# IEC104 Inspector



# IEC104 Inspector Overview

| | |
|---|---|
| Type | Inspector (service) |
| Usage | Inspect |
| Instance Type | Multiton |
| Other Inspectors Required | `stream_tcp` |
| Enabled | `false` |

The IEC 60870-5-104 (IEC104) protocol describes a communication standard to exchange telecontrol messages between electric power systems. The IEC104 protocol uses TCP port 2404.

The `iec104` inspector detects IEC104 messages in network traffic. The `iec104` inspector analyzes and normalizes IEC104 messages by either combining a message spread across multiple frames, or splitting apart multiple messages within one frame.

When enabled, the intrusion rule options provide access to the IEC104 application protocol control information (APCI) type and the application service data unit (ASDU) function code.

# IEC104 Inspector Parameters

### IEC104 TCP port configuration

The `binder` inspector defines the IEC104 TCP port configuration. For more information, see the Binder Inspector Overview.

**Example:**

```
[
    {
        "when": {
            "role": "server",
            "proto": "tcp",
            "ports": "2404"
         },
        "use": {
            "type": "iec104"
        }
    }
]
```

**Note** The `iec104` inspector does not provide any parameters.

# IEC104 Inspector Rules

Enable the `iec104` inspector rules to generate events and, in an inline deployment, drop offending packets.

***Table 1: IEC104 Inspector Rules***

| GID:SID | Rule Message |
|---|---|
| 151:1 | Length in IEC104 APCI header does not match the length needed for the given IEC104 ASDU type id |
| 151:2 | IEC104 Start byte does not match 0x68 |
| 151:3 | Reserved IEC104 ASDU type id in use |
| 151:4 | IEC104 APCI U Reserved field contains a non-default value |
| 151:5 | IEC104 APCI U message type was set to an invalid value |
| 151:6 | IEC104 APCI S Reserved field contains a non-default value |
| 151:7 | IEC104 APCI I number of elements set to zero |
| 151:8 | IEC104 APCI I SQ bit set on an ASDU that does not support the feature |
| 151:9 | IEC104 APCI I number of elements set to greater than one on an ASDU that does not support the feature |
| 151:10 | IEC104 APCI I Cause of Initialization set to a reserved value |
| 151:11 | IEC104 APCI I Qualifier of Interrogation Command set to a reserved value |
| 151:12 | IEC104 APCI I Qualifier of Counter Interrogation Command request parameter set to a reserved value |
| 151:13 | IEC104 APCI I Qualifier of Parameter of Measured Values kind of parameter set to a reserved value |

| GID:SID | Rule Message |
|---|---|
| 151:14 | IEC104 APCI I Qualifier of Parameter of Measured Values local parameter change set to a technically valid but unused value |
| 151:15 | IEC104 APCI I Qualifier of Parameter of Measured Values parameter option set to a technically valid but unused value |
| 151:16 | IEC104 APCI I Qualifier of Parameter Activation set to a reserved value |
| 151:17 | IEC104 APCI I Qualifier of Command set to a reserved value |
| 151:18 | IEC104 APCI I Qualifier of Reset Process set to a reserved value |
| 151:19 | IEC104 APCI I File Ready Qualifier set to a reserved value |
| 151:20 | IEC104 APCI I Section Ready Qualifier set to a reserved value |
| 151:21 | IEC104 APCI I Select and Call Qualifier set to a reserved value |
| 151:22 | IEC104 APCI I Last Section or Segment Qualifier set to a reserved value |
| 151:23 | IEC104 APCI I Acknowledge File or Section Qualifier set to a reserved value |
| 151:24 | IEC104 APCI I Structure Qualifier set on a message where it should have no effect |
| 151:25 | IEC104 APCI I Single Point Information Reserved field contains a non-default value |
| 151:26 | IEC104 APCI I Double Point Information Reserved field contains a non-default value |
| 151:27 | IEC104 APCI I Cause of Transmission set to a reserved value |
| 151:28 | IEC104 APCI I Cause of Transmission set to a value not allowed for the ASDU |
| 151:29 | IEC104 APCI I invalid two octet common address value detected |
| 151:30 | IEC104 APCI I Quality Descriptor Structure Reserved field contains a non-default value |
| 151:31 | IEC104 APCI I Quality Descriptor for Events of Protection Equipment Structure Reserved field contains a non-default value |
| 151:32 | IEC104 APCI I IEEE STD 754 value results in NaN |
| 151:33 | IEC104 APCI I IEEE STD 754 value results in infinity |
| 151:34 | IEC104 APCI I Single Event of Protection Equipment Structure Reserved field contains a non-default value |
| 151:35 | IEC104 APCI I Start Event of Protection Equipment Structure Reserved field contains a non-default value |
| 151:36 | IEC104 APCI I Output Circuit Information Structure Reserved field contains a non-default value |
| 151:37 | IEC104 APCI I Abnormal Fixed Test Bit Pattern detected |

| GID:SID | Rule Message |
|---|---|
| 151:38 | IEC104 APCI I Single Command Structure Reserved field contains a non-default value |
| 151:39 | IEC104 APCI I Double Command Structure contains an invalid value |
| 151:40 | IEC104 APCI I Regulating Step Command Structure Reserved field contains a non-default value |
| 151:41 | IEC104 APCI I Time2a Millisecond set outside of the allowable range |
| 151:42 | IEC104 APCI I Time2a Minute set outside of the allowable range |
| 151:43 | IEC104 APCI I Time2a Minute Reserved field contains a non-default value |
| 151:44 | IEC104 APCI I Time2a Hours set outside of the allowable range |
| 151:45 | IEC104 APCI I Time2a Hours Reserved field contains a non-default value |
| 151:46 | IEC104 APCI I Time2a Day of Month set outside of the allowable range |
| 151:47 | IEC104 APCI I Time2a Month set outside of the allowable range |
| 151:48 | IEC104 APCI I Time2a Month Reserved field contains a non-default value |
| 151:49 | IEC104 APCI I Time2a Year set outside of the allowable range |
| 151:50 | IEC104 APCI I Time2a Year Reserved field contains a non-default value |
| 151:51 | IEC104 APCI I a null Length of Segment value has been detected |
| 151:52 | IEC104 APCI I an invalid Length of Segment value has been detected |
| 151:53 | IEC104 APCI I Status of File set to a reserved value |
| 151:54 | IEC104 APCI I Qualifier of Set Point Command ql field set to a reserved value |

# IEC104 Inspector Intrusion Rule Options

### iec104_apci_type

Verifies that the IEC104 message matches the IEC104 application protocol information control (APIC) type set in the option.

The `iec104_apci_type` intrusion rule option accepts a string specified using the full APIC type name, or uppercase or lowercase APIC type abbreviation.

**Type:** string

**Syntax:** `iec104_apci_type: <apic_type>;`

**Examples:**

```
iec104_apci_type: unnumbered_control_function;
```

```
iec104_apci_type: S;
iec104_apci_type: I;
iec104_apci_type: i;
```

### iec104_asdu_func

Verifies that the IEC104 message matches the IEC104 application service data unit (ASDU) function code set in the option.

The `iec104_asdu_func` intrusion rule option accepts a string specified using the uppercase or lowercase ASDU function code.

**Type:** string

**Syntax:** `iec104_asdu_func: <asdu_func>;`

**Examples:**

```
iec104_asdu_func: M_SP_NA_1;
iec104_asdu_func: m_sp_na_1;
```