http://dx.doi.org/10.14236/ewic/icscsr19.3

Increasing Visibility of IEC 104 Communication in the Smart Grid

Petr Matoušek
Brno University of Technology
Božetěchova 1/2
Brno, Czech Republic
matousp@fit.vutbr.cz

Ondřej Ryšavý
Brno University of Technology
Božetěchova 1/2
Brno, Czech Republic
rysavy@fit.vutbr.cz

Matěj Grégr
Brno University of Technology
Božetěchova 1/2
Brno, Czech Republic
mgregr@fit.vutbr.cz

Energy systems like smart grids are part of critical infrastructure and their interruption or blackout may have fatal consequences on energy production, distribution, and eventually the life of individual people. In order to secure communication in Industrial Control Systems (ICS) and detect cyber attacks on smart grids, we need to increase visibility of ICS communication so that an operator can see what commands are sent between ICS devices. Security monitoring of ICS transmission requires (i) retrieving monitoring data from ICS packets, (ii) processing and analyzing extracted data, (iii) visualizing the ongoing communication to the operator. The proposed work presents a concept of ICS flow monitoring system that extracts meta data from ICS packet headers and creates ICS flow records similarly to Netflow/IPFIX system. ICS flows represent communication in the smart grid network that is further visualized using dashboard and communication charts. Unlike traditional monitoring approach that works with network and transport layer data only, we extend flow monitoring to application layer with focus on ICS protocols. The proposed approach is demonstrated on monitoring IEC 60870-5-104 communication.

IEC 104, smart grid, ICS, security monitoring, SCADA, flow monitoring

1. INTRODUCTION

With the progress of digitization and industrial automation, *Industrial Control System* (ICS) plays an essential role in monitoring and controlling industrial devices, processes and events. The main function of ICS is to gather real-time data from industrial devices, realize device automation, and supervise the system, see Knapp and Langill (2015). An ICS concept covers a variety of communication systems including distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, and many others.

ICS communication was originally designed for serial communication that was physically separated from external networks. Recently, it has been adopted to operate over standard Ethernet link layer and the Internet Protocol (IP) with UDP and TCP transport on top of IP. This solution made possible to interconnect ICS networks over wide-area networks (WANs) and provide remote control and monitoring. Figure 1 shows various industrial protocols (MMS, Goose, Modbus, SV, IEC 104) operating within a smart grid substation and interconnecting Intelligent Electronic Devices (IEDs) controls power system equipment such as circuit breakers, bay controllers, or relays.

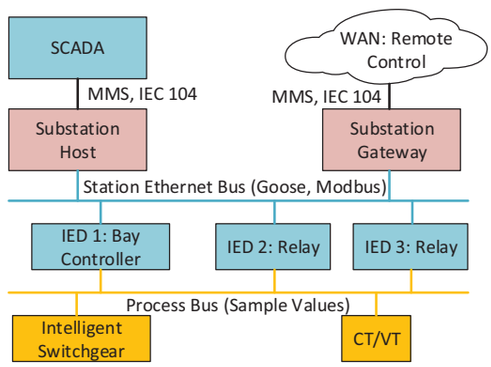


Figure 1: *SCADA communication in the substation*

Interconnection of ICS systems with IP networks uncovered lack of security of industrial protocols. Vulnerability of ICS communication to external attacks was revealed by the cyber attacks against Ukraine's power grid in December 2015, see Lee et al. (2016), and 2016, see analysis in Assante et al. (2017) and Cherepanov (2017). An ICS system of Ukrainian power grid was infected by

a malware that was installed on operator's station without noticing it. The malware called Industroyer by ESET or CrashOverride by Dragos, Inc., see Dragos (2017), masqueraded as a legitimate process for communication with Remote Terminal Units (RTUs). First, the malware scanned the internal network for RTUs and learnt their addresses and functions. Following that it tested ability to switch on and off RTU devices. Since the malware was communicating from inside the network, its behavior became unnoticed by an IDS system and a firewall that were located on the edge of the network. The case also unveiled missing visibility of ICS transmissions within the power grid as mentioned in Assante and Lee (2015). Without monitoring of ICS communication, it is hard to detect common cyber attacks like scanning, command injection, data spoofing, etc.

The issue of missing monitoring of ICS networks was highlighted by the Report of European Union Agency for Network and Information Security (ENISA), see ENISA (2016), which states that *without active network monitoring, it is very difficult to detect suspicious activity, identify potential threats, and quickly react to cyber attacks.* Firewalls, anti-virus software or IDS systems can detect security threats against ICS systems only partially.

For monitoring ICS communication, we can get inspiration from IP networks where security monitoring is well established. Monitoring techniques that are widely deployed in IP networks include SNMP monitoring, see Presuhn et al. (2002), IP flow monitoring, see Claise (2004), and system logging, see Gerhards (2009). These approaches can be applied on ICS systems to a certain extent. Since IP monitoring relies on IP layer, it cannot be applied on ICS protocols that run directly over link layer, e.g., Modbus or GOOSE. Also, due to the restricted hardware and firmware of RTUs and IEDs, it is not easy to implement SNMP agent or Syslog client on these devices.

However, passive network monitoring based on IPFIX protocol, see Claise et al. (2013), seems to be a viable option for ICS networks. IPFIX systems include an IPFIX probe or exporter that observes a traffic and creates IPFIX records with statistics data about ongoing network flows. IPFIX records are then exported to the IPFIX collector where are stored and visualized to network operator. Since IPFIX supports flexible definition of monitoring data, it is possible to extend IPFIX records so that they also include ICS monitoring data.

The proposed approach is demonstrated on passive monitoring of IEC 60870-5-104 (aka 104) communication, see IEC (2006) and Matoušek (2017). We show how retrieved monitoring data are obtained from IEC 104 packets and sent to the IPFIX collector. By analyzing and visualizing ICS monitoring data, we are able to get network statistics about the communication in a ICS network (number of connected hosts, transmitted data, etc.), detect cyber security incidents (unauthorized access, scanning, DoS attack), or system operation (detection of malfunctioning devices, misconfiguration, etc.).

1.1. Structure of the text

The paper is structured as follows. Section 2 gives an overview of published work related to the monitoring and security of IEC 104 communication. Section 3 describes IEC 104 communication and shows how IEC 104 flows are built from packet headers. Section 4 focuses on IEC 104 visibility, namely, what we can learn from monitoring data about IEC communication. Section 5 compares different levels of ICS visibility and shows what can be observed from monitoring data. The last section concludes our work.

1.2. Contribution

The main contribution of the paper is a design of IEC 104 monitoring system that provides application visibility of IEC 104 communication. The system is based on IPFIX flow monitoring extended by IEC 104 operations obtained from IEC 104 packet headers. Using IEC 104 flow records we can increase visibility of smart grid control communication that helps to detect cyber attacks and anomaly behavior of the system. The proposed system was implemented as a plugin to the IPFIX monitoring probe and evaluated on available datasets.

2. STATE-OF-THE-ART

Protection of industrial control systems in smart grids is an important task especially with relation to the recent cyber attacks, see Lu et al. (2010) and Miller and Rowe (2012). NIST Guide to ICS Security, see Stouffer et al. (2015), gives an overview of past attacks on ICS systems with recommendation how to secure ICS architecture using network segregation, firewall rules, NAT translation and other techniques.

Security of ICS/SCADA networks is often arranged by proprietary IDS systems with deep-packet inspection (DPI) focused on selected ICS protocols. Generally, IDS systems parse ICS packets and extract selected data from ICS payload that are further subject to signature-based or behavior-based analysis. If a suspicious communication is detected, an alert is risen and the traffic is filtered out. IDS systems with DPI provide active scanning and analysis of incoming ICS traffic which puts huge

requirements on processing power and memory. Because of DPI analysis, a pre-processor (parser) is to be implemented for each ICS protocol that is part of IDS system, see Horkan (2015). IDS systems are usually located at the edge of ICS networks which limits the protection to external threats only. The proposed system of monitoring ICS visibility can be deployed both on the edge of the network or inside the network which covers both external and internal threat scenarios.

Similar monitoring system for protecting SCADA communication in power grid was proposed by Jarmakiewicz et al. (2017) where the authors implemented SCADA probes observing IEC 104 and IEC 61850 communication. Protection includes two phases: training and detection. In the first phase, the SCADA probe learns profiles of authorized control messages transmitted between SCADA nodes (white list). Then the probe observes active SCADA communication and compares it against learnt profiles. Unlike SCADA probes, our monitoring approach uses IPFIX standard which is supported by many Security Information and Event Management (SIEM) systems, so that ICS monitoring can be incorporated into common monitoring systems. Obtained IPFIX monitoring data can be used for whitelisting or anomaly detection similar to SCADA probes.

Another IDS system for IEC 104 with Snort rules defining various types of attacks was proposed in Yang et al. (2013). As discussed above, IDS systems are useful for protecting the SCADA network for external threats, however they do not provide visibility of internal communication which is our main focus.

Common attacks on IEC 104 communication including replay attack, man-in-the-middle attack, command modification and command injection are described in Maynard et al. (2014) where the authors simulate these attacks in order to show how attacker can compromise the integrity of SCADA communication. Communication patterns of these attacks can be revealed in IPFIX records of IEC 104 communication as proposed in this paper.

Recent papers discussing ICS communication also focus on advanced protocol analysis and anomaly detection. For example, Lin and Nadjm-Tehrani (2018) observe IEC 104 traffic patterns such as inter-arrival times of spontaneous events and classify communication into previously observed five different groups. This helps them to identify anomaly in communication. Unlike our approach, they do not observe relations between IEC 104 commands. Our approach is more general because the monitoring system observes any IEC 104 communication (not only spontaneous events) and the obtained data can be used for time-based analysis but also for detecting communication exchange patterns, statistics, etc.

3. MONITORING IEC 104 COMMUNICATION

IEC 104 protocol is a part of IEC Telecontrol Equipment and Systems standard IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation. IEC 104 operates over TCP using client-server communication model and delivers supervisory data and acquisition request for controlling power grids.

IEC 104 messages are exchanged between the controlled and the controlling station. *Controlled station* (also called outstation, RTU slave) is monitored or commanded by a master station. *Controlling station* (typically a PC with SCADA system, RTU master) performs control of outstations. IEC 104 communication is delivered in the *monitoring direction*, i.e., from controlled station to the controlling station, or in the *control direction*, i.e., sent by a SCADA system towards the controlled station (RTU), see Figure 2.

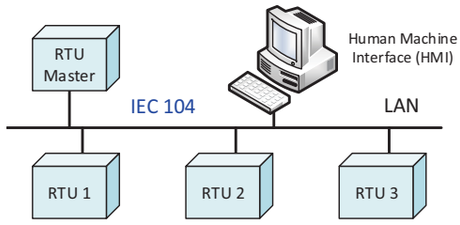


Figure 2: *IEC 104 topology*

3.1. IEC 104 Protocol

IEC 104 protocol IEC (2006) is implemented on application layer (Layer 7) of TCP/IP stack using Application Protocol Data Unit (APDU) and Application Service Data Unit (ASDU), see Figure 3. Based on APDU Control field 1, three APDU formats are defined: I-frames for transmitting data, S-frames for numbered supervisory operations, and U-frames transmitting unnumbered control functions (test frame, start transfer, stop transfer).

The most important APDUs for security monitoring are I-frames that transmit ASDUs. The ASDU includes two sections: fixed-length ASDU header and a variable-length list of information objects. The header includes *ASDU type* (e.g., single point of information, measured value, regulating step command, read command), *number of transmitted objects*, *cause of transmission* (COT, e.g., periodic, spontaneous, activation, interrogation) and *ASDU address* (station address).

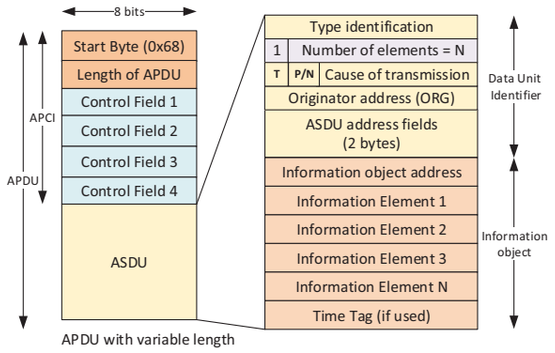


Figure 3: *IEC 104 protocol header*

Each *information object* is addressed by *Information Object Address* (IOA) that identifies particular data on the given node. For each ASDU type, the IEC 104 standard defines the format of information object, that includes information elements which form the object and structure of the data. For example, information object in ASDU with type 36 (Measured value, scaled value with time tag) and cause of transmission 20 (interrogation) contains two information elements: SVA (Scaled value) and QDS (Quality descriptor), see Figure 4.

Type = 36 (M_ME_TF_1)		
1	Number of elements = 1	
T	P/N	COT=20 (interrogation)
Originator address = 1		
Common ASDU Address = 1		
IO Address (IOA) = 50		
Scaled Value (SVA) = 46		
Quality Descriptor (QDS) = 0x00		
CP56Time = Jul 11, 2018 16:23		

Figure 4: *Example of IEC 104 packet*

Typical IEC communication is depicted in Table 1 that shows selected IEC 104 transactions (transactions no. 2,6,8,10,14) exchanged between the IEC 104 master and slave in both directions: control and monitoring. Each transaction contains at least one ASDU with an object addressed by the Information Object Address (IOA), Cause of Transmission (COT) and transmitted value or command. You can notice that one ASDU may transmit several IOA objects with different IOA addresses, COTs and data. The proposed monitoring system retrieves interesting data from IEC 104 packets in order to create IEC 104 flows for ICS monitoring.

Master (10.20.102.1) < --- > Slave (10.20.100.108) communication				
No.	**Direction**	**object**	**Cause of transmission (COT)**	**Setting values of the information element**
2	---->	IOA=13	activation	single command ON
	<----	IOA=13	activation confirmation	single command ON
		IOA=13	activation termination	single command ON
		IOA=13	spontaneous	SIQ=0x01 (SPI=ON) with time tag
6	---->	IOA=1	activation	regulating step cmd: UP
	<----	IOA=1	activation confirmation	regulating step cmd: UP
		IOA=1	activation termination	regulating step cmd: UP
		IOA=1	spontaneous	step position = 1
8	---->	IOA=3	activation	bitstring = 0x 02 00 00 00
	<----	IOA=3	activation confirmation	bitstring = 0x 02 00 00 00
	<----	IOA=3	activation termination	bitstring = 0x 02 00 00 00
		IOA=3	spontaneous	bitstring = 0x 02 00 00 00
10	---->	IOA=1	activation	set point, normalized value = 0.03125
	<----	IOA=1	activation confirmation	set point, normalized value = 0.03125
	<----	IOA=1	activation termination	set point, normalized value = 0.03125
		IOA=1	spontaneous	measured valued, normalized value = 0.03125
14	---->	IOA=1	activation	set point, short float = 3.14
	<----	IOA=1	activation confirmation	set point, short float = 3.14
		IOA=1	activation termination	set point, short float = 3.14
		IOA=1	spontaneous	measured value, short float= 3.14

Table 1: *Example of IEC 104 communication*

3.2. Building IEC 104 Flows

IP flow monitoring is a well-established technique defined by RFC 3954 for Netflow protocol, see Claise (2004), or for IPFIX protocol, see RFC 7011 and 7012 defined by Claise et al. (2013) and Claise and Trammel (2013). An IP flow is a sequence of packets going through an observation point and having the same properties. The key five properties that defines the IP flow and are obtained from packet headers are source and destination IP addresses, source and destination ports, and IP protocol. All packets having the same key properties form one IP flow. IPFIX monitoring probe observes ongoing IP flows and collects statistical data about them, e.g., timestamp of the first packet, number of transmitted packets and bytes of the flow, flow duration, etc. Statistical data are written into a IPFIX flow record that is later sent to the IPFIX monitoring center (collector).

The IP flow uses Layer 3 and 4 data for monitoring only. In order to increase IEC 104 visibility, we have to redefine the flow and add new fields extracted from IEC 104 header. For our purposes, IEC 104 flow will include all five key properties of the IP flow extended by the following IEC 104 values:

- APDU frame type
- ASDU type
- ASDU cause of transmission (COT)
- Number of information object
- Originator address (ORG)
- ASDU address (COA)

In addition to standard IP flows, we have to deal with several ASDUs encapsulated in one TCP packet. Using traditional IP flow monitoring these ASDUs would be aggregated into one IP flow record. In such case, IEC 104 visibility would be lost since the flow record cannot keep several different values within one field, e.g., COT. To deal with this issue, we need

to split an IP flow with multiple ASDUs into several separated IEC 104 flows where each IEC 104 flow transmits one ASDU. On one side, this will increase the number of monitoring flows, on other side the required IEC 104 visibility will be preserved.

Table 2 shows an example of IEC 104 flows extracted from IEC 104 communication. For space limit, not all flow items are showed. Besides IP addresses and ports we can also see APDU format, ASDU type, number of information objects, cause of transmission, originator address and ASDU address.

	Src IP	Dst IP	Src Port	Dst Port	Len	Format	Type	Item no.	COT	ORG	COA
1	192.168.1.113	10.209.13.145	50876	2404	4	2	NIL	NIL	NIL	NIL	NIL
2	10.209.13.145	192.168.1.113	2404	50876	4	2	NIL	NIL	NIL	NIL	NIL
3	192.168.1.113	10.209.13.145	50876	2404	14	0	100	1	6	1	37133
4	10.209.13.145	192.168.1.113	2404	50876	14	0	70	1	4	0	37133
5	10.209.13.145	192.168.1.113	2404	50876	14	0	100	1	7	1	37133
6	192.168.1.113	10.209.13.145	50876	2404	4	1	NIL	NIL	NIL	NIL	NIL
7	10.209.13.145	192.168.1.113	2404	50876	23	0	1	10	20	1	37133
8	10.209.13.145	192.168.1.113	2404	50876	14	0	3	1	20	1	37133
9	192.168.1.113	10.209.13.145	50876	2404	4	1	NIL	NIL	NIL	NIL	NIL
10	10.209.13.145	192.168.1.113	2404	50876	14	0	100	1	10	1	37133
11	10.209.13.145	192.168.1.113	2404	50876	16	0	11	1	3	0	37133

Table 2: *Example IEC 104 flows (only selected fields)*

The fields with NIL value in entries no. 1,2,6 and 9 indicate APDUs without the ASDU payload, i.e., U-frames (frame type=2) or S-frame (frame type=1). Only I-frames (with frame type=0) transmit ASDUs as showed in Figure 3.

By observing IEC 104 flow, we can see that there are two controlling stations with originator addresses ORG=0 or 1 running on the same IP address 192.168.1.113. Flow no. 3 describes an APDU with an I-frame (type=0) which was sent by a controlling station with ORG=1 to the controlled station with ASDU address 37133. Type of this ASDU is 100 (interrogation command) and COT = 6 (activation). The ASDU transmitted one information object.

The above described IEC 104 flows were obtained by an IEC 104–enabled IPFIX probe that monitored IEC 104 communication. The parser for IEC 104 was developed in frame of IRONSTONE research project and is freely available at project web site[1].

4. TOWARDS IEC 104 VISIBILITY

Network visibility provides an insight into day-to-day activities of the monitored network. The intrinsic characteristics of industrial networks, namely stable communications patterns, static topologies, periodic behavior and a limited number of applications and protocols, can be used to implement effective network visibility solution. IEC 104 communication is strict with the use of a limited number of fixed communication patterns. By collecting monitoring data, it is possible to identify whether the endpoint plays the role of controlling or controlled station. Due to the static topology of IEC 104 networks, the number and function of connected devices does not change so much.

Visibility can be detected at different levels of details. Communication visibility provides aggregated network information that can be represented, for example, by the statistical profile of the entire network communication. At a lower level, the visibility characterizes the aggregated communication between two devices. The lowest level enables to view and analyze a single data transaction with transmitted object values. Different techniques can be adopted for network monitoring providing the required information.

- *Packet-based monitoring* analyzes every single packet and offers the most abundant data source for network visibility. Decoded information from packet traces usually needs to be aggregated to provide adequate information for network visibility.
- *Flow-based monitoring* deals only with the selected data from the communication that should, however, provide enough information on important events in the network as well as on the overall network state. Flexible format of flow records using IPFIX allows users to implement new user-defined fields, and thus to provide enough data for network visibility at multiple levels.

Following text demonstrates how IEC 104 flows increase IEC 104 visibility on typical scenarios.

4.1. Observing IEC 104 Activity

The main goal of ICS visibility is to discover all communicating ICS nodes on the network and all transmission initiated by them. By observing IEC 104 flows we get a list of active IEC 104 hosts, see Table 3. The table shows that node 10.209.13.145 was communicating with two other IEC 104 nodes. The table contains data aggregated per connection identified by the IP address and port number of the source and destination.

srcIP	srcPort	dstIP	dstPort	packets
10.209.13.145	2404	192.168.1.113	50876	14
10.209.13.145	2404	192.168.1.44	1099	124
192.168.1.113	50876	10.209.13.145	2404	12
192.168.1.44	1099	10.209.13.145	2404	86

Table 3: *A list of active IEC 104 hosts*

[1]See `http://www.fit.vutbr.cz/research/prod/index.php.en?id=558` [April 2019]

Going into detailed communication, we can analyze ASDU types and causes of transmission (COT) that are part of extended IPFIX records. Detailed view on IEC 104 transmission is in Table 4 that reveals details of transmitted ASDUs and COTs. For example, the last row in the Table describes communication of the IEC node with IP address 192.168.11.248. The node sent 9,104 messages with type 36 (measured value, short floating point) and COT 3 (spontaneous transfer) to station 192.168.11.111. The entry describes regular monitoring of the IEC 104 object.

srcIP	srcPort	dstIP	dstPort	ASDU type	COT	packets
192.168.11.111	56693	192.168.11.248	2404	122	13	62
192.168.11.111	56693	192.168.11.248	2404	124	13	42
192.168.11.248	2404	192.168.11.111	56693	120	13	21
192.168.11.248	2404	192.168.11.111	56693	121	13	21
192.168.11.248	2404	192.168.11.111	56693	123	13	24
192.168.11.248	2404	192.168.11.111	56693	125	13	9
192.168.11.248	2404	192.168.11.111	56693	36	3	9104

Table 4: *Analyzing ASDU types of IEC 104 communication*

We can also notice the file transfer that happened between nodes 192.168.11.111 and 192.168.11.248. By interpreting ASDU types and COTs, we see that (i) node 192.168.11.111 invoked operation *call directory, select and call the file* in node 192.168.11.248 (type=122), then (ii) node 192.168.11.248 confirmed that the file is ready (type=120,121) and finally (iii) the file segments were transmitted (type=125).

We can also identify IEC 104 nodes sending data in control direction. Table 5 shows communication of an RTU master sending data to a RTU slave in control direction. Following commands are sent by the master RTU: interrogation commands (type=100), single commands (type=45,58), double commands (type=59), or set-point commands (type=50).

srcIP	srcPort	dstIP	dstPort	ASDU type	COT	packets
10.0.0.10	1075	10.0.0.10	2404	100	6	1
10.0.0.10	1075	10.0.0.10	2404	45	6	2
10.0.0.10	1075	10.0.0.10	2404	50	6	4
10.0.0.10	1075	10.0.0.10	2404	58	6	2
10.0.0.10	1075	10.0.0.10	2404	59	6	4

Table 5: *RTU master to RTU slave communication*

Long-term time analysis of IEC 104 flow monitoring exposes stable behavior of IEC 104 communication. Figure 5 shows IEC 104 communication between two IEC 104 nodes within 3 days. The green line represents ASDUs sent with monitoring data to the RTU with COT=3 (spontaneous event), the blue line depicts file transfers between these nodes (COT=13, data transmission).

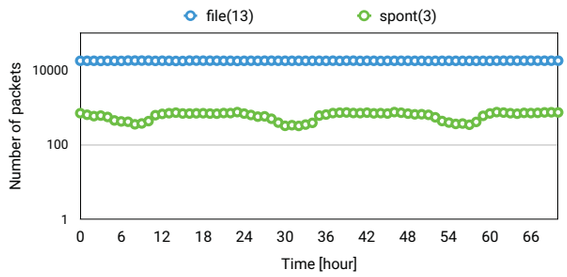


Figure 5: *IEC 104 communication*

4.2. Activation of an IEC 104 device

Considering time sequences of IEC 104 communication, we can observe typical communication patterns, for example, activation of a IEC 104 node. Table 6 shows IEC 104 flows related to the activation of node 10.33.232.121 by node 10.33.232.120 with the timestamp.

timestamp	SrcIP	srcPort	dstIP	dstPort	ASDU type	COT	COA
08:24:42.18	10.33.232.120	44216	10.33.232.121	2404	45	6	83
08:24:52.336	10.33.232.121	2404	10.33.232.120	44216	45	7	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	45	10	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	1	3	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	1	3	83

Table 6: *IEC 104 node activation*

The same communication can be visualized using message flow chart, see Figure 6. Having IEC

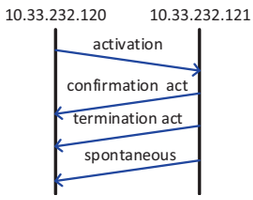


Figure 6: *IEC 104 node activation command sequence*

104 flows, a monitoring system can learn typical communication profiles from previously observed IEC 104 flows. Based on that, it can check if the current IEC 104 communication matches any of known profiles and if not, it can classify the traffic as anomalous, similarly to the approach by Lin and Nadjm-Tehrani (2018).

4.3. Requesting Unknown Resources

IEC 104 flow monitoring data also reveals a scenario when an IEC 104 node requests unknown resources. This may indicate either misconfiguration of the sending device or the scanning attack. Table 7 shows IEC 104 communication that was sent by a master RTU with 10.211.55.2 to a slave RTU at 10.21.55.5.

srcIP	dstIP	ASDU type	COT	ORG	COA	Description
10.211.55.2	10.211.55.5	50	6	2	65281	Activation
10.211.55.5	10.211.55.2	50	46	2	65281	Unknown ASDU address
10.211.55.2	10.211.55.5	50	6	2	1	Activation
10.211.55.5	10.211.55.2	50	47	2	1	Unknown object
10.211.55.2	10.211.55.5	50	10	2	1	Activation Termination
10.211.55.5	10.211.55.2	50	45	2	1	Unknown COT

Table 7: *IEC 104 wrong data*

The flows contain a set-point command (ASDU type=50) that is used to control the information object, e.g., to set the value of the object. Packets in this scenario were sent with a wrong ASDU address, a wrong object address IOA and an unknown COT value. Such ASDUs were refused by the receiver node by response ASDUs with COT=46 (unknown ASDU address), COT=47 (unknown object ID), or COT=45 (unknown Cause of Transmission) in IEC 104 flow database. When such IEC 104 responses are detected, the monitoring center may raise an alert to inform the system operator about the unknown request. The IEC 104 flow record contains an ASDU that was requested and identification of the original sender. For example, the second entry in Table 7 says that a node with IP address 10.211.55.2 and ASDU originator address 2 requested data from IEC node with IP address 10.211.55.5 and ASDU address 65281. The request was refused because of unknown destination ASDU address.

4.4. Identifying Cyber Attacks

By observing long-term communication patterns of IEC traffic we are able to identify unusual behavior that deviates from typical communication profiles. Figure 7 shows a case when an attacker tries to manipulate with IED node by sending Act and ActTerm ASDUs. The blue line represents the number of Act commands (a), resp. ActTerm commands (b) sent during 10 minutes period of normal traffic. The green line shows the number of Act and ActTerm commands during the attack. During normal communication only 1 or 2 activation commands were sent within 10 minutes while during the attack 12 activations were detected within 2 minutes.

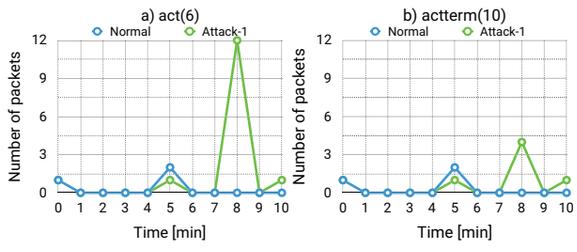


Figure 7: *Distribution of (a) Act packets and (b) ActTerm packets during the normal usage and during the attack.*

By comparing the number of sent Act ASDUs with the number of received ActTerm ASDUs we can notice, that that the number of Acts and ActTerms is the same for the normal communication which means that all Act ASDUs were confirmed by ActTerm ASDUs. However, during the attack, some Act commands were ignored, i.e., the number of received ActTerm ASDUs is lower than the number of requested Act commands. This presented attack simulated behavior of the Industroyer malware Dragos (2017) when an IED device was continuously switched on and off for a few seconds. Using IEC 104 flow monitoring we are able to detect such behavior in flow statistics.

5. INCREASING IEC 104 VISIBILITY

As our experiments show, passive monitoring using the IPFIX architecture enhanced by selected IEC 104 header values increases visibility of ICS communication. IEC 104 flow records are stored in the IPFIX collector and visualized by ICS monitoring center using tables, charts and timelines that reveal active transmissions on the network. Using historical IEC 104 flows we can build a baseline of IEC 104 communication and observe normal behavior of IEC transmission by comparing active transmission with the baseline as demonstrated in Figure 7.

The question is what level of details of IEC 104 communication is sufficient for security monitoring? Naturally, with the increased number of details, more processing power is required by the probe and more storage is needed to save monitoring data. Let us look at attack described in Section 4.4 and see how the granularity of flow records impacts the visibility of ICS communication.

5.1. IEC 104 flows

Table 8 shows repeated patterns of ASDUs with COT 6 (Activation), 7 (Activation Confirmation), and 10 (Activation Termination).

srcIP	dstIP	srcPort	dstPort	bytes	len	fmt	type	num	cot	org	coa
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	10	2	3
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	10	2	3
172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3
172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3
172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL

Table 8: *IEC 104 flows during the attack.*

We can also notice that the sending node with IP 172.16.1.100 sent `double command` (type=46) but we do not see details about the command. Nevertheless, we can at least detect abnormal behavior with respect to the IEC 104 communication baseline, identify ASDU nodes related with the attack and list operations that caused the attack.

5.2. IP flows

The above mentioned approach can be compared to the traditional IP flow monitoring where only Layer 3 and Layer 4 data are observed by an IPFIX monitoring probe. Table 9 shows IP flows related to the attack and obtained by the Silk analyzer[2]. We can see that each packet with an ASDU content forms an individual flow, however without processing ASDU layer, we cannot see much details about ICS behavior. However, by analyzing flow statistics, we can at least build similar baseline like in the case of IEC 104 flows.

Src IP	Dst IP	Src Port	Dst Port	Proto	Pkts	Bytes	Starting time	Ending Time
172.16.1.100	172.16.1.1	13748	2404	6	1	56	2017/11/03T13:57:08.419	2017/11/03T13:57:08.419
172.16.1.1	172.16.1.100	2404	13748	6	1	56	2017/11/03T13:57:08.424	2017/11/03T13:57:08.424
172.16.1.100	172.16.1.1	13748	2404	6	1	40	2017/11/03T13:57:08.464	2017/11/03T13:57:08.464
172.16.1.100	172.16.1.1	13748	2404	6	1	46	2017/11/03T13:57:11.763	2017/11/03T13:57:11.763
172.16.1.1	172.16.1.100	2404	13748	6	1	40	2017/11/03T13:57:11.963	2017/11/03T13:57:11.963
172.16.1.100	172.16.1.1	13748	2404	6	1	56	2017/11/03T13:57:12.347	2017/11/03T13:57:12.347
172.16.1.1	172.16.1.100	2404	13748	6	1	56	2017/11/03T13:57:12.466	2017/11/03T13:57:12.466
172.16.1.100	172.16.1.1	13748	2404	6	1	40	2017/11/03T13:57:12.507	2017/11/03T13:57:12.507
172.16.1.1	172.16.1.100	2404	13748	6	1	56	2017/11/03T13:57:12.517	2017/11/03T13:57:12.517
172.16.1.100	172.16.1.1	13748	2404	6	1	40	2017/11/03T13:57:12.556	2017/11/03T13:57:12.556
172.16.1.100	172.16.1.1	13748	2404	6	1	56	2017/11/03T13:57:14.667	2017/11/03T13:57:14.667
172.16.1.100	172.16.1.1	13748	2404	6	1	46	2017/11/03T13:57:14.764	2017/11/03T13:57:14.764
172.16.1.1	172.16.1.100	2404	13748	6	1	40	2017/11/03T13:57:14.765	2017/11/03T13:57:14.765
172.16.1.1	172.16.1.100	2404	13748	6	1	56	2017/11/03T13:57:14.792	2017/11/03T13:57:14.792
172.16.1.100	172.16.1.1	13748	2404	6	1	40	2017/11/03T13:57:14.832	2017/11/03T13:57:14.832

Table 9: *IP flows during the attack obtained by Silk.*

As we could see, Silk analyzer forms IP flows from each packet which is not typical for IP flow monitoring. Table 10 shows IP flows obtained by softflowd[3]. The whole attack is aggregated into two IP flows exchanged between IEC 104 nodes. Using this flow monitoring, we cannot detect or reconstruct attacks against ICS communication.

Starting time	Ending Time	Duration	Src IP	Dst IP	Src Port	Dst Port	Proto	Flags	Pkts	Bytes
3.11.2017 13:48	3.11.2017 14:04	949.946	172.16.1.1	172.16.1.100	2404	13748	TCP	.AP...	120	6280
3.11.2017 13:48	3.11.2017 14:04	949.946	172.16.1.100	172.16.1.1	13748	2404	TCP	.AP...	97	4462

Table 10: *IP flows during the attack obtained by softflowd.*

5.3. Extended IEC 104 flows

The level of details of monitoring ICS communication depends on the ICS processor in the IPFIX probe. Table 11 adds IOA address that shows which information objects is a target of the attack.

By analyzing information elements forming the information object, as described in Section 3.1, we can also see what operations were applied on the information object with IOA=11272301, see Table 12.

[2]See `https://tools.netsa.cert.org/silk/` [May 2019].
[3]See `https://github.com/irino/softflowd` [May 2019].

Timestamp	srcIP	dstIP	srcPort	dstPort	bytes	len	fmt	type	num	cot	org	coa	ioa
14:57:08.41	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:08.42	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:11.76	172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL	NIL
14:57:12.34	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:12.46	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:12.51	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	10	2	3	311272301
14:57:14.66	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:14.76	172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL	NIL
14:57:14.79	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:16.96	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:16.96	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:17.76	172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL	NIL
14:57:18.70	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:18.83	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:18.87	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	10	2	3	311272301
14:57:20.65	172.16.1.100	172.16.1.1	13748	2404	56	14	0	46	1	6	2	3	311272301
14:57:20.78	172.16.1.1	172.16.1.100	2404	13748	56	14	0	46	1	7	2	3	311272301
14:57:21.76	172.16.1.100	172.16.1.1	13748	2404	46	4	1	NIL	NIL	NIL	NIL	NIL	NIL

Table 11: *IEC 104 flows extended by IOA address.*

srcIP	dstIP	fmt	type	num	cot	org	coa	Details
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=ON
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: negative confirmation
172.16.1.100	172.16.1.1	1	NIL	NIL	NIL	NIL	NIL	
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=OFF
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: ok
172.16.1.1	172.16.1.100	0	46	1	10	2	3	IOA=11272301, ActTerm: ok
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=ON
172.16.1.100	172.16.1.1	1	NIL	NIL	NIL	NIL	NIL	
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: negative confirmation
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=OFF
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: ok
172.16.1.100	172.16.1.1	1	NIL	NIL	NIL	NIL	NIL	
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=ON
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: ok
172.16.1.1	172.16.1.100	0	46	1	10	2	3	IOA=11272301, ActTerm: ok
172.16.1.100	172.16.1.1	0	46	1	6	2	3	IOA=11272301, Double Command Operation=OFF
172.16.1.1	172.16.1.100	0	46	1	7	2	3	IOA=11272301, ActConf: negative confirmation
172.16.1.100	172.16.1.1	1	NIL	NIL	NIL	NIL	NIL	

Table 12: *IEC 104 flows with information elements.*

5.4. Summary

As seen above, the proposed model of ICS visibility using IPFIX flows extended by ICS values is flexible. Granularity of visibility of ICS communication depends on ICS pre-processor (plugin) of ICS-enabled probe and can be enhanced according to the operational requirements. Figure 8 displays multiple levels of granularity of IEC 104 monitoring.

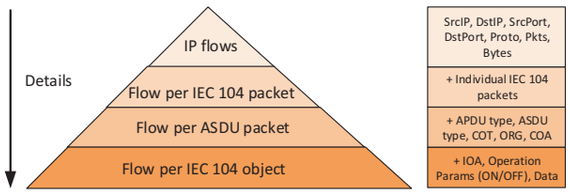


Figure 8: *IEC 104 visibility.*

Traditional IP flows offer only statistics about source and destination on Layer 3 and 4 which does not provide sufficient visibility of ICS transmission, as demonstrated on scenario in Table 10.

Splitting an IP flow into IEC104-based flows as shown in Table 9 unveils detailed statistics about individual IEC 104 packets but further analysis relies on Layer 3 and 4 data only and no real ICS visibility is provided. However, some types of attacks can be detected on this level.

The third level requires Layer 7 processing on the monitoring probe. Monitoring data reveals details about ASDUs such as type, cause of

transmission, originator address, ASDU address and number of transmitted information objects. As showed in previous scenarios, such level of visibility is sufficient for observing day-to-day behavior of IEC 104 nodes, creating communication profiles as mentioned in Section 4.2, detecting IEC 104 resource scanning and identifying cyber attacks described by communication patterns or deviation from the baseline.

The most detailed level is obtained when processing individual IEC 104 information objects and information elements. This corresponds to full packet capturing. However, Layer 7 processing is CPU and memory intensive. This level of details is implemented by IDS and IPS systems which are able to process much lower traffic bandwidth (around 100 Mb/s) comparing to IPFIX probes on level 3 which processes data on tens of Gb/s. As demonstrated on previous scenarios, level 3 is sufficient to give visibility of active IEC 104 communication.

6. CONCLUSIONS

In recent years, several vulnerabilities have been exploited in ICS systems demonstrating the need to improve security of these critical systems. Many attacks became unnoticed by security devices that protect ICS network perimeter but do not prevent attacks from the inside of the system.

This paper presented the monitoring system of ICS communication based on extended IPFIX probes that captures the selected application protocol data. In our study we focused on smart grid communication protocol IEC 104. The presented approach describes how IPFIX can be extended for IEC 104 protocol pre-processing which increases the visibility of smart grid control communication. Since it is passive monitoring, it does not affect perfomance of the monitored system.

We demonstrated that IEC 104 flows can be used to detect cyber attacks and as a source data for analysis of system behavior. Various levels of details can be implemented in the ICS-enabled IPFIX probe as presented in Section 5.4. In real-world deployment level 3, i.e., monitoring flows per ASDU packet, is sufficient to visualize important details of ICS transmission and detect common cyber attacks such as network scanning and manipulation with IEC 104 resources. By applying statistical analysis, we can also reveal unusual behavior as shown in Section 4.4.

Further work will be focused on detailed analysis of IPFIX flow data aiming to provide methods for attack detection and diagnostics. We plan to evaluate and adapt existing methods proposed for anomaly detection of ICS communication. Because of lack of available long-term datasets of ICS communications, we also aim to create a corpus of IEC 104 communication samples that would help other researchers who work with network monitoring and anomaly detection of ICS systems.

ACKNOWLEDGMENTS

This work is supported by BUT project ”ICT Tools, Methods and Technologies for Smart Cities” (2017–2019), no. FIT-S-17-3964, and project ”IRONSTONE: IoT Monitoring and Forensics” (2016–2019), no. TF03000029, funded by the Technological Agency of the Czech Republic.

REFERENCES

Assante, M. J. and R. M. Lee (2015, October). The Industrial Control System Cyber Kill Chain. Technical report, SANS Institute.

Assante, M. J., R. M. Lee, and T. Conway (2017, August). Modular ICS Malware. Technical report, Electricity Information Sharing and Analysis Center (E-ISAC).

Cherepanov, A. (2017, June). Win32/Industroyer. A new threat for industrial control systems. Technical report, ESET.

Claise, B. (2004, October). *Cisco Systems NetFlow Services Export Version 9*. IETF RFC 3954.

Claise, B. and B. Trammel (2013, September). *Information Model for IP Flow Information Export (IPFIX)*. IETF RFC 7012.

Claise, B., B. Trammel, and P. Aitken (2013, September). *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*. IETF RFC 7011.

Dragos (2017, June). CrashOverride. Analysis of the Threat of Electric Grid Operations. Technical report, Dragos Inc.

ENISA (2016, December). Communication network dependencies for ICS/SCADA Systems. Technical report, European Union Agency for Network and Information Security (ENISA).

Gerhards, R. (2009, March). *The Syslog Protocol*. IETF RFC 5424.

Horkan, M. (2015, July). Challenges for IDS/IPS Deployment in Industrial Control Systems. Technical report, SANS Institute.

IEC (2006, June). Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles. Standard IEC 60870-5-104:2006, International Electrotechnical Commission, Geneva.

Jarmakiewicz, J., K. Parobczak, and K. Maślanka (2017). Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection 18*, 20 – 33.

Knapp, E. D. and J. T. Langill (2015). *Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress.

Lee, R. M., M. J. Assante, and T. Conway (2016, March). Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. Technical report, Electricity Information Sharing and Analysis Center (E-ISAC).

Lin, C.-Y. and S. Nadjm-Tehrani (2018). Understanding IEC-60870-5-104 Traffic Patterns in SCADA Networks. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, CPSS '18, New York, NY, USA, pp. 51–60. ACM.

Lu, Z., X. Lu, W. Wang, and C. Wang (2010, Oct). Review and evaluation of security threats on the communication networks in the smart grid. In *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, pp. 1830–1835.

Matoušek, P. (2017). Description and analysis of IEC 104 Protocol. Technical Report FIT-TR-2017-12, Brno University of Technology.

Maynard, P., K. McLaughlin, and B. Haberler (2014). Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks. In *Proceedings of the 2Nd International Symposium on ICS & SCADA Cyber Security Research 2014*, ICS-CSR 2014, UK, pp. 30–42. BCS.

Miller, B. and D. C. Rowe (2012). A survey of SCADA and critical infrastructure incidents. In *In Proceedings of the 1st Annual conference on Research in information technology, RIIT '12*, pp. 51–56. ACM.

Presuhn, R., J.Case, K.McCloghrie, M.Rose, and S.Waldbusser (2002, December). *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*. Ietf rfc 3416.

Stouffer, K., V. Pillitteri, M. Abrams, and A. Hahn (2015). Guide to Industrial Control Systems (ICS) Security. Technical Report NIST-SP-800-82r2, National Institute of Standards and Technology.

Yang, Y., K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang (2013, July). Intrusion detection system for iec 60870-5-104 based scada networks. In *2013 IEEE Power Energy Society General Meeting*, pp. 1–5.