

The actual Ingeteam-project (asdu 157)

- false data-types
- unexpected Inrogen-telegrams after general-request

Wireshark capture showing a list of packets and a detailed view of an IEC 60870-5-104-Asdu telegram. The packet details pane shows the following structure:

```

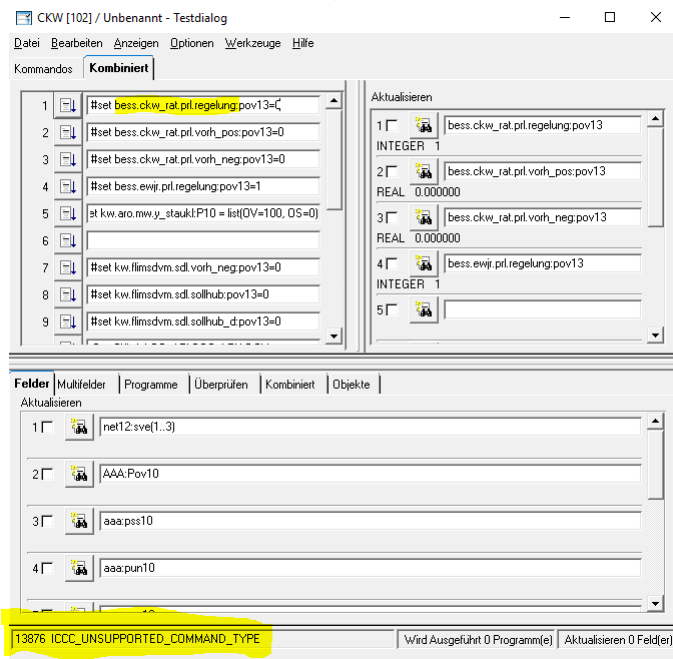
IEC 60870-5-104-Asdu: ASDU=157 M_SP_NA_1 Inrogen IOA=656129 'single-point information'
  TypeId: M_SP_NA_1 (1)
  1... .. = SQ: True
  .000 0001 = NumIx: 1
  ..01 0100 = CauseTx: Inrogen (20)
  .0... .. = Negative: False
  0... .. = Test: False
  OA: 0
  Addr: 157
  IOA: 656129
  SIQ: 0x01
    .... ..1 = SPI: On
    ..0 .... = BL: Not blocked
    ..0. .... = SB: Not Substituted
    .0. .... = NT: Topical
    0... .. = IV: Valid
  
```

Wireshark capture showing a list of packets and a detailed view of an IEC 60870-5-104-Asdu telegram. The packet details pane shows the following structure:

```

IEC 60870-5-104-Asdu: ASDU=157 M_ME_NC_1 Inrogen IOA[2]=656651-656652 'measured value, short floating point number'
  TypeId: M_ME_NC_1 (13)
  1... .. = SQ: True
  .000 0010 = NumIx: 2
  ..01 0100 = CauseTx: Inrogen (20)
  .0. .... = Negative: False
  0... .. = Test: False
  OA: 0
  Addr: 157
  IOA: 656651
    Value: 0
  QDS: 0x00
  IOA: 656652
    [IOA: 656652]
    Value: 0
  QDS: 0x00
  
```

- it isn't possible to send any commands:



Example of a plant that is in charge (asdu 334):

Wireshark capture window titled "104asdu.addr==334 and (104asdu.ioa==656129 or 104asdu.ioa==656651)".

No.	Time	Source	Destination	Protocol	Length	Info
969078	2022-03-11 11:49:50.541584	172.18.1.4	172.18.0.4	104asdu	70	-> I (32205,21449) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
972283	2022-03-11 11:50:10.559665	172.18.1.4	172.18.0.4	104asdu	74	-> I (32287,21461) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
985030	2022-03-11 11:51:30.720219	172.18.1.4	172.18.0.4	104asdu	70	-> I (32589,21496) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
988166	2022-03-11 11:51:50.759494	172.18.1.4	172.18.0.4	104asdu	74	-> I (32651,21501) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
999336	2022-03-11 11:53:00.907936	172.18.1.4	172.18.0.4	104asdu	70	-> I (130,21524) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
1002486	2022-03-11 11:53:20.930016	172.18.1.4	172.18.0.4	104asdu	74	-> I (201,21529) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
1015253	2022-03-11 11:54:41.051638	172.18.1.4	172.18.0.4	104asdu	70	-> I (508,21573) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
1018244	2022-03-11 11:55:00.095292	172.18.0.4	172.18.1.4	104asdu	70	<- I (21581,576) ASDU=334 C_SC_NA_1 Act IOA=656129
1018245	2022-03-11 11:55:00.095720	172.18.1.4	172.18.0.4	104asdu	70	-> I (576,21582) ASDU=334 C_SC_NA_1 ActCon IOA=656129

Packet 1018244 details:

```

> Frame 1018244: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Vmware_le:0f:4a (00:0c:29:1e:0f:4a), Dst: Cisco_9f:1f:27 (50:2f:a8:9f:1f:27)
> Internet Protocol Version 4, Src: 172.18.0.4, Dst: 172.18.1.4
> Transmission Control Protocol, Src Port: 53563, Dst Port: 2404, Seq: 81757, Ack: 736414, Len: 16
> IEC 60878-5-104-Asdu: <- I (21581,576)
  IEC 60878-5-104-Asdu: ASDU=334 C_SC_NA_1 Act IOA=656129 'single command'
    TypeId: C_SC_NA_1 (45)
    0... .. = S0: False
    .000 0001 = NumIx: 1
    ..00 0110 = CauseTx: Act (6)
    .0... .. = Negative: False
    0... .. = Test: False
    OA: 0
    Addr: 334
    IOA: 656129
    > S0: 0x01
  
```

Wireshark capture window titled "104asdu.addr==334 and (104asdu.ioa==656129 or 104asdu.ioa==656651)".

No.	Time	Source	Destination	Protocol	Length	Info
1063121	2022-03-11 11:59:41.561528	172.18.1.4	172.18.0.4	104asdu	70	-> I (1601,21678) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
1066367	2022-03-11 12:00:01.571966	172.18.1.4	172.18.0.4	104asdu	74	-> I (1661,21683) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
1070901	2022-03-11 12:00:30.089691	172.18.0.4	172.18.1.4	104asdu	74	<- I (21693,1769) ASDU=334 C_SE_NC_1 Act IOA=656651
1070917	2022-03-11 12:00:30.142712	172.18.1.4	172.18.0.4	104asdu	158	-> I (1770,21694) ASDU=334 C_SE_NC_1 ActCon IOA=656651 -> I (1771,21694) ASDU=335 C_SE_NC_1 ActTerm IOA=656652 -
1070927	2022-03-11 12:00:30.173815	172.18.1.4	172.18.0.4	104asdu	74	-> I (1775,21694) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
1077562	2022-03-11 12:01:11.896885	172.18.1.4	172.18.0.4	104asdu	70	-> I (1921,21710) ASDU=334 C_SC_NA_1 ActTerm IOA=656129
1085525	2022-03-11 12:02:01.976024	172.18.1.4	172.18.0.4	104asdu	74	-> I (2101,21727) ASDU=334 C_SE_NC_1 ActTerm IOA=656651
1093491	2022-03-11 12:02:52.111790	172.18.1.4	172.18.0.4	104asdu	164	-> I (2287,21748) ASDU=339 M_ME_TF_1 Spont IOA[2]=3933697,... -> I (2288,21748) ASDU=334 C_SC_NA_1 ActTerm IOA=65
1101549	2022-03-11 12:03:42.134895	172.18.1.4	172.18.0.4	104asdu	74	-> I (2548,21801) ASDU=334 C_SE_NC_1 ActTerm IOA=656651

Packet 1070901 details:

```

> Frame 1070901: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Vmware_le:0f:4a (00:0c:29:1e:0f:4a), Dst: Cisco_9f:1f:27 (50:2f:a8:9f:1f:27)
> Internet Protocol Version 4, Src: 172.18.0.4, Dst: 172.18.1.4
> Transmission Control Protocol, Src Port: 53563, Dst Port: 2404, Seq: 84729, Ack: 772068, Len: 20
> IEC 60878-5-104-Asdu: <- I (21693,1769)
  IEC 60878-5-104-Asdu: ASDU=334 C_SE_NC_1 Act IOA=656651 'set point command, short floating point number'
    TypeId: C_SE_NC_1 (50)
    0... .. = S0: False
    .000 0001 = NumIx: 1
    ..00 0110 = CauseTx: Act (6)
    .0... .. = Negative: False
    0... .. = Test: False
    OA: 0
    Addr: 334
    IOA: 656651
    Value: 1
    > Q0S: 0x00
  
```