IEC TR 62351-90-3

Edition 1.0 2021-03

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 90-3: Guidelines for network and system management

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 62351-90-3

Edition 1.0 2021-03

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 90-3: Guidelines for network and system management

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-9529-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-3: Guidelines for network and system management

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TR 62351-90-3 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Report.

The text of this Technical Report is based on the following documents:

DTR	Report on voting
57/2255/DTR	57/2337/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

A list of all parts of the IEC 62351 series, under the general title: *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-3: Guidelines for network and system management

1 Scope

This part of IEC 62351, which is a technical report, provides guidelines for efficiently handling both IT and OT data in terms of their monitoring, classification and correlations on them to deduce any possible useful outcomes about the state of the power system.

The convergence of information technologies (IT) and operational technologies (OT) refers to the integration of the systems, processes and data associated with the domains of IT and OT. This document provides guidelines for a comprehensive security monitoring for power grid components based on IT/OT convergent systems. The emphasis is about the development of a methodology and a set of recommendations for utility operators to build a general monitoring framework based on the analysis of the data collected from different IT and OT systems through network management, traffic inspection, and system activity readings. As such, the monitoring framework that this document introduces relies on the integration of management and logging information obtained using IEC 62351-7 and IEC 62351-14, respectively. Further systems and data sources from IT and OT would be considered such as the data obtained, for instance, through the IT network management using the Simple Network Management Protocol (SNMP), the passive network monitoring, and the functional characterization of control and automation processes.

This document's recommendations include the implementation of data collection, filtering and correlation mechanisms. The development of data analytics algorithms is out of the scope of this document and would be left to utility operators and owners. Finally, applications of the general monitoring framework guidelines and recommendations are provided for different power grid environments, namely for IEC 61850 substations and for Distributed Energy Resources (DER) systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC TS 62351-14, *Power systems management and associated information exchange – Data and communications security – Part 14: Cyber Security Event Logging*[1]

IEC TR 62351-90-2, *Power systems management and associated information exchange – Data and communications security – Part 90-2: Deep packet inspection of encrypted communications*

IEC TR 61850-90-4, *Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines*

IEC 60870-5-101, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

IEC 60870-5-104, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

IEEE 1815-2012, *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and IEC 62351-7 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

4 Abbreviated terms and acronyms

Additional abbreviated terms and acronyms are given in IEC TS 62351-2.

ASN.1	Abstract Syntax Notation One
DER	Distributed Energy Resource
DTLS	Datagram Transport Layer Security
DPI	Deep Packet Inspection
GIS	Geographical Information System
HMI	Human Machine Interface
ICS	Industrial Control System
IED	Intelligent Electronic Device

[1] Under preparation. Stage at the time of publication: IEC TS/PCC 62351-14:2021.

KDC	Key Distribution Center
MIB	Management Information Base
MMS	Manufacturing Message Specification
NSM	Network and System Management
NTS	Network Time Security
OID	Object IDentifier
PCI	Protocol Control Information
PLC	Programmable Logic Controller
PDU	Protocol Data Unit
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
TLS	Transport Layer Security
TSM	Transport Security Model
UML	Unified Modelling Language
USM	User-based Security Model

5 Information collection, filtering and processing

5.1 IT/OT elements

Converging IT/OT networks in a power grid include a wide range of components that allow the connection of systems together and communication in a local or wide area network. A brief overview of the elements is:

- IEDs, PLCs and RTUs – equipment connected with field sensors and actuators and able to coordinate with other elements through Ethernet and other means. These elements use protocols like IEC 60870-5-104/101 or IEEE 1815-2012 (protected with IEC 62351-3, IEC 62351-5), IEC 61850-8-1 and IEC 61850-8-2 (protected with IEC 62351-4), IEC 61850-8-1 and IEC 61850-9-2 (protected with IEC 62351-6), and other proprietary protocols for configuration and diagnostics.
- Substation controllers – are used within Substation Automation Systems to implement and automate controls, communication and monitoring. Also, these elements can use a variety of protocols like the ones mentioned above for IEDs, PLCs and RTUs.
- Gateways – implemented either as a software function or hardware, allow to connect elements in the network at application level, allowing a finer-grained segregation and/or a change of communication protocol.
- HMIs – equipment dedicated for human interaction, often purpose-built computers with touchscreens and software able to interact with the IEDs, PLCs and RTUs to understand the status of the system or change it using the protocols listed above.
- Computers and servers – more classical IT equipment with software able to interact with IEDs and similar devices. Many different kinds of protocols are used by these equipments, that can include standard protocols to interact with IEDs, PLCs and RTUs but also other standard and proprietary protocols to interact with other parts of the system.
- Switches, routers and firewalls – networking gear used to interconnect end systems together in an efficient and secure manner. These equipments support and can interact with a wide range of protocols like SSH, SNMP, Syslog, etc.

- VPN tunnels – generally composed of several sub-elements, can be implemented as software functions of other network elements like firewalls. They play an important role in IT/OT networks as they allow to interconnect different systems in a secure manner. From the other side, they are a critical part of the system as they may allow access to otherwise segregated networks.

Moreover, the way these components are provisioned and maintained is evolving. Virtualization for example has become a well-accepted tool also in OT systems to provide a reliable and flexible virtual version of most of the components above. Cloud computing on the other side is an established IT way to deploy services and systems and is becoming an emerging IT/OT integration technical mean that needs to be considered for the purposes of this document.

5.2 Network and system monitoring tools

5.2.1 SNMP monitoring agents

IEDs and also networking equipment implement SNMP mechanisms that are available today and will arrive/are arriving (IEC 62351-7) – SNMPv2c (most common) SNMPv1 (less common), SNMPv3 (more advanced and closer to IEC 62351-7).

It is interesting to note that network equipment come with both standard and vendor-specific MIBs that are well supported and accepted in the industry and provide a common set of information about generic health status of devices. In addition to these, the monitoring objects defined in IEC 62351-7 allow OT-specific information to be collected, thus allowing better control of the health and operational status of IEDs and similar devices.

The key takeaway is that SNMP is well-accepted and broadly implemented. It's important to remember that there are many MIBs, many versions and there is a need for some smart SNMP Manager able to support different versions and configurations (e.g. v2c, v3 with USM or TSM, etc) to normalize data and hide complexities (backward compatibility).

5.2.2 IDS/IPS probes

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are aimed at monitoring network communication packets and detecting any packet that is somehow foreign in a particular network. In such a case, the IDS will send an alert to a SIEM, leading the operators to execute appropriate actions following the intrusion detection and the identification of the vulnerability that is being exploited.

The substantial difference between IDS and IPS is that the first are aimed only to detect possible events informing other systems of the occurrence while IPS will also provide a possible direct reaction agains the detected threat (i.e. dropping a malicious connection). The choice between IDS and IPS should be dictated by either the need of a complete assurance of not affecting operation (IDS) or the desire to have some form of inline protection (IPS), at the cost of introducing delays due tue the fact that the packet need to pass its control logic and lack of complete control over network operation as detection techniques are subject to false positives.

Even if classical IDS/IPS systems are physical entities collecting traffic from switch/bridge/router mirror ports, the IDS/IPS function is often available in some other network devices (i.e. firewall or routers) or end systems as well.

The less disruptive passive observation techniques (i.e. requiring no modifications to the system, communication stack, or application) require only the addition of dedicated network-based IDS devices without any modification to the existing equipment, thus making these security upgrades easier and less expensive to implement. For this reason, passive IDSs are the preferred approach when considering systems and equipment which are already installed in a much consolidated way.

IDS and IPS work using a "signature-based attack detection" approach through a pattern or behavioural recognition logic. This approach does not require accessing the semantics of traffic payload but IDS/IPS are able to detect the most of already known network attacks. These probes need of course a constant signature update process in order to keep the best possible detection capabilities. Anomaly-based approaches on the contrary permit to detect even unknown attacks after a learning phase, by highlighting baseline deviations – this approach allows the prevention of new attacks to be unnoticed but need further analysis by the user to understand how the deviation may affect the monitored systems. Modern IDS/IPS probes often combine both approaches.

To be effective in power grid systems, IDS probes need to be aware of the OT-specific devices, protocols and architectures in order to be able to detect the different kinds of threats. Another important effectiveness piece comes from the possibility to cope with encrypted communications and be able to identify issues encrypted traffic. In regards of IEC 62351-secured system (meaning the health of the end-to-end secure system), IEC TR 62351-90-2 contains an overview of how to apply DPI to IEC 62351-secured communications.

5.2.3 Network and system management central platforms

The NSM Operation center collects events and health status data from the devices through agents deployed inside the device itself and collecting information from IDS probes located in strategic positions on the telecommunication network.

Please note that the management data are collected from both ICS (OT systems) and corporate networks (IT systems). This approach is aimed at providing a stronger correlation between events arising from different perspectives.

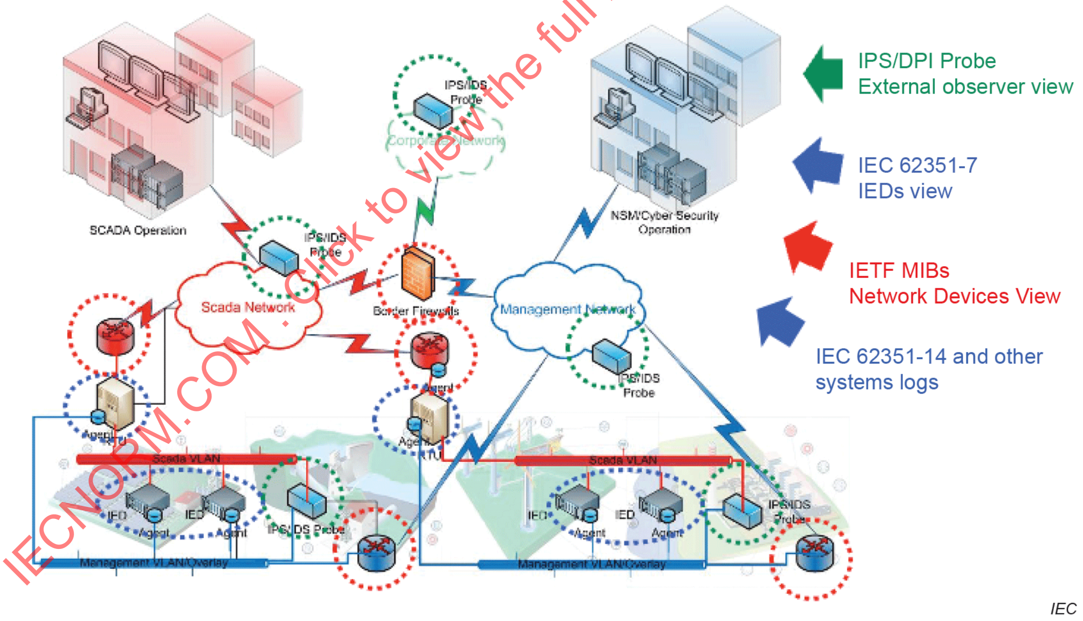

Figure 1 – NSM/Cybersecurity overall architecture

The left-hand side of Figure 1 depicts the OT operation perspective, in terms of SCADA systems and field devices, accessed with dedicated OT protocols.

The right-hand side depicts the Network and System Monitoring/Cyber Security operation center that is in charge of the collection of events and information from both IT and OT environments.

Multiple information sources points are required and available:

- Endpoint devices (IEDs) health and Data Objects and events, providing information and events through IEC 62351-7 MIBs and in some cases also IETF MIBs
- Intermediate systems (RTUs, Network devices like routers and switches) Data Objects and events, providing information and events through IEC 62351-7 MIBs, and IETF MIBs
- Network status information on packet flows, service classes, performance and congestion information, typically derived from switches, bridges and routers
- Deep Packet Inspection new generation probes and IPS/IDS probes providing information through passive traffic analisys.

Each device will provide also its own collected logs (e.g. collected through syslog messages).

The different purpose of SNMP information/events collection and log records collection should be noted and understood.

SNMP MIBs provide information on the current health and security state of the device, using "objects" that represent meaningful state variables (e.g. CPU usage, Memory usage, Anomalous packet reception number, failed authentication count). SNMP information can be queried whenever it's needed to catch the specific situation of a system.

Log records are meant to collect the history of the system events in an ordered way with the aim to provide both the diagnostic but also the (forensic) proof of "what happened". Log records are locally stored and then sent to a central collection system (entirely or filtered).

Some events can be tracked both with SNMP notifications and log records, but the target usage is very different.

5.3 Log management tools

5.3.1 Log collection architecture

A typical log collection and management architecture (Figure 2) has some log collection nodes, and some form of log analysis/storage nodes. The former are nodes that receive (or get, depending on the protocol and system type) logs from endpoints and the latter are nodes able to store and analyze the logs. Sometimes there are additional node types in the architecture where the analysis part can be split (storage vs display vs analysis) but staying at high level the necessary pieces are there.

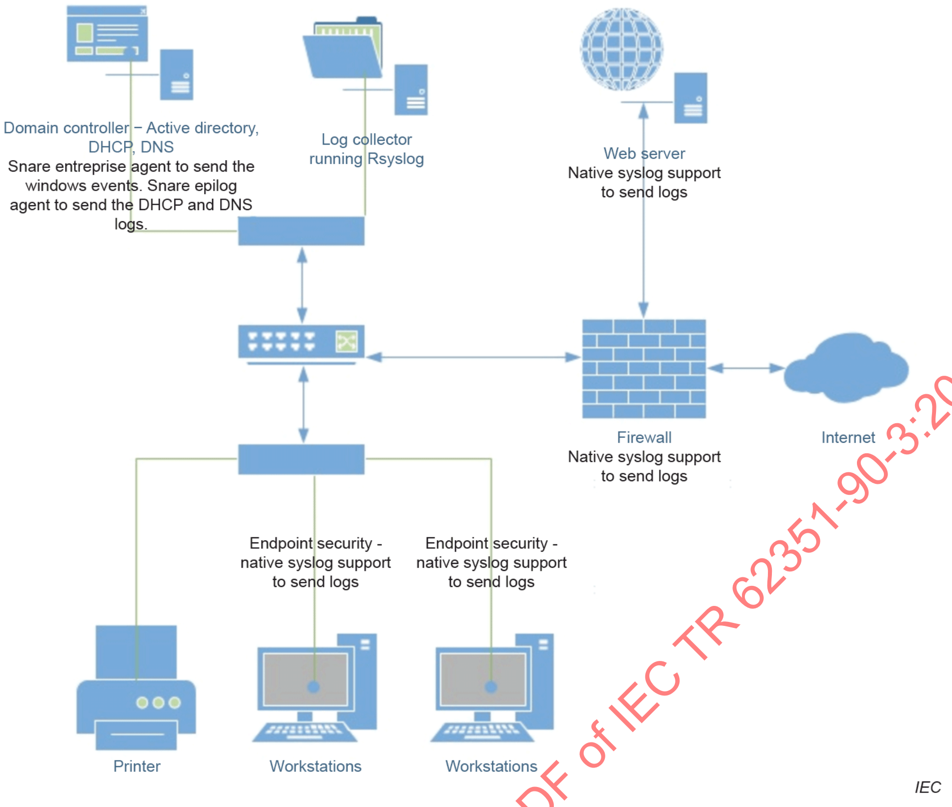
Domain controller – Active directory, DHCP, DNS
Snare entreprise agent to send the windows events. Snare epilog agent to send the DHCP and DNS logs.
Log collector running Rsyslog
Web server
Native syslog support to send logs
Firewall
Native syslog support to send logs
Internet
Endpoint security - native syslog support to send logs
Endpoint security - native syslog support to send logs
Printer
Workstations
Workstations
IEC

Figure 2 – A logging infrastructure

(Source: SANS, Creating a Logging infrastructure, 2017)

A key feature of the logging architecture is to make sure that the log event is captured and stored in its raw format, and that some kind of signature/hashing technique is used to make sure that the logs are not tampered through their lifecycle.

An important aspect that needs to be considered when implementing and maintaining a logging infrastructure is the time synchronization between all the involved parties (that can be achieved in several accurate and secure ways, like NTP/NTS, PTP v2.1, etc) and when the system is geographically spread into large territories. In addition, a clear choice of how to cope with timezones is important.

5.3.2 Log agents

As mentioned in 5.1 there are a variety of different kinds of nodes in a power grid information system that need to be monitored and that can produce various kinds of logs.

The most common form is to not have an agent on the system but to send out logs via Syslog. With syslog, nodes can send out logs to collectors in a somewhat standard format, but as will be seen in 5.3.3 some form of normalization is needed to really be able to use the information contained in the Syslog payloads. Devices supporting Syslog are typically Unix-derivatives and networking equipment.

A variation of the above is the possibility to send out the logs with an agreed semantic, that can help in the subsequent normalization phase (see 5.3.3). The historically most common format is the Common Event Format, but other similar alternatives exist.

The second most common form is to have some kind of agent for Windows machines able to collect the Windows Event Log. As Windows is a very commonly used operating system also in power grids, these events play a significant role. Windows Event Log contains an interesting amount of system and security logs that can be used to monitor health and security aspects of such machines.

Of course, logging solutions existing on the market allow the collection of logs for basically any existing device, and thus other kind of less-common agents or log format exist to reach the goal. The underlying idea and concept are always the same, though.

Log sources can be very different and coming from different kinds of systems. Each system may produce logs about itself or about its observed systems (like an IDS/IPS). A well-known concept in log management is the possibility to assign a credibility level to its source, that can be either automatically or manually and is related to the level of trust that the operator can have and confidence of the device itself -- a measure that the device can express on certain decisions. It can depend on how good the system is known to behave or based on the fact that such logs are coming from a device with built-in security or using a secure protocol to transfer the logs.

5.3.3 Log normalization

While collecting logs is important, allowing machines to interpret them is even more important at scale. The first step towards that is to make sure that uniform information is extracted from the logs no matter of the log agent or log format that was used in the specific case.

There are mainly two approaches to this step; one is to make sure that the log is sent by the log agent already in a structured form where each field already has well-specified semantics and the other is to perform this step after-the-fact inside of the log infrastructure. This second approach requires to have specific parsers for the various log payloads. Often a hybrid approach is used, with some equipment able to send out logs already in a normalized manner and others being normalized afterwards.

5.3.4 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) are products able to focus on the security aspects and semantics coming from the logs and other sources and enact the users to perform security investigations and store such activities for later user. They also allow live dashboards that can be used in Security Operation Centers (SOC) – operating structures that are responsible to monitor the security health of an IT/OT infrastructure.

Very often the need for a Log management infrastructure is driven by the need to deploy a SIEM solution, which is why sometimes the SIEM word is used to represent a system that has the logging infrastructure as one of its parts. In other words, SIEM may be used to describe a logging infrastructure used for cyber-security purposes. Even though historically SIEMs have born in the Log management area, current SIEMs go beyond the Log management features, allowing to integrate other sources (like for example those coming from NSMs) to create broader correlation.

Being part of a convergent IT/OT system it is important that the SIEM is able to have OT-specific extensions and functionalities, to let it leverage the OT-specific information coming from the IEC 62351-7 and IEC 62351-14 series. With such additional extensions, it is possible to leverage the OT-specific semantics that these standards are able to capture.

5.4 Other relevant data sources

In addition to NSMs and Log infrastructures, other interesting data do exist in a power grid that can be used to monitor the global health status from a cyber resilience perspective. Environmental information, weather data and forecast, physical security information – all input makes sense for an analysis to have a clearer picture and prevent false positives as well.

Bad weather conditions may be coupled with anomalous grid operation, while a physical security incident may be correlated with a social engineering action to infect the plant. All the data are interesting to be recorded for further analysis and for sure can also be used to automatically correlate these data with a holistic view.

6 Information correlation and presentation

6.1 Information selection and collection profiles

6.1.1 General

The goal of this clause is to provide some guidance in selecting and filtering the data to be collected, stored and analyzed. At scale, having too much information with a too grained time resolution may hurt the system performance, while at the other end not having good enough time resolution and detail may create issues reconstructing complex events.

6.1.2 NSM and 62351-7

An overall NSM implementation needs to think about all the different equipment available in the system no matter of the information that they can provide or the standard they support to provide such information. The goal of this clause is to expand on details specific to IEC 62351-7 but before going into details it is important to remember that not all the equipment may already support the standard, and consequently other standards / protocols need to be used to collect the information. A notable example of such equipment can be computers with the Windows operating system – that if left unpatched or without an antivirus software can become a critical attack vector.

Another universal NSM aspect is the frequency of data acquisition. While it is important to have updated information, it may not be for all the objects and from the other side having too much data collected can lead to an overload of the storage systems used to archive the collected data points. An interesting aspect that comes into play to significantly increase efficiency is the use of an event-based approach (SNMP notifications) instead of polling. The latter has to be managed in a proper way because while the poll-based approach does not give any doubt about the health of the monitored system and consumes more bandwidth, the event-based approach only uses the bandwidth when some change occurs but may give uncertainty of freshness. A hybrid approach is recommended to benefit from the best of the two approaches.

IEC 62351-7 compliant devices may implement different sets of agents depending on the communication protocols they support. In addition, they may implement only a subset of the standard objects contained in each MIB as all the objects are optional and is left to the vendors to choose which to implement. Some rationale about how to collect such data will now be detailed.

- IED agent – is the agent responsible to provide information about the IED as a device and gives information about its health status. Notable objects:
  - iEDAtkCnt(Ts) – provides a high-level indication of the amount of cyber attacks detected. This object requires the implementing device to have advanced attack-detection capabilities but provides a readily consumable information to be tracked over time.
  - iEDLastEvent(Ts) – combined with the previous object, it permits retrieval of the last event, that can be an attack.
  - iEDConfigurationCRC(Ts) and iEDConfigurationVersion(Ts) provide the CRC and version of the running configuration.
  - iEDFirmwareVersion(Ts) provide the version and timestamp of upload of the current device firmware. Combined with the configuration objects above these are very critical objects when it come to track down change of behavior of the device.

  - iEDWatchdog(Ts) provide a way to understand the number of times that the system watchdog has intervened. It is an interesting object since malicious modifications to the code running on the IED can affect for instance its capability to respect the real time execution constraints.
  - iEDCpuUsage(Ts) allow the monitoring of CPU usage of the IED. Combined with the object above allows to track and detect behavior changes that can be due to an update in the software or the configuration.
  - *iEDMemUsage(Ts)* allow the monitoring of Memory usage of the IED. Combined with the object above allows to track and detect behavior changes that can be due to an update in the software or the configuration.
  - *iEDExpCerts(Ts)* and *iEDNearToExpCerts(Ts)* permit knowledge of whether the device has, if any, expired certificates or if any certificate is about to expire soon.
  - *iEDPhyHealth*(Ts) permit knowing if the device has hardware and software in good health conditions, and can be used to spot a wide range of issues in the IED itself.
- Environment agent – provides information about the environment where the IED is located, its external chassis and power supply. Notable objects:
  - envAppDatSt(Ts) – permits knowledge of whether the status of the environment and the power supply is in good conditions.
  - envLastEvent(Ts) – provides the last environmental event.
  - envPSPled(Ts) – indicates that direct access to the IED is in progress. This event should be monitored carefully as direct access allow to perform disruptive actions while leaving less trace into the system (e.g. network traffic).
  - envPSPPanel(Ts) – Indicates that front-panel access is in progress.
  - envPSUPOn(Ts) – permits understanding of the health status of the power supply; useful especially in redundant power supply configurations.
- Interfaces agent – provides information about the interfaces of the IED, including non-ethernet ones (serial, USB, etc). It provides several objects to understand all the interfaces in the system, and which ones are active, online or faulty.
- Clock agent – Provides information about the clock synchronization system inside the IED. Notable objects:
  - cLKclockTamperDetected(Ts) – permits knowledge of the last event of clock tampering, if any.
  - cLKLastClockHoldover(Ts) – permits knowledge of the last event of clock holdover, if any.
- IEEE 1815 DNP and IEC 60870-5-104 agents – provides information specific to master and slave connections for these protocols. Notable objects:
  - tCLastEvent(Ts) – permits knowledge of the last event happened regarding this family of communication protocols. Can be about security or health events.
  - tCMasterTable – provides a table of connections from master to the current IED. While this object contains a lot of information and may not be suited for frequent update, it is very helpful to understand which are the actors interacting with the device and the status of the communications with such actors.
  - tCOutstationTable – provides a table of connections to outstations. Just like the masters table, it permits a clear picture of the actors interacting with the IED.
  - tCAuthFailCnt(Ts) – provides a counter of failed authentications. Can be useful to detect unauthorized tenatives of access.
  - tCSessKeyFailCnt(Ts) – provides a counter of failed session key negotiations.
  - tCUpKeyFailCnt(Ts) – provides a counter of failed update key negotiations.
  - tCDecryptFailCnt(Ts) – provides a counter of PDUs that were not decrypted due to some error. It may reveal issues in the communication or an attacker trying to inject packets.
  - tCInErrCnt(Ts) – provides a counter of PDUs that were in error state.

- IEC 61850 ACSI agent – provides overall IEC 61850 communications information. Notable objects:
  - aCSILastEvent(Ts) – permits knowledge of the last event happened regarding this family of communication protocols. Can be about security or health events.
  - aCSIAcsCtlFail(Ts) – provides the number of access control failures detected (i.e., when a data object that the client wanted to access exists in the server, but based on the access view of the association with that client, an access to the data object was refused).
- IEC 61850 GSE agent – provides Generic Substation Events information. Notable objects:
  - gSEDecryptFailCnt(Ts) – provides the number of PDUs received that could not be decrypted. It may reveal issues in the communication or an attacker trying to inject packets.
  - gSEInErrCnt(Ts) – provides the number of PDUs received that were in error due to malformed content, parity errors or configuration mismatch.
  - gSEKDCAuthFailCnt(Ts) and gSEKDCSessionKeyFailCnt(Ts) – provide a counter of authentication to KDC failures and session key establishment failures between peer and KDC.
  - gSESIPMessageIntegrityFailCnt(Ts) – provides the number of PDUs that were not using the proper Group Key.
  - gSESL2MessageIntegrityFailCnt (Ts) – provides the number of PDUs that were not using the proper Group Key.
- IEC 61850 Sampled Value agent – provides information for Sampled Value protocol communications. Notable objects:
  - sVDecryptFailCnt(Ts) – provides the number of PDUs received that could not be decrypted. It may reveal issues in the communication or an attacker trying to inject packets.
  - sVKDCAuthFailCnt(Ts) and sVKDCSessionKeyFailCnt(Ts) – provide a counter of authentication to KDC failures and session key establishment failures between peer and KDC.
  - sVSIPMessageIntegrityFailCnt(Ts) – provides the number of PDUs that were not using the proper Group Key.
  - sVSL2MessageIntegrityFailCnt(Ts) – provides the number of PDUs that were not using the proper Group Key.
- IEC 61850 MMS agent – provides information about IEC 61850 communications happening using the MMS protocol. Notable objects:
  - mMSILastEvent(Ts) – permits knowledge of the last event happened regarding this family of communication protocols. Can be about security or health events.
  - mMSAuthFail(Ts) – provides the number of authentication failures.
  - mMSConnFailInCnt(Ts) – provides the number of incoming connections that have been refused.
  - mMSConnFailOutCnt(Ts) – provides the number of outgoing connections that have been refused.
  - mMSDecryptFailCnt(Ts) – provides the number of PDUs received that could not be decrypted. It may reveal issues in the communication or an attacker trying to inject packets.
  - mMSAProfileDecryptFailCnt(Ts) – number PDUs received that could not be decrypted within A-Profile session.
  - mMSTProfileDecryptFailCnt(Ts) – number PDUs received that could not be decrypted within T-Profile session.
  - mMSUpKeyFailCnt(Ts) – number of update key negotiations that failed.
  - mMSSessKeyFailCnt(Ts) – Number of session key negotiations that failed.

- mMSErrorRxCnt(Ts) and mMSErrorTxCnt(Ts) – number of errors that have been received and transmitted.
- mMSMMSTable – provides a table of client connections to the peer. While this OBJECT contains a lot of information and may not be suited for frequent update, it is very helpful to understand which are the actors interacting with the device and the status of the communications with such actors.
- mMSERptReceptionDelay(Ts) – the time required to receive the last Report. This time is the difference between the reception time and the emission timestamp stored inside the report. It is inteteresting to monitor as some attacks may impact the responsiveness of the device.

A practical approach to monitor all the available objects is to make sure that all the most critical (for example, the notable ones mentioned above) are monitored frequently (at least every 15 minutes) with a poll-based approach, while the others are monitored less frequently (at least once a day) and on-demand in case of need. Events (notifications) can be used in both cases to have fresh information as soon as something happens.

6.1.3 NSM and 61850-specific monitoring

The NSM plays an important role into the continuous, detailed, and holistic monitoring of a networked system.

Within the digital substation standardized by IEC 61850, specific guidelines have been documented in IEC TR 61850-90-4 to properly set up and monitor the IEC 61850-compliant networked equipment of a substation. In that document, mappings have been provided between the IEC 61850 data model and standard SNMP OBJECTs in order to provide visibility across all available equipment – with an operational and troubleshooting point of view.

IEC 61850 Information exposed to SNMP is about asset information and health (logical nodes LLN0 and LPHD, for information like vendor, firmware version, physical health status, etc.), and more specifically IEC TR 61850-90-4 recommends the mapping of several communication details of bridges with SNMP, for example:

LPCP – Physical Communication Ports: permit knowledge of the physical status of ports (up/down), and amount of transferred bytes

LBRI – Bridge logical node: permit knowing bridge topology information

LBSP – Port Spanning Tree Protocol: permit inspection of the spanning tree internal

LCCH – Communication Channel: permit inspection of the HSR/PRP redundancy status of interfaces

All these aspects permit to monitor the health status of bridges and help to detect malfunctions and possible unauthorized changes in the network layout.

6.1.4 NSM with other SNMP objects

To obtain maximum visibility and detail, it is recommended to monitor all the possible relevant OBJECTs that the the different equipment have implemented, as in practice there will be a mixture of choices in the field and sticking with a single approach may not lead to proper visibility.

With this in mind, in this subclause some industry standard MIBs and relevant OBJECTs will be described, to give a high-level idea of the information that can be monitored with (mainly) networking equipment that is not implementing any IEC standard.

- SNMPv2-MIB

This MIB contains a wide range of information that has been introduced and standardized with the version 2 of the protocol.

- sysName – this OBJECT usually contains the hostname of the system, if it has been set.
- sysDescr – contains a decription of the system and it's commonly used by vendors to describe the asset and provide additional information like the firmware version (example from a switch: STRING: Siemens, SIMATIC NET, SCALANCE XF208, 6GK5 208-0BA00-2AF2, HW: Version 4, FW: Version V05.02.02, SVPK9138691)
- sysLocation – this OBJECT may contain a text description of where the system is located.
- sysUptime – this OBJECT reports the uptime of the system. Although a simple metric, can be interesting to monitor to spot malfunctioning or unexpected reboots of the system.
- authenticationFailure – this OBJECT is used for a trap notifying about an authentication failure to the SNMP system itself. It can be useful to monitor unauthorized access to the monitoring system itself.

– HOST-RESOURCES-MIB

This MIB describe various kind of resources of a system, including installed software and all related information.

- hrSystemUptime – this OBJECT is basically a duplicate of SNMPv2-MIB::sysUptime and show how important is to try to support all the possible implementations as different equipment may choose to implement different standards.
- hrSystemDate – permits knowledge of the system date. Useful to monitor and understand the time settings of the system, can be useful to detects attacks or malfunctions of the device clock.
- hrSystemInitialLoadDevice – permits knowledge of the boot/OS peripheral of the system. Monitoring this property can be useful to spot unexpected change in the software (e.g. rogue OS installed on the system).
- hrSWInstalled – this OBJECT lists software installed in the system. Useful to track any change in the kind and version of software, that may be due to maintenance / ugrades or other unauthorized / malicious events.

– IF-MIB

This MIB describes network interfaces and their operational status. Implemented by network equipment like switches and routers, permits to monitor the physical and logical status of the network.

- ifOperStatus – this OBJECT is instantiated one per interface and allows to know the status of of the link (up/down) and to understand if a physical disruption or malfunctioning is in progress for the interface.
- ipNetToMediaPhysAddress – allows understanding of the physical address (Ethernet MAC address) that has been recognized for an IP address. Basically, permits seeing the ARP table of the device and can be useful to detect man-in-the-middle attacks.

6.1.5 Logs

In the log management world, there are two extremely different ways to collect logs and get information out of it.

The first approach requires carefully selecting which equipment should send the logs and figure out which are the events that need to be sent (for example, we may be interested only in security-related events like authentication, or we may focus on events with a certain level of importance).

The second approach is to just get all the possible logs from all the possible equipment that can produce logs.

While the former approach enables bootstrapping of the infrastructure with a lower footprint and permits to have a better control of what each equipment can and cannot produce, it may leave out some less relevant information that can be useful at a later stage for forensic analysis. From the other side, collecting all the possible logs from all the possible devices can require a substantial amount of resource and requires in any case some form of analysis and post-filtering of the logs to identify the useful information.

Choosing between the two approaches should be based on the available resources, knowledge of the involved systems, number of logs produced every day, etc. – and the approaches can be mixed when it makes sense, for instance critical systems may be subject to a full collection while less critical systems may be subject to a filtered-upfront approach.

6.2 Events, incidents and correlations

No matter if data is coming from the NSM or from Logs or other sources, low-level information creates an event. Temperature can change on the CPU of an RTU and be detected through the NSM, and we can receive a log about a user failing to log-in because of a wrong password – both are Events. However, the first may raise an Incident (or Alarm) if the temperature is too high for a long time, and the second can raise an Incident as well if too many Events of that kind occur in a limited time frame.

The idea is that the overall monitoring platform will store and analyze an interesting amount of data, but ideally it will need to produce a minimal number of Incidents about real problem to be understood and resolved.

Incidents are often generated from correlations, that take into account multiple types of events that may be not interesting if observed in isolation but can become an evidence when observed as part of a wider context.

6.3 Security metrics (KPI)

Once the SIEM is setup and operation with all the relevant data sources connected to it, it is possible to establish Key Performance Indicators (KPI) to monitor the evolution of the security posture over time.

Three main groups of KPIs can be created, to monitor and drive three different aspects of the security monitoring infrastructure:

- KPIs about the monitored system: these KPIs are about the system being monitored and help to syntetize its security posture. They are subject to change when the security posture is improved or weakened. Examples:
  - Number of assets with incidents, in absolute and relative form (amount of assets with incidents vs. total number of assets)
  - Number of Incidents in the last 24h, week, month – this number can help to understand the amount of security problems in the infrastructure and how they evolve over time. It may offer a different angle with respect to the previous KPI, because a problematic Asset with frequent and recurring Incidents will be more visible here.
- KPIs about the monitoring system itself: these KPIs are closer to the technology used and its configuration and are useful to understand if the current mixture of settings and software is good or not. Examples:
  - Number of false positives, in absolute and relative form – this KPI is helpful to understand the amount of overhead that the underlying technology and configuration is creating, since false positives need to be analyzed and understood by analysts to determine that they are such. Moreover, they tend to decrease the confidence in the system and to create a bias when an Incident is generated. This KPI can be used to track improvement of software, configurations and ruleset over time.

  - Ratio of unused logs – the quantity of logs that is not considered by correlation logics or taken in considerations during. This KPI can be useful to understand if the current log filtering setup is good or not.
- KPIs about the team managing the system: these KPIs are useful to capture the perfomance of the team managing the SIEM, or better to see if the current team is big enough to manage the amount of Assets and Incidents. Examples:
  - Mean time to respond to security Incident: this can be split into finer grained time to respond KPIs (first reply, close of the incident, etc) and is a high level simple KPI that tracked over time can help to understand if the team need to be expanded.
  - Number of open incidents related to your critical assets (Devices, systems, applications and users): this is another way to understand the pressure of the team, and how it affects the monitored infrastructure.

6.4 Risk Management platforms

Risk Management is about understanding the Risk that comes from a given infrastructure and providing a way to accept, manage or decrease it. In the NIST SP800-37 publication, a guidance on key steps for a Risk Management Framework are provided (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor).

Risk Management platforms allow the management of the complete lifecycle of Risk Management Framework steps and tasks and are often implemented alongside Log management infrastructure and SIEMs. The reason for that is because Risk Management Frameworks ultimately require the implementation of a set of controls on Assets and Users, and the data needed to implement such controls is already gathered for security monitoring purposes or if not gathered, is very close to what is already collected.

A very simple example of a control and how the monitoring infrastructure allows verification of its compliance is about the generic risk of malware infection and the subsequent control: all applicable Assets where the technology requires or allows an antivirus software must have it and it should be updated. Such information can be retrieved by the NSM infrastructure and used as starting point to generate Assets compliance reports for Risk Management.

7 Monitoring use cases

7.1 General

The purpose of this clause is to provide an overview of the monitoring use cases and how their peculiarities may change the monitoring strategy due to different amount of assets, bandwidth and priorities.

7.2 Substation

In the Substation use case, there are dozens of assets that cooperate to implement the digital protection and control functionalities. Such assets are mainly computers and IEDs, mainly in the form of protection relays and substation controllers. The substation is usually connected north to a control center that can see its status and in case send down manual commands. With this amount of assets, it can make sense to have local IDS/IPS probes, local NSM agents and log forwarder in order to monitor the substation locally and forward up all or part of the data to central collection systems. A challenge is given by the available bandwidth up to the control center, that can be limited and available with high priority for operational communications (it is advisable that some form of QoS is put in place to guarantee separation, however the media used to connect the substation at some point will have a bandwidth limit). A local monitoring console can be useful to give to local staff a view into the health of the system, but still keeping the need to forward all meaningful information to a central monitoring system.

7.3 DER systems

DER systems can be very distributed, with each local site having as low as one asset to a few, and consequently they give an interesting challenge to monitoring for many reasons: costs, bandwidth. On the other side, a DER system can be made up of hundreds or thousands of distributed assets, even though distributed. In this situation each monitoring technique needs to be properly filtered and tuned in order to make sure that all the critical information is gathered or can be received in a central monitoring system. In addition, sometimes DER systems are not connected all the times, but they do regularly connect to central systems to synchronize all the data and receive commands.

Another challenge found in DER systems is that it can span across different domains, for instance the utility and a third party (e.g. private house with solar panel). This scenario adds more challenges from a security and monitoring perspective since likely there will be restricted remote interaction possibilities.

7.4 Large Hydro

In a Large Hydro environment, a multitude of Hydro generation plants, dams and ancillary systems are interconnected to manage the power that can be obtained and store thanks to water. All these parts are geographically distributed and may hold from a few to dozens of assets each and may have a variety of networking between them – from high to very low bandwidth. All these hydro systems are then connected up to a control center for operation.

Key points of attention of the use case are limited bandwidth (and thus, filtering and prioritization can play a big role), and overall number of assets.

7.5 Generation

The generation Use case is very much like the substation one: there is usually a big local LAN with dozens of assets, that at some point are connected to a control center for remote control. As for the substation case, it can make sense to provide a local view of the monitoring system to local operators, while synchronizing all relevant information to a central monitoring site.

8 Monitoring profiles for attack scenarios

8.1 General

We are considering some attack scenarios, and for each one we can describe how each monitoring piece comes into play and how it can be configured to maximize efficacy and efficiency.

8.2 Scenario: Malicious IED program change

A malicious user is able to reprogram an IED to perform malicious activity and hide it to the operators.

A malicious user has prepared a malware able to change the program of an IED in order to disrupt operation in a subtle way. The rootkit is able to modify the current ladder logic of the running program and change it in a subtle way (for instance, alterate the reaction times to safety events). To perform this, he infects a Windows computer by means of an USB stick with the malware and runs it. The malware downloads the ladder logic from the IED and changes it, and then uploads it again to the IED.

- Cybersecurity logs from the Windows computer highlights that an USB removable media has been inserted and one executable has been taken from it. In the log entry, the computer is identified by its IP address and hostname.