Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots

Elisavet Grigoriou, Athanasios Liatifis, Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis, Thomas Lagkas, Evangelos Markakis, Ioannis Moscholios

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Authors

Elisavet Grigoriou
Sidroco Holdings Limited
Nicosia, Cyprus
egrigoriou@sidroco.com

Athanasios Liatifis, Panagiotis Radoglou Grammatikis, Panagiotis Sarigiannidis
Department of Electrical and Computer Engineering
University of Western Macedonia, Kozani, Greece
{aliatifis, pradoglou, psarigiannidis}@uowm.gr

Thomas Lagkas
Department of Computer Science, International Hellenic University, Thessaloniki, Greece
tlagkas@cs.ihu.gr

Evangelos Markakis
Hellenic Mediterranean University, Greece
emarkakis@hmu.gr

Ioannis Moscholios
University of Peloponnese, Tripoli, Greece
idm@uop.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

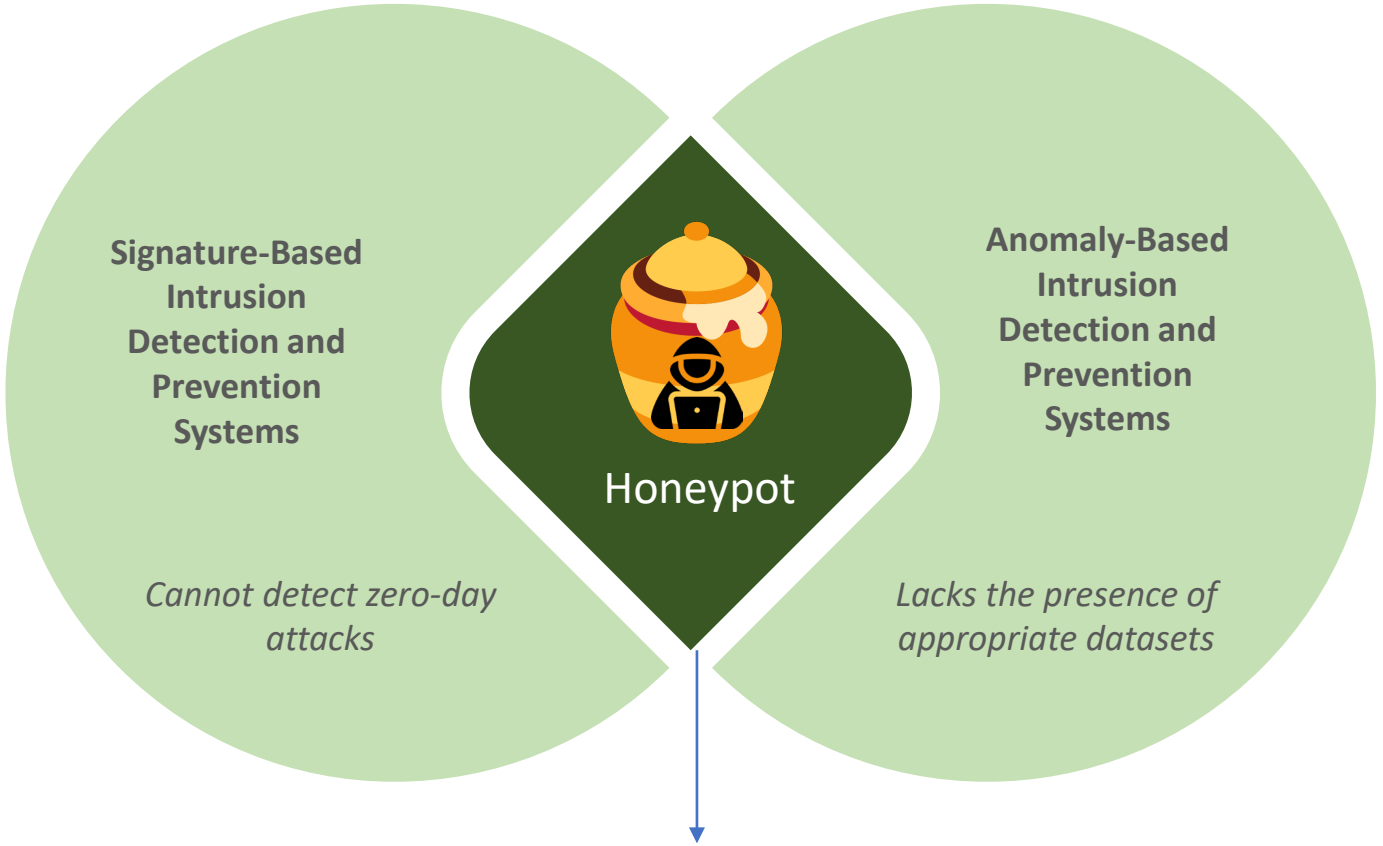
Outline

- Motivation
- Background
- Proposed IEC 60870-5-104 Honeypot
- Experimental results
- Conclusion

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

MOTIVATION

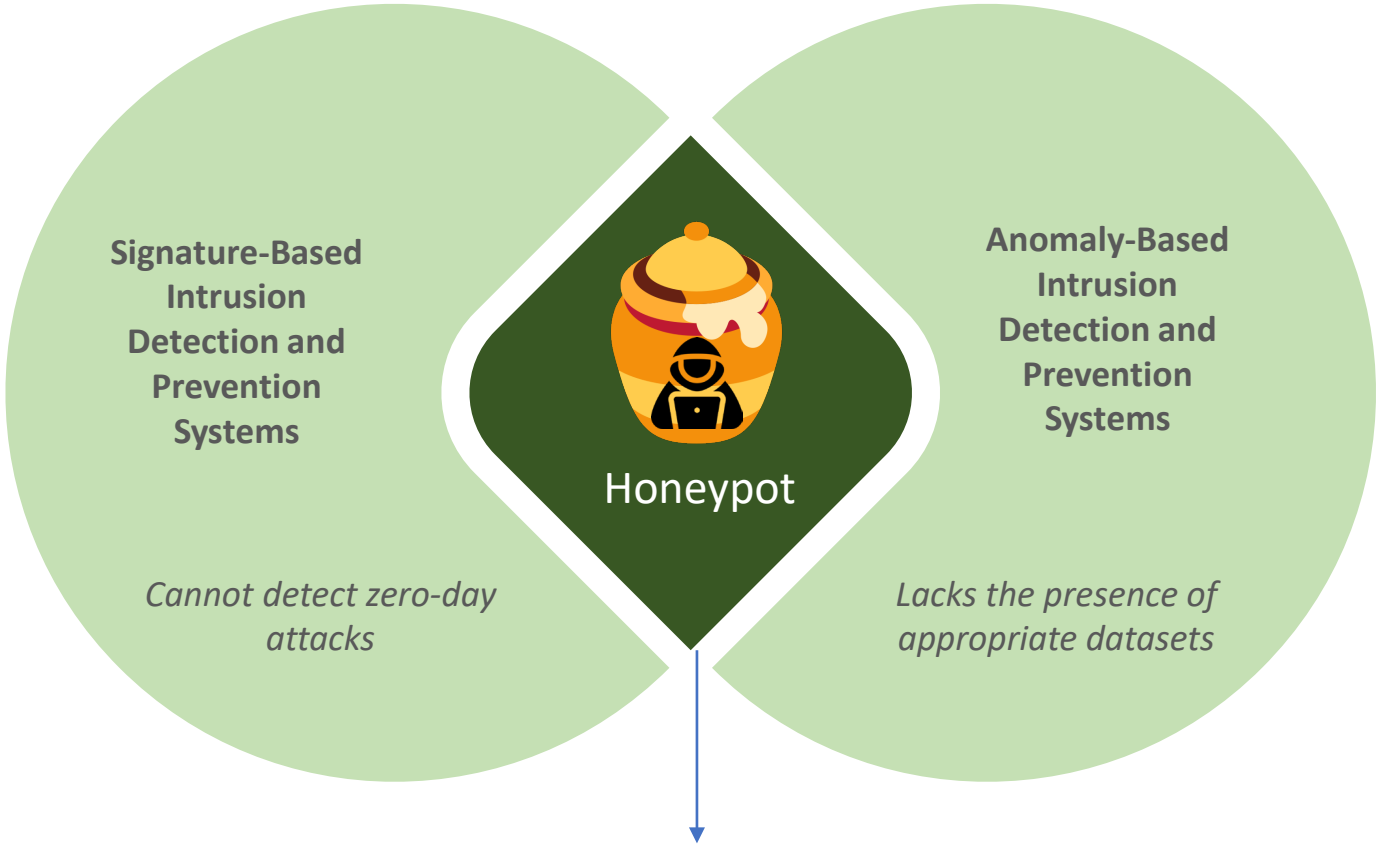
Motivation



Honeypots are used to hide and protect critical assets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Motivation



IEC104 lacks critical security features, such as encryption, integrity protection and authentication.

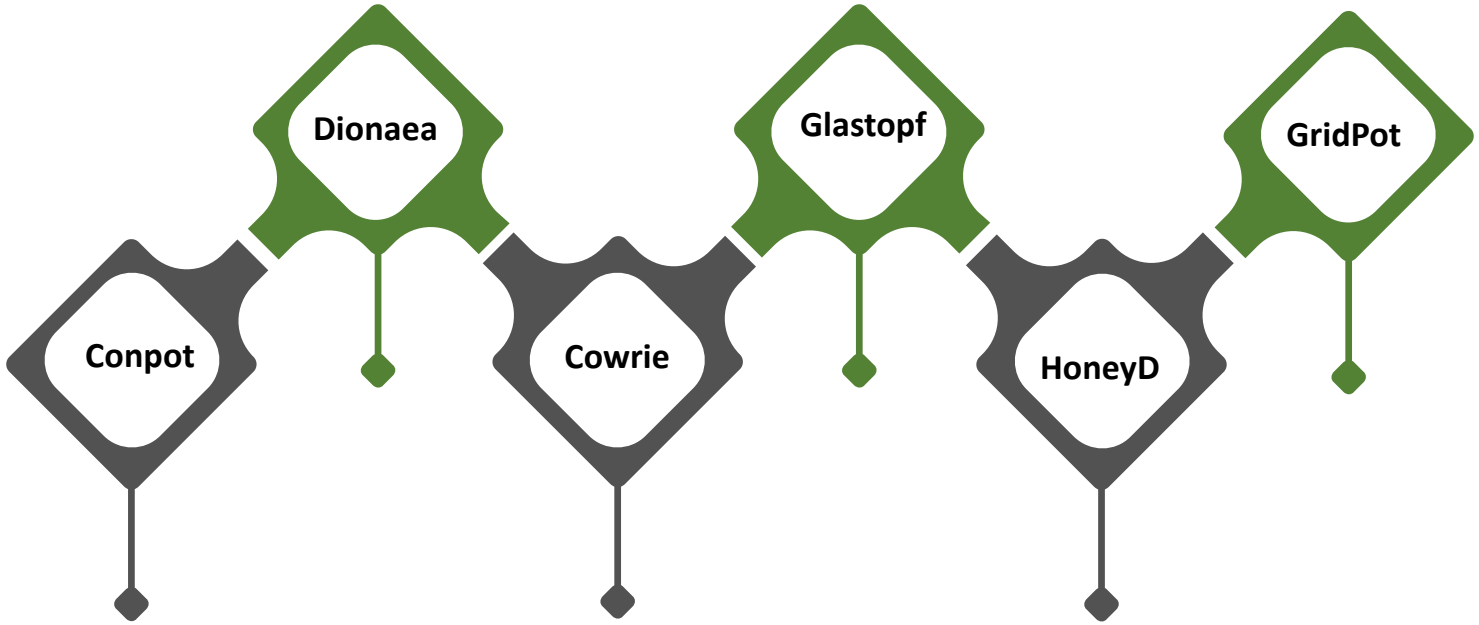
This work presents the IEC104 honeypot, which is capable of hiding the actual IEC104 assets and detecting potential intrusions and anomalies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

BACKGROUND

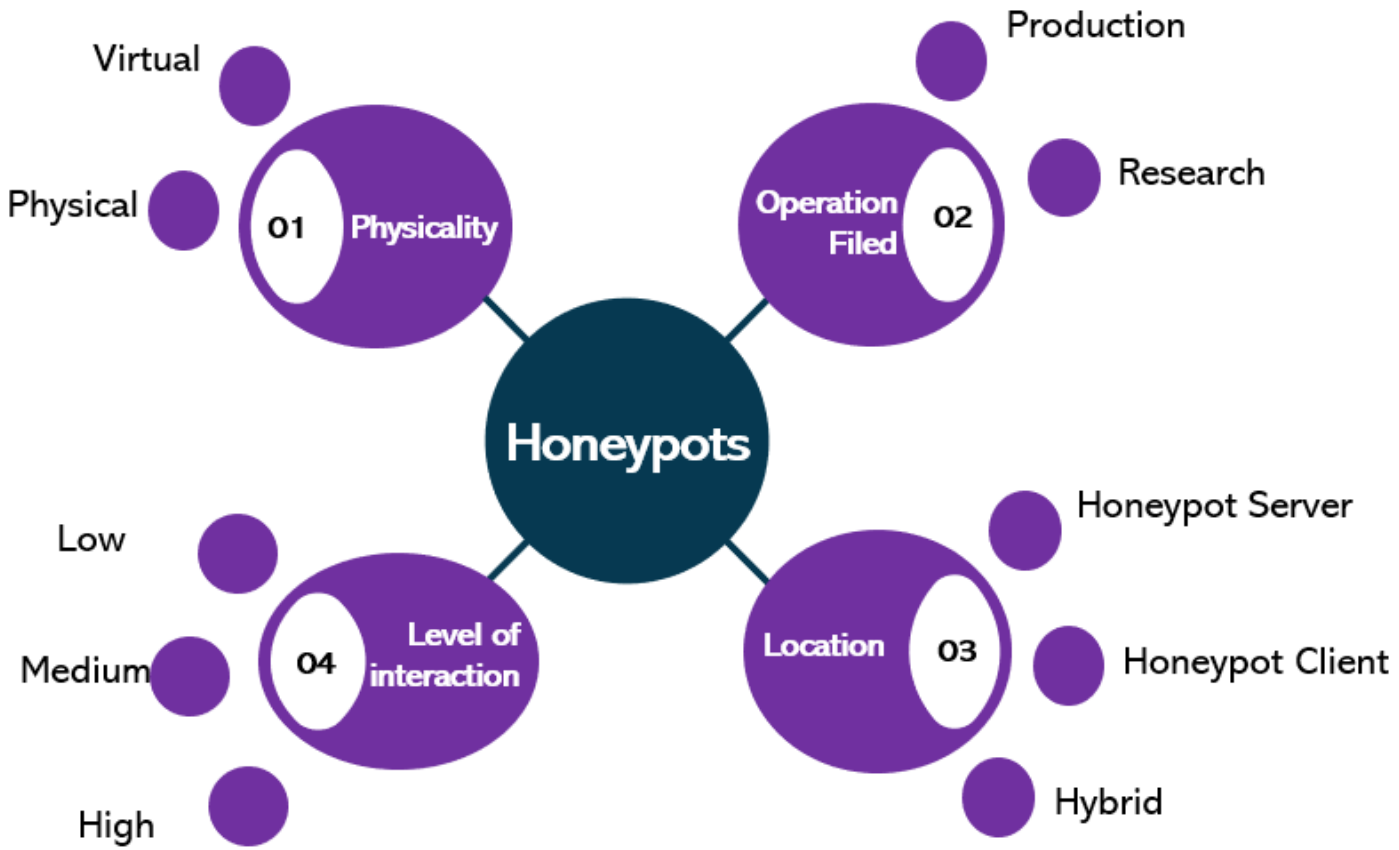
Honeypots

- Used to obtain information about an attacker.
- The honeypot enables the security team to comprehend the techniques of attackers, learn more about known and new assaults, and so safeguard the actual production systems more effectively.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Honeypots Classification



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

IEC 60870-5-104 Protocol

- IEC104 is an expansion of the IEC 60870-5 network protocol standard that allows for TCP/IP connection.
- The protocol is a remote control and communication standard designed specifically for electric power installations and power grids.
- TCP port 2404 is used by the protocol.

The IEC 101/104 interaction between the controlled station and the controlling station can be

01 **RTU Master**
Controlling Station

02 **RTU Slave**
Controlled Station

IEC 101/104 provides three direction modes

1 **Monitor Direction**

2 **Control Direction**

3 **Reversed Direction**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

IEC 60870-5-104 Protocol

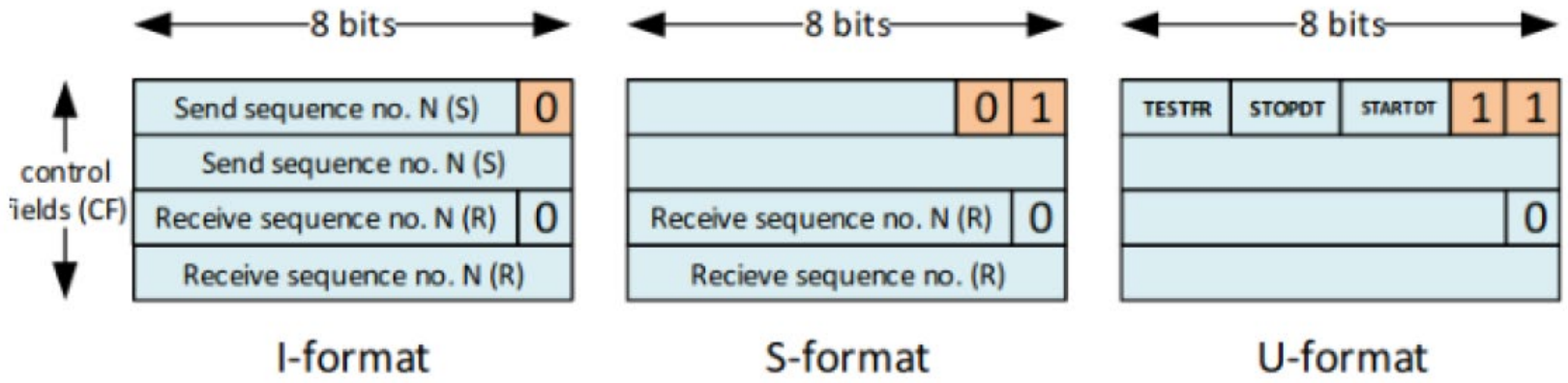
IEC104 is implemented in the TCP/IP stack's application layer via the **Application Protocol Data Unit (APDU)** and **Application Service Data Unit (ASDU).**

Three APDU formats are established based on the APDU Control :

- The an **i-frame** to send data. It is divided into two sections: a fixed-length ASDU header and a variable length.

list of information objects.

- The **s-frame** is used for supervisory tasks.
- The **u-frame** for transmitting uncounted control functions (test frame, start transfer, stop transfer)



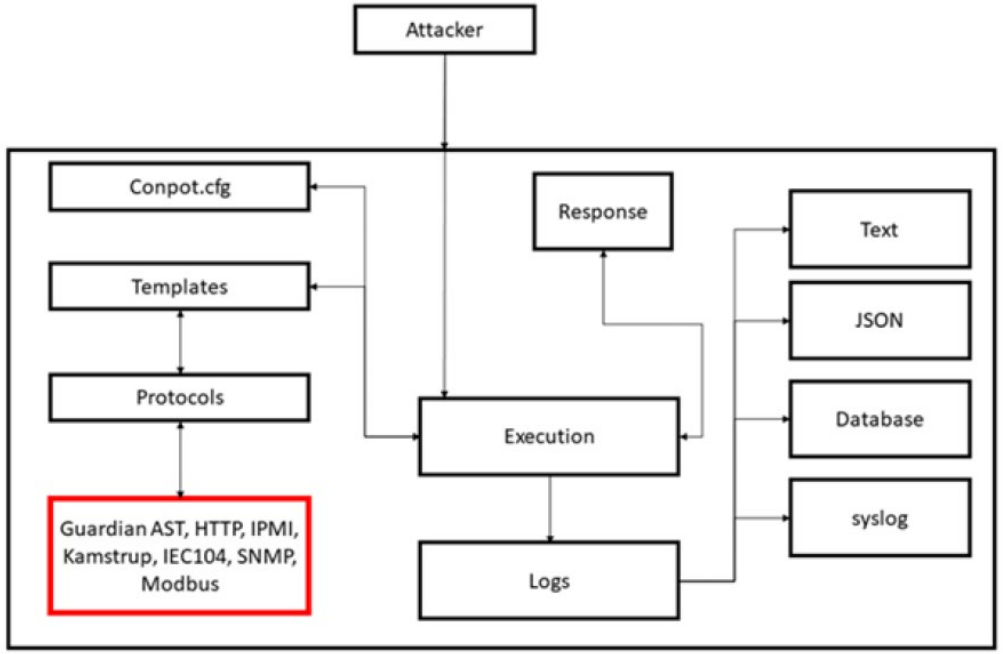
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

PROPOSED IEC 60870-5-104 HONEYPOT

Proposed IEC 60870-5-104 Honeypot

IEC104 Honeypot existing and newly added commands

Existing commands	Newly added commands
M_SP_NA_1, M_SP_TA_1,	C_CI_NA_1
M_DP_NA_1, M_DP_TA_1	C_RD_NA_1
M_DP_NA_1, M_DP_TA_1	C_CS_NA_1
M_ME_NB_1, M_ME_TB_1	C_TS_NB_1
M_ME_NC_1, M_ME_TC_1	C_RP_NC_1
M_SP_TB_1, M_DP_TB_1	C_CD_NA_1
M_ME_TE_1, M_ME_TF_1	
C_SC_NA_1, C_DC_NA_1	
C_SE_NB_1, C_SE_NC_1	
C_IC_NA_1	



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

EXPERIMENTAL RESULTS

Experimental Results – Test Scenario 1

Description: To execute information transfer, the Master sends a Counter Interrogation (CI) command to RTU (i.e. IEC104 honeypot) in an I-format. The RTU is compatible with Counter Interrogation Mode A ”Counter freeze without reset”. In this case the totals are frozen at common time using the CI command.

Procedure steps:

(1) An IEC104 client (Slave) seeks to establish a connection with the Master.
(2) Determine whether the Master delivers a ”Activation”.
(3) Determines if the RTU gets the Master’s CI command.
(4) A check is realized to observe if the RTU responds with ”Activation Confirmation” and if the IOA’s Sequence number (SQ) is increased.
(5) Determine if the RTU delivers the ”Activation termination” command in response to the CI command.
(6) A check to observe if the IEC104 honeypot recorded this occurrence in the ”iec104 logs.log” file.

The “Counter Interrogation command” is sent.

```
IEC 60870-5-104-Asdu: ASDU=1 C_CI_NA_1 ActCon  IOA=0 'counter interrogation command'
    TypeId: C_CI_NA_1 (101)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 0101 = CauseTx: ActCon (5)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 1
    IOA: 0
```

It was received by the RTU

```
2020-07-22 20:19:22,305 Received: 65 01 0a 00 01 00 00 00 00 14 'CounterInterrogationCommand'
```

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021936

Experimental Results – Test Scenario 2

Description: To transfer information, the Master sends a Read Command (C RD NA 1) to the RTU in I-format. In order to obtain each value of a register, the ”Read command” is invoked with an IOA address. It responds with the corresponding IEC104 register/bit value.

Procedure steps:

(1) An IEC104 client (Slave) seeks to establish a connection with the Master.
(2) It determines, if the Master delivers a ”Activation”.
(3) Determine if or not the RTU receives the ”RD command” from the Master.
(4) If more than one value is requested, the meter answers with an ASDU sequence with the SQ bit set to ”1”.
(5) If a single value is requested, the meter replies to a read request with an ASDU sequence with the SQ bit in the variable structure.
(6) A check if the RTU sends the ”Activation Termination”
(7) A check to observe if the IEC104 honeypot recorded this occurrence in the ”iec104 logs.log” file.

The RTU receives the command to Read.

```
2020-07-22 20:52:12,525 Received: 66 01 0a 00 01 00 00 00 00 14 'Read from Register'
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

CONCLUSION

Conclusion

- This work describes the IEC104 honeypot that mimics an industrial protocol.
- Encourage the industry to strengthen its efforts to secure ICSs and to continue monitoring new risks as they emerge.

- Future work:
  - ✓ Produce replies artificially that are indistinguishable leveraging Artificial Intelligence, dynamically adjust the behaviour profile of the honeypot to match a certain environment state
  - ✓ Design an open repository where stakeholders can upload industrial device profiles and behaviour models.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936

Thank you!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021936