Bandwidth Req.	Low	Low/Medium	High
Latency	Low, Consistent	Low, Consistent	NA, Retransmission is acceptable
Protocols Used	Realtime	Realtime	Non realtime

What is Real time in Networks?

Term used to refer to any live telecommunications that occur without transmission delays

Real time communication (RTC) is nearly instant with minimal latency

RTC data and messages are not stored between transmission and reception

RTC is generally a peer-to-peer,

- Rather than broadcasting or multicasting, transmission

WebRTC

Importance of Industrial Network Protocols

To understand how industrial networks operate

- Where they are used, why?
- Specialized protocols for industrial automation and control

Most industrial protocols are designed for real-time operation to support precision operations

- Forgo any feature or function that is not absolutely necessary, for the sake of efficiency
  - Including security; authentication and encryption
- Some of these protocols run over IP Networks

Overview of INPs

SCADA and/or fieldbus protocols

- SCADA -> Communication of supervisory systems
- Fieldbus -> Communication of industrial, automated systems
- Most protocols are interchangeable

Realtime protocols

- Designed for serial communication
- Evolved to operate on Ethernet (IP network)

A few most common INPs

Modicon Communication Bus (Modbus)

Distributed Network Protocol (DNP3)

Inter Control Center Protocol (ICCP)

Object Linking and Embedding for Process Control (OPC)

Modbus

Was designed in 1979 by Modicon (now part of Schneider Electric) that invented the first Programmable Logic Controller (PLC)

Has been widely adopted as a de facto standard and has been enhanced over the years into several distinct variants

- Ease of use:
  - Raw messages without restrictions of authentication or excessive overhead
- Open standard, free distribution
- Widely supported by members of Modbus Organization

Modbus Characteristics

Application layer messaging protocol

Efficient communications between interconnected assets

Can be used by extremely simple devices such as sensors or motors

- Communicate with a more complex computers that read measurements and perform analysis and control

Requires very little processing overhead

- Suitable for PLCs and RTUs to communicate supervisory data to a SCADA system

Modbus Characteristics

Request/response protocol

Three Protocol Data Units (PDUs):

- Modbus Request
- Modbus Response
- Modbus Exception Response

Each devices is assigned unique address

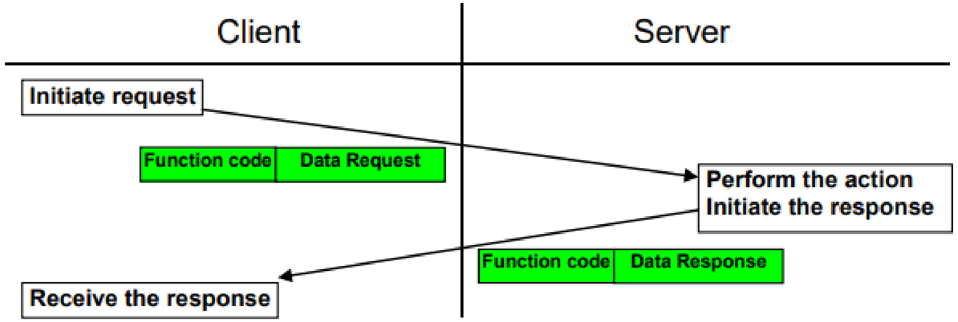
- All of them may hear the message, only the addressed device responds

Modbus Operation

Starts with initial Function Code and a Data Request within a Request PDU

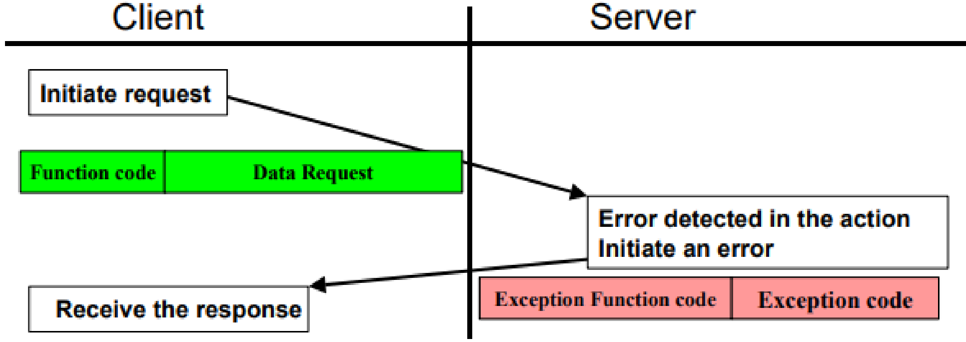
Response either:

- Function Code and Data Response, if no error
- Exception Function Code and Exception Code, if error



Examples of Function Codes and Data Requests:

- Read from an I/O interface
- Write a value to a register (i.e., change the value in register)



Modbus Variants

Modbus RTU: binary data representation,

Start	Address	Function	Data	CRC	End
1 Char	2 Chars	2 Chars	n Chars Contiguous stream	2 Chars	2 Chars CRLF

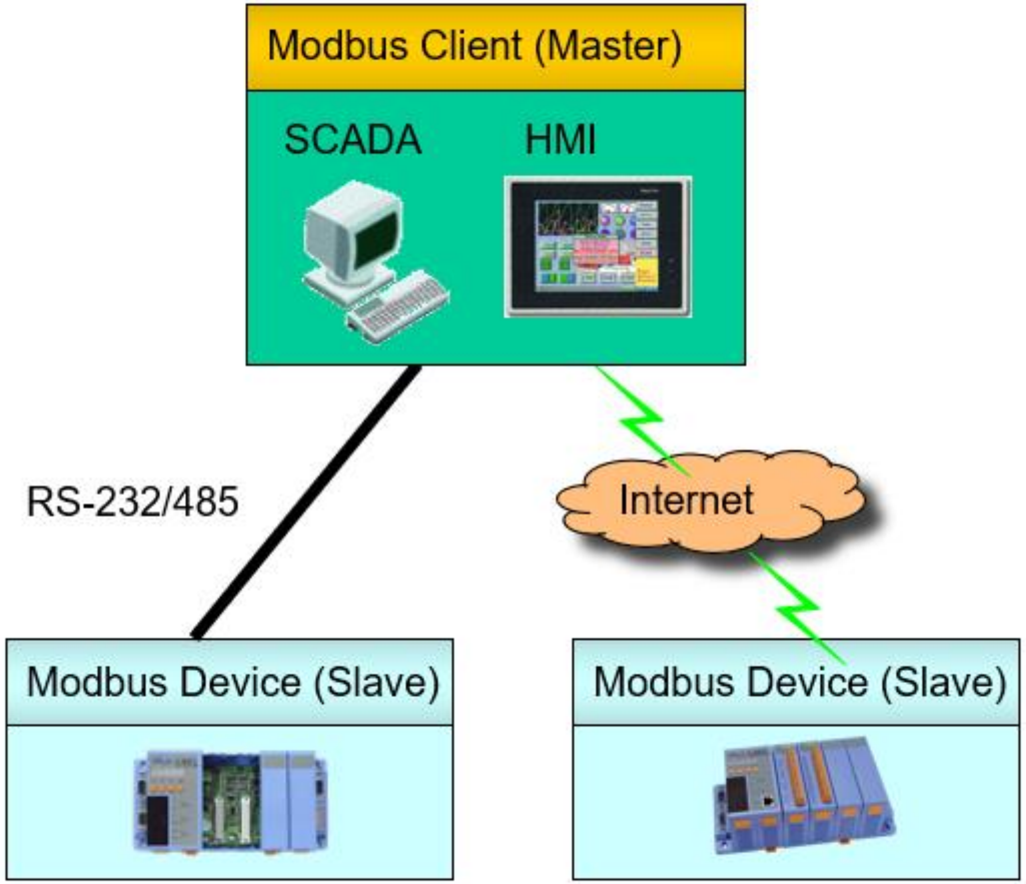
Modbus ASCII: ASCII characters to represent data

Start	Address	Function	Data	CRC	End
Silent (T1–T4)	8 Bits	8 Bits	n x 8 Bits contiguous stream	16 Bits	Silent (T1–T4)

Modbus TCP

Uses Transmission Control Protocol/Internet Protocol (TCP/IP) to transport Modbus commands and messages over Ethernet

- Uses TCP/IP layers
- Port 502
- Client/server model



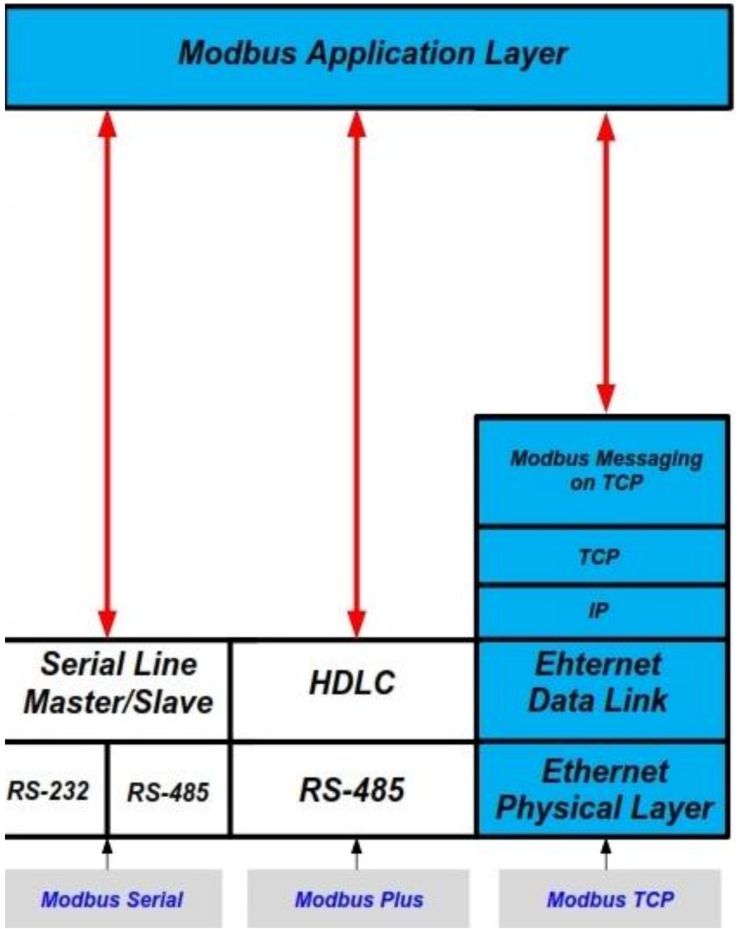
Modbus Protocol Stack

Modbus RTU/ASCII

Modbus TCP

Modbus Plus

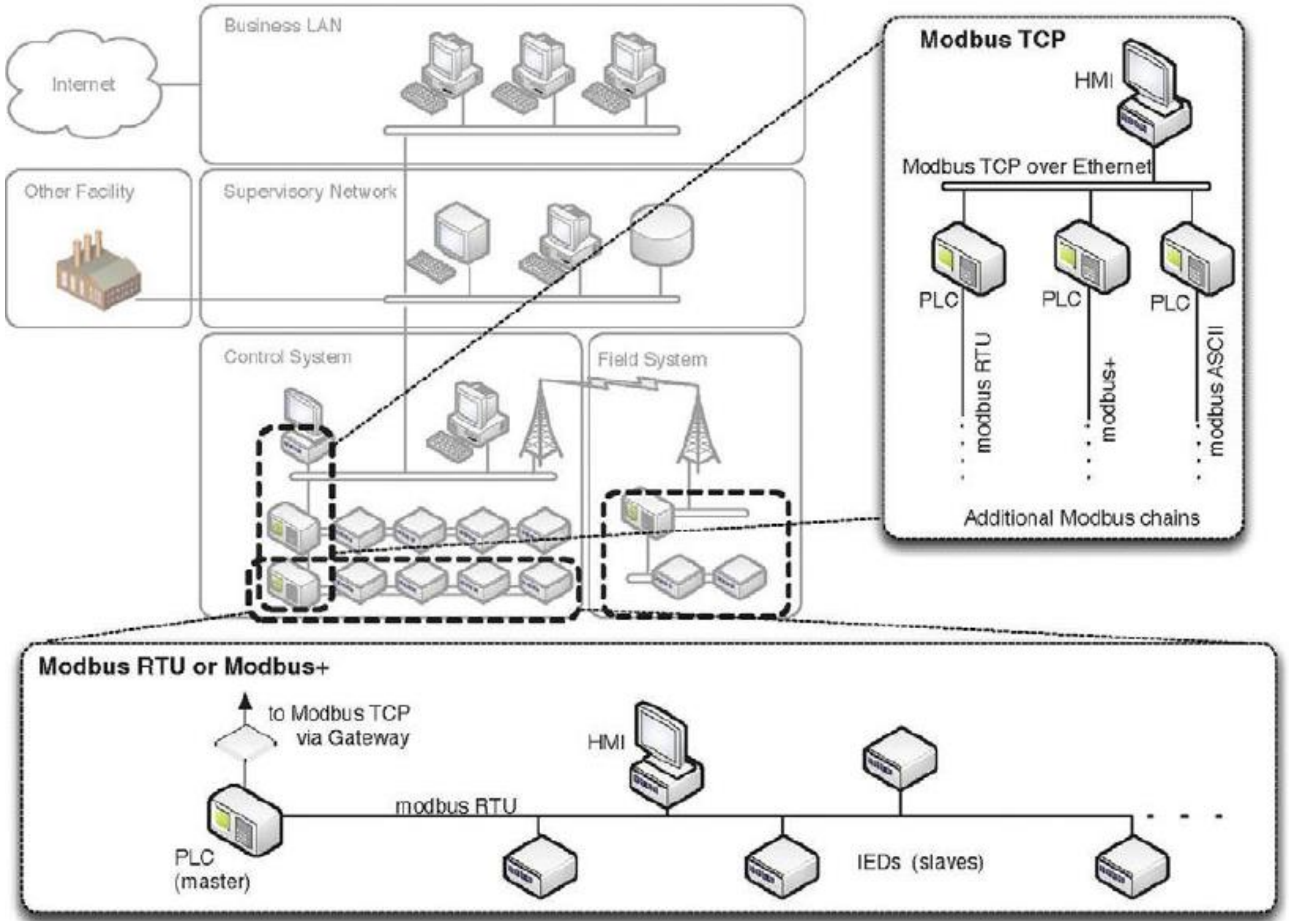
- Proprietary



Where Modbus is used

Typically deployed:

- Between PLCs and HMIs, or
- Between a Master PLC and slave devices such as PLCs, HMIs, IEDs



Security Concerns of Modbus

Lack of authentication:

- Modbus sessions only require the use of a valid Modbus address and valid function code

Lack of encryption (confidentiality):

- Data transmission in clear text

Lack of message checksum (integrity):

- No integrity checks built into the MODBUS
- Depends on lower layer protocols

Security Concerns of Modbus

Lack of broadcast suppression:

- All serially connected devices will receive all messages
- Simple DoS attack
  - Broadcast of unknown addresses

Programmability with command:

- Dangerous logic to PLC or RTU can be installed

Examples of Security Problem in Modbus

If there is a bus connecting multiple Modbus slaves to a master, it is possible to do denial of service by fake broadcasts

Injection of malicious logic to controllers (PLC)

How about sending invalid function codes?

- Reconnaissance activity can be performed on the SCADA network
  - Repeatedly send those packets with invalid function codes
  - What happens if the slave address is invalid?

Examples of Security Problem in Modbus

Maximum Protocol Data Unit (PDU)

- Modbus TCP limits this to 260 bytes
- If you create more than 260 bytes, what happens?
  - Buffer overflow

Solution: For each message use encryption and sign those messages

- How realistic?

Modbus Security Recommendations

ICS-aware IDS

- Instead of IPS
  - Due to false negatives

Whitelisting

Application aware firewall

Recent Modbus news/updates

Please check these:

PRESS RELEASE Modbus Security – New Protocol to Improve Control System Security

https://modbus.org/docs/Modbus-SecurityPR-10-2018.pdf

PRESS RELEASE Modbus Organization Replaces Master-Slave with Client-Server

https://modbus.org/docs/Client-ServerPR-07-2020-final.docx.pdf

Distributed Network Protocol (DNP3)

Began as a serial protocol designed for use between master control stations and slave devices, as well as for RTUs and IEDs within a control station

Was extended to work over IP

- Encapsulated in TCP or UDP packets
- In order to make remote RTU communications more easily accessible over modern networks

Very reliable, while remaining efficient and well suited for real-time data transfer

- CRC (Cyclic redundancy check) checks

DNP3 Characteristics

Primary motivation: reliable communication that include high level of electromagnetic interference

Based on International Electrotechnical Commission (IEC) 60870-5 standard

Several standardized data formats and supports time-stamped (and time-synchronized) data,

- Making real-time transmissions more efficient and thus even more reliable

Optional retransmission in case of no confirmation received

DNP3 Characteristics

The payload is very flexible and can be used to

- Simply transfer informational readings, or
- Send control functions, or
  - Direct binary or analog data for direct interaction with devices such as Remote Terminal Units (RTUs), as well as other analog devices such as IEDs

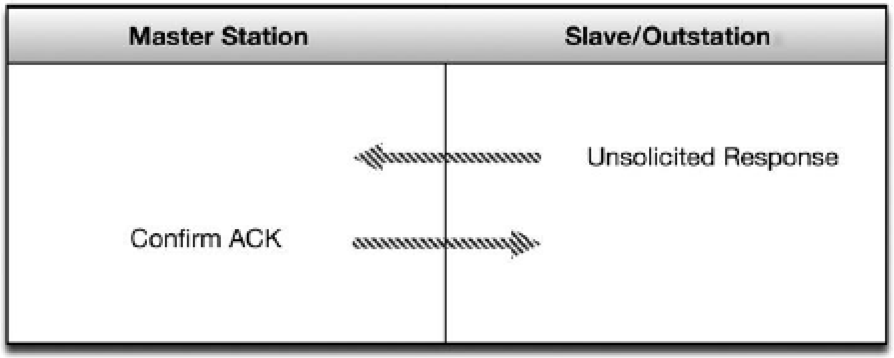
Supports two kinds of data

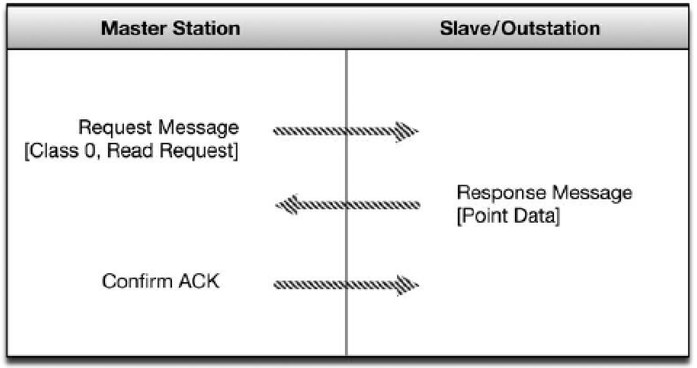
- Static or Class 0 such as point readings
- Event data such as alarm:
  - Priority class 1 (highest) - 3 (lowest) allows operate more efficiently

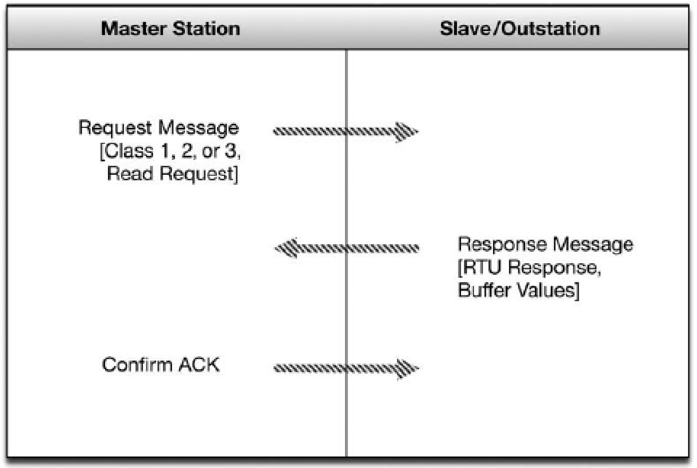
DNP3 Characteristics

Bidirectional (supporting communications from both Master to Slave and from Slave to Master) and supports exception-based reporting

- Possible for a DNP3 outstation to initiate an unsolicited response to notify the Master of an event outside of the normal polling interval
  - Such as an alarm condition







DNP3 Layers

Runs on application layer

- However, proposes its lower layer protocols as well
  - Transport and Link Layer

Link Layer Responsibility:

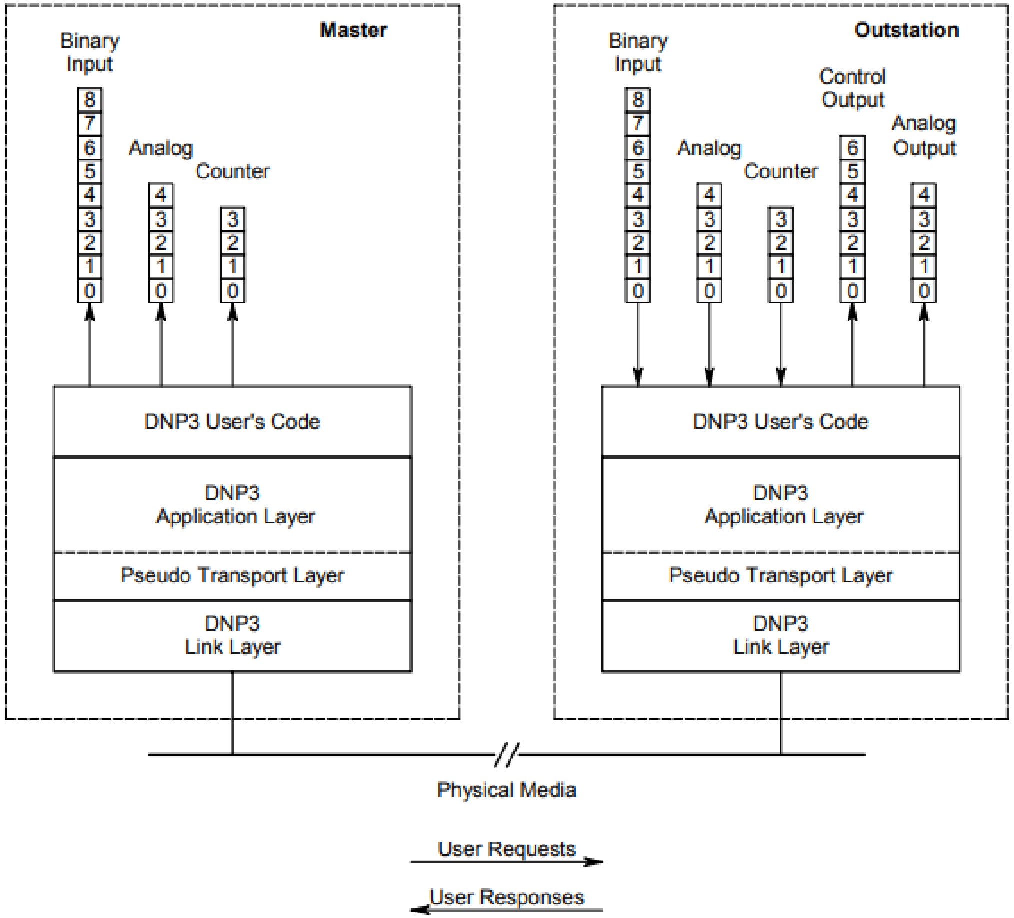
- Making the physical link reliable
  - Error detection

DNP3 Frame

Header	Data Section

Header

Sync	Length	Link Control	Destination Address	Source Address	CRC



DNP3 Benefits: Short Term

Interoperability between multi-vendor devices

Fewer protocols to support in the field

- Reduced software costs
- No protocol translators needed

Independent conformance (compliance) testing

Support by independent users group and third-party sources (e.g. test sets, source code)

- Less testing, maintenance and training
- Improved documentation

DNP3 Benefits: Long Term

Easy system expansion

- 65520 individual addresses

More value-added products from vendors

Major operations savings

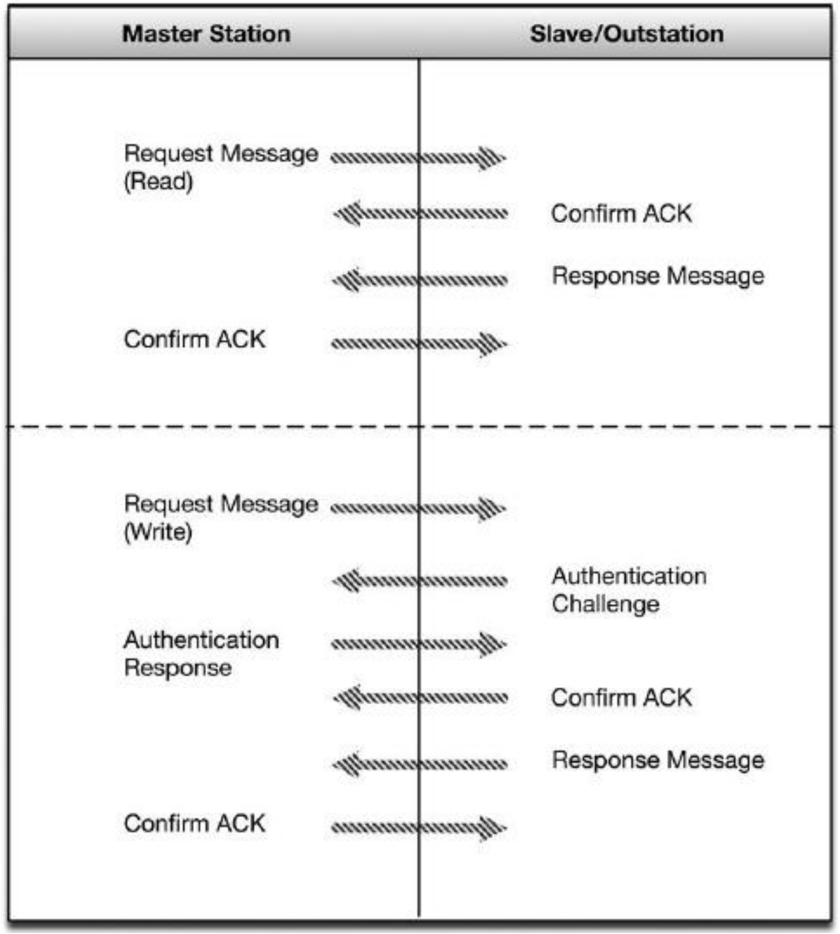
Secure DNP3

Adds authentication to the response/request process

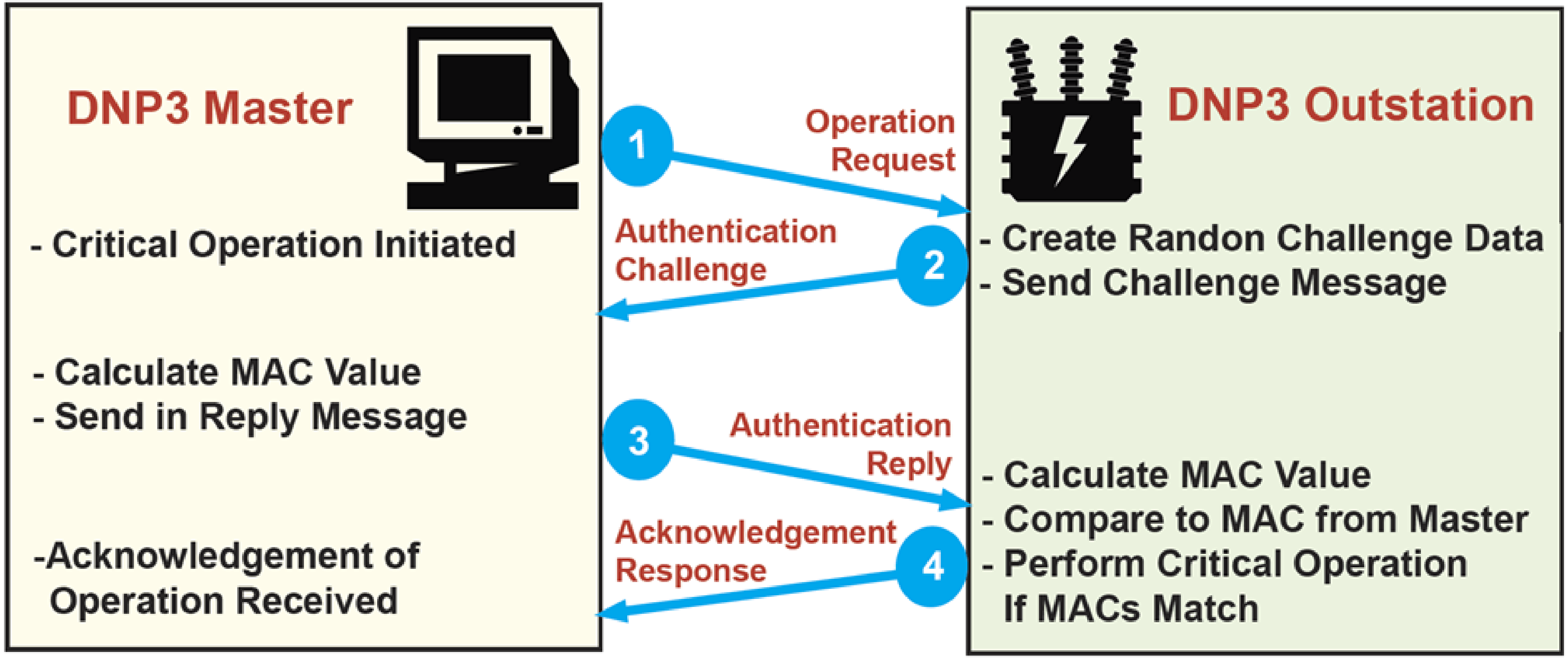
- Challenge by the receiving device
  - Upon session initiation after a preset period of time
  - Or upon a critical request
- Unique session key hashed with message data

Verifies authority, integrity, and pairing

- Difficult to perform data manipulation, code injection, or spoof



Secure DNP3 Standard

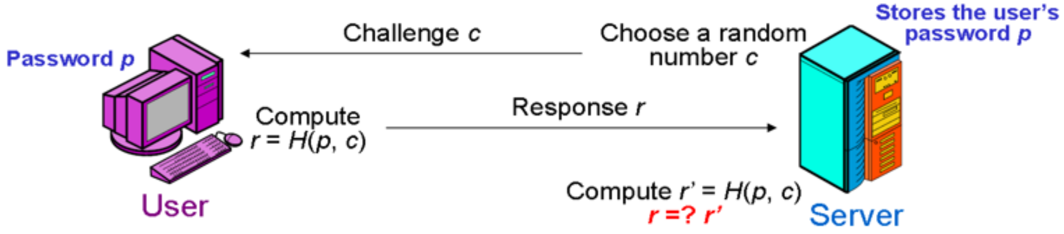


What is MAC?

Message authentication codes (MAC) provides authentication as MAC = Hash(p || c)

The sender has the same secret key p with the receiver for message authentication

- The sender computes the MAC of a message c as follows: MAC p(c) = H(p || c)
  - The message-MAC pair is then transmitted to the receiver
- The receiver authenticates r by recalculating the r′ and comparing it with the received
  - If the two MACs match, the receiver is assured that the message comes from the legitimate sender (authentication) and has not been altered during transmission (integrity)



Where DNP3 is used

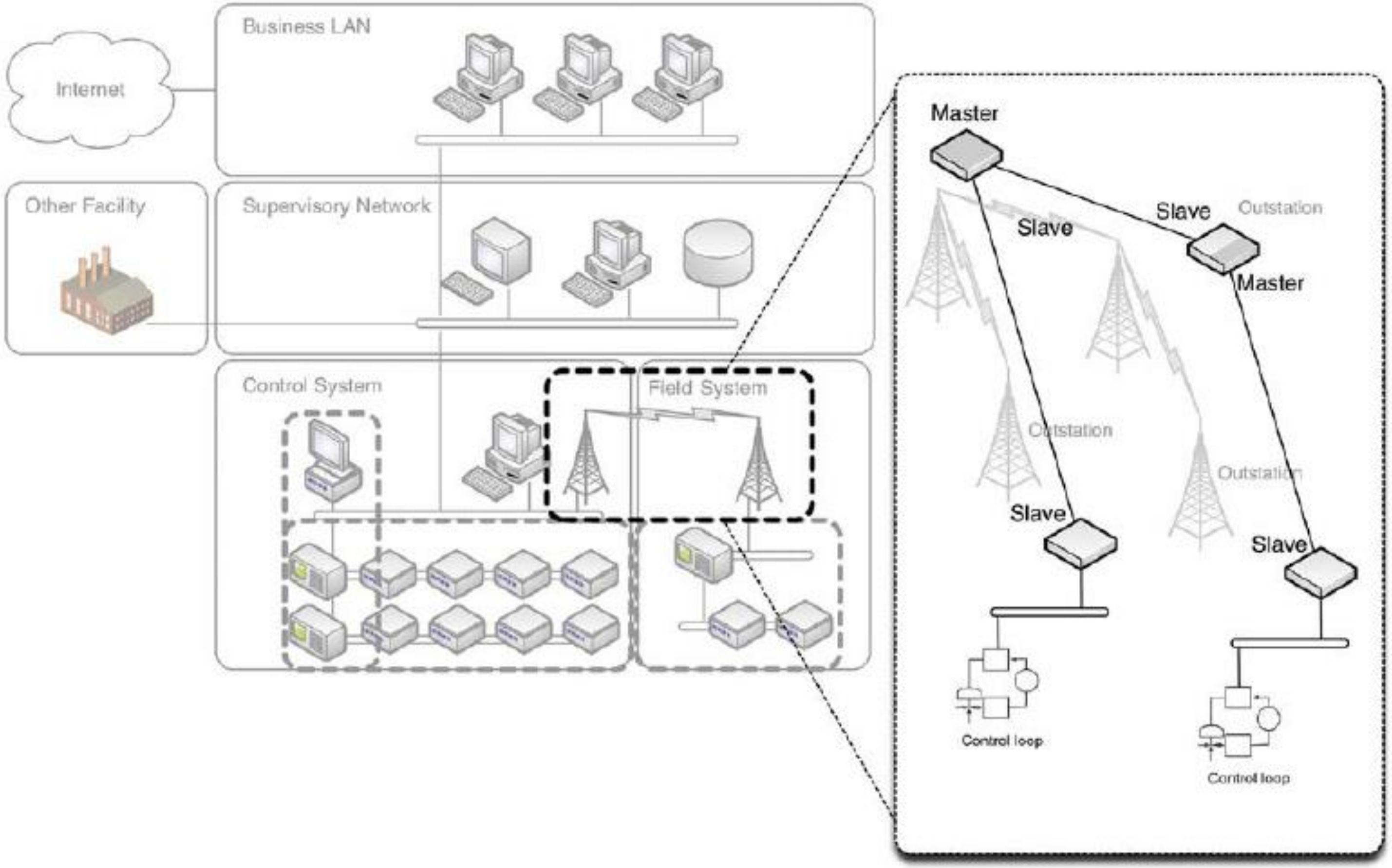
Between a master control station and an RTU in a remote station

- Over almost any medium including wireless, radio, and dial-up

Between RTUs and IEDs

- Competes with Modbus

Well suited for hierarchical and aggregated point-to-multipoint topologies



DNP3 Security Concerns

No authentication and encryption

Man in the Middle (MitM) attacks are possible

- Capturing addresses

Some examples of attacks:

- Spoofing unsolicited responses to the Master to falsify events
- Performing a DoS attack through the injection of broadcasts
- Manipulating time synchronization data for communication loss
- Issuing unauthorized stops, restart or other functions

Secure DNP3's Security Concerns

Command in cleartext

- What is the concern here, considering CIA?

Any other concerns?

- Good topic to investigate

DNP3 News

Please check:

https://www.dnp.org/Resources/Public-Documents

Overview of DNP3 Security Version 6 2020-01-21