Syslog in IEC 62351 Compliant Systems: Maximizing Effect & Expanding Utilization in OT

Nicolas Trezza¹, Georgios Michail Makrakis², and Dakota Roberson¹

¹Department of Electrical & Computer Engineering, University of Idaho
²Department of Computer Science, University of Idaho

June 07, 2024

Abstract
This article explores how syslog contributes to IEC 62351 compliance, particularly in incident response scenarios. Additionally, it outlines the extended benefits of incorporating syslog into OT environments, beyond the confines of the IEC 62351 standard.
The numerous components resident in Operational Technology (OT) networks provide an ever-growing allure for different types of attackers. Recent trends show that ransomware has grown to be one of the most common and effective methods from which threat actors can derive a profit, with correspondingly minimal effort [1], [2]. Furthermore, nation-state funded actors may embed themselves in critical infrastructure networks and stay dormant while waiting for an opportune time to enact a larger planned mission. Along with the critical nature and the economic impact that intrusions in such networks might have, these concerns serve as justification for asset owners to continue improving their cyber defenses.

Simultaneously, corporate executives seeking growth may harness new technologies by integrating IT with existing OT to streamline operations and reduce costs, particularly in digital operations, i.e., integration of IT with existing OT. Many times four of the six Purdue Enterprise Reference Architecture levels are entirely dependent on IT components running commodity operating systems and applications. Therefore, problems generated by the once IT-specific systems can intentionally or unintentionally influence the services of their OT counterparts. More burden is placed on the teams responsible for securing this transition, as they must ensure the integrity of productivity or profitability of business operations.

As the cybersecurity posture of organizations can affect those operations, one of the primary teams which ensure that these issues are addressed promptly and effectively is the Security Operations Center (SOC). This team performs identification, triage, and remediation of incidents. At the same time, it makes sure that the actions taken both before and after such events comply with an organization’s policies and industry standards. However, compliance with standards in real-world operational environments (such as substation automation systems or Distributed Energy Resources (DERs) management systems) is oftentimes open to interpretation by the personnel implementing these features or controls. For example, the security measures established according to IEC 62351, require a thorough study of the IEC 61850 family of standards [3], Role-Based Access Control (RBAC), encryption, security architecture, and more. Having all that, there are a plethora of tools that can be utilized to ensure the security of both hosts and their communication paths in the environment without generating undue work for integrators or operators.

Providing technological capabilities that are widely accepted and successfully deployed in various domains can be beneficial in multiple ways. This can assist in a smoother transition to a more secure system while also complying with the requirements of known and newly developing standards and/or frameworks. A capability worth noting is the syslog protocol [4], which formalizes the process to dispatch logs of varying priority and context from local instances to servers and analyzed by security tools such as Security Information and Event Management (SIEM) systems. The security goal of applying this protocol is to collect events from the network and endpoint landscape to a centralized location. This showcases potential issues as they arise.
without requiring analysts to remotely collect or view their correlated logs. Additionally, varying data sources can corroborate a kill chain of events that lead to cyber-physical disruption.

IEC 62351-8 guides the usage of RBAC in power management control systems. The main benefit of establishing RBAC gives security practitioners a favorable view as to who is attempting access to what, when, and where across many digital assets in both IT and OT networks. From this point, the employment of syslog for the logging and consumption of this information has the ability to identify and address anomalous and potentially illicit activity on networks using statistical or other forms of analysis. This proactive approach to basic security principles complies with the IEC 62351 requirements but also enriches security posture in OT networks without any additional involvement of control system personnel.

Contributions. We provide a conceptual model for syslog integration in control system environments that can provide visibility to all the aspects of RBAC. Furthermore, we elaborate on the attainment of RBAC requirements pertaining to the IEC 62351 standard via syslog, and we define where syslog collection can enhance other aspects of security monitoring. This is a first-of-its-kind discussion about the reinforcement of RBAC via syslog in OT environments. We ultimately delineate the advantages of syslog’s incorporation in control system domains that do not include any form of IEC 62351 compliance.

Syslog and RBAC

To better understand the nature of syslog, as well the implementation of RBAC as specified in IEC 62351, an overview of both is needed.

Syslog

Syslog is commonly used to transmit various information (logs) about a system to a server via network transport using a standard client-server architecture. The server is commonly referred to as a syslog server and provides security and administration personnel with a centralized location to observe and analyze the behavior of their networked systems. Most syslog-based tools come in the format of a command line or GUI application, and a software library to send the collected logs to the syslog server. One distinct feature of syslog is the use of tiered severity levels, such as EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, and DEBUG.

It must be noted that the incorporation of severity levels is not mandated per syslog’s specification, but if utilized, this capability can provide instant context or indicators of importance to analysts. Regarding both IT and OT, two examples services that can provide events based on the application of syslog in such networks include the following:

Firewall Audit Log. As firewalls are the most common way to create secure network perimeters defined by various standards such as NERC CIP and IEC 62443, logging and aggregating such activity can provide paramount insight into attackers’ actions. Syslog can assist the tasks of SOC personnel by transmitting information such as that related to the number of rules matched, and to the deny/drop of suspicious connections.

Host Audit/Event Logs. Operating systems produce several logs for actions such as user authentication, remote access, and command line actions. The majority of them are designed for debugging and troubleshooting purposes and not for security evaluation. However, such logs can assist in the investigation of security incidents if they are analyzed accordingly by security personnel. A syslog server can contain audit and event logs, and create notifications about emerging issues in near-real-time. Recently, OT-specific hosts have begun incorporating native syslog capabilities [5], [6].

Other services and devices that can be utilized include HTTP and Active Directory servers, engineering hosts, and Human Machine Interfaces (HMIs). An example of such logs’ information flow production and digestion, can be found in Figure 1.

FIGURE 1. Example of logs production and consumption in a typical OT environment.

Role-Based Access Control in IEC 62351

The IEC 62351 standard has been created to address the cybersecurity issues of different IEC power system
communication standards, such as those found in IEC 61850, among many others. This family of standards consists of 14 parts which have evolved incrementally since the year 2000. Recently, IEC 62351 parts 3 and 4 have been revised, and parts 7, 9, and 12-14 were added. The standard covers cybersecurity topics such as encryption and authentication for TCP/IP and 61850-based protocols, RBAC, cryptographic key management, and XML security. A comprehensive analysis of the different parts of IEC 62351 can be found in literature [7].

Of particular interest to this conversation are the RBAC guidelines, of Part 8. RBAC is a security methodology based on managing user access to protect resources including data, applications, and systems from improper actions such as access, modification, addition, or deletion. Specifically, in an RBAC-enabled infrastructure, users are not given individual rights, properties, or parameters in a per-user case. Instead, users and permissions are assigned within the infrastructure along with one or more role assignments [8], [9]. Roles can be assigned to groups or individual users and provide them with all the necessary access and permissions to achieve their tasks.

A real-world analog is easily visualized in the academic environment. Custodians are allowed access to all rooms within their purview and to tools like mops, carts, and brooms. However, they are blocked from access to zones not in their cleaning assignment and items such as lecture notes and student grades. Meanwhile, professors would have full access to their classroom, chalk, notes, and student grades, but not allowed access to mops, brooms, and locker rooms.

Table 1 presents the roles as well as some permissions assigned per role for a common OT environment as defined in IEC 62351-8. Permissions are binary (allowed, not allowed) in a per-use-case fashion. For example, user Security Administrator (SECADM) includes most of the permissions with the exception of Reporting and FileWrite. On the other end, the Viewer role has nearly no permissions, aside from View and Reporting. This roles’ assignment can be implemented in an OT infrastructure, with the support of existing tools, for example, Active Directory servers.

Syslog Use Cases in IEC 62351

As has been previously mentioned, syslog events are typically categorized by severity. Each severity type has the ability to classify events based on its parameters and qualification. We present some illustrative examples of how the previously mentioned data types can be used to create syslog events based on the controls outlined in IEC 62351:

- **Emergency Logs.**
  - Authentication service failure.
  - Authentication service records have been modified.

- **Alert.**
  - Unknown user authentication (or Login/Logout).
  - User without command privileges attempted action (RBAC mismatch).

- **Critical.**
  - User session timed out: logout enforcement failure.
  - Unknown file certificate/signature.

- **Error.**
  - User authentication failure.
  - Incorrect role request from user authentication.

- **Warning.**
  - User session timing out: logout will be enforced.
  - Incorrect signature for authentication.

- **Information.**
  - User authentication success.
  - New user credential.

While the above list is not exhaustive, many cases can be conjured up where these events would take place. Operators and engineers might not, to a great extent, capitalize on the value of the information that is contained in such events, although their deep knowledge of the physical system, in combination with the appropriate analysis from cybersecurity personnel, can provide better situational awareness in the case of security incidents.

Based on these elements, we outline the following scenarios where syslog and IEC 62351 compliant systems may be utilized during incident response events. Those scenarios aim to include cases where the accurate and precise collection of logs can assist the process of cybersecurity analysis but also to offer others where a more thorough approach to such collection is needed.

![Attacker tactics and produced logs for Scenario 1.](image-url)
TABLE 1. An IEC 62351-based mapping of roles and mandatory pre-defined rights (adapted from [3]).

<table>
<thead>
<tr>
<th>Value</th>
<th>Role/Rights</th>
<th>VIEW</th>
<th>READ</th>
<th>DATASET</th>
<th>REPORTING</th>
<th>FILEREAD</th>
<th>FILEWRITE</th>
<th>FILEMNGT</th>
<th>CONTROL</th>
<th>CONFIG</th>
<th>SETTING GROUP</th>
<th>SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0&gt;</td>
<td>VIEWER</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;1&gt;</td>
<td>OPERATOR</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;2&gt;</td>
<td>ENGINEER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;3&gt;</td>
<td>INSTALLER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;4&gt;</td>
<td>SECADM</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;5&gt;</td>
<td>SECAUD</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;6&gt;</td>
<td>RBACMNT</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;7...32767&gt;</td>
<td>RESERVED</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;32767...1&gt;</td>
<td>PRIVATE</td>
<td></td>
<td></td>
<td></td>
<td>For future use.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Scenario 1
The SOC team of ACME Energy LLC received several alerts via syslog on Saturday morning in their security analysis dashboard titled “Plant Z Security Overview”. These alerts were the following: “User Remote Desktop Protocol (RDP) Authentication During Off Hours”, “Guest User Multiple Authentication Attempts”, and “User Without Access Privileges Attempted Authentication”. The first two alerts source from Windows machines used as “jump hosts” which are the exclusive access points for Plant Z. The third one was generated from an IEC 62351 compliant machine in the plant yard. Noticing the unusual behavior, the SOC teams contacted process and plant operators to ask if there has been any changes to normal operations. The operations team stated that their processes were running as intended and no significant fluctuations have been observed in the last 24 hours.

The security team investigated the timeline of the events they received to discover that an unknown remote user was hijacking a wireless network without authentication at the corporate office. A “Guest” account was utilized to navigate through network segments and successfully access the “jump host” remotely. The “Guest” account had no password authentication, and there was no Explicit Allow List on the RDP application of the “jump host”. As a last step, the actor then authenticated into account “Temp”, with the role Installer, by using guessed credentials after accessing an HMI. The attacker attempted but failed to close a breaker. The attacker’s steps and tactics in the above scenario along with the corresponding syslog data that assist in the incident’s investigation are depicted in Figure 2.

Lessons Learned:
› Enabled logging for authentication attempts in all accounts enhanced the tracing of events.
› Logging of actions that include individual privileges in process network, rapidly pinpointed the performed activities.
› The problematic points in the security posture were identified with the centralized collection of logs.
› Logs can help determine both operational and security events.

FIGURE 3. Attacker tactics and produced logs for Scenario 2. The threat is still unknown and an insider (employee) misconfiguration is assumed.
Scenario 2

ABC Energy Inc. did retrofit a backup substation feeding an industrial zone (food, textile, and steel manufacturing) with RBAC-designed user profiles and enabled syslog on most devices of Purdue Level 2 and higher. The company envisioned validating the feasibility of installing security controls at the plant level without hampering the physical process. This new security architecture was going to be enabled utilizing a hypervisor system that would host substation control systems. This would also allow for ease of backup, redundancy, and testing new infrastructure with the new hypervisor capabilities.

System operations and cybersecurity teams came to an agreement, where the latter would enable the security controls on devices such as HMIs and historians, while the former would be in charge of creating accounts and designating roles per account. Afterward, the cybersecurity personnel would review accounts to ensure the “least privilege” practice was followed and operations would ensure that all systems are functional.

However, due to an security incident shortly after the initial substation hypervisor installation, the cybersecurity team was too short-staffed to manually issue user account updates to the backup substation Virtual Machine (VM). About a year later during peak demand hours from a manufacturing plant, (primary) Substation-A became overloaded, requiring fail-over to the (backup) Substation-B. This fail-over is unsuccessful, and during the investigation of this incident, it comes to light that the backup control system VM had been modified to trip breakers continuously via a local malicious script. There were no reported logs of operators accessing this machine to generate such activity.

In an attempt to identify which user had last modified the secondary VM control system, the cybersecurity team reviewed syslog events from the substation to pinpoint user activity. They assumed that the user responsible would have had the role of Installer or Engineer assigned to their account. They observed that every event in syslog had a local user field of “User”. When checking local user configuration, “User” had Security Admin and Engineer roles applied. The cybersecurity personnel assumed that as operators were performing accounts setup and testing, it was simpler to have one local account for all personnel to use with maximized privileges to reduce extra steps. The security team discovered that a threat actor had gained access to the OT enclave through a vulnerability in the unpatched hypervisor infrastructure. Next, they uncovered the local “User” account and utilized it to manipulate the backup control system machine. Without capability to enact any change on the RBAC controlled primary control system, the threat actor settled for installing a living-off-the-land type script in the system they had access to easily rendered the control system ineffective when needed. Figure 3 presents the attacker’s potential steps and the incident’s investigation logs.

Lessons Learned:

› Improper roles assignment can be discovered in logs.
› Investigation of the 1:1 relationship of roles to account can be performed with precise logging.
› Modern IT solutions are more patch compulsory and present new conveniences paired with new maintenance requirements.
› Role Based Access Control should be supported in backup and testing environments.
› Domain and procedures understanding is required in the determination of which actions should be logged.

Syslog in ICS Networks Beyond IEC 62351

The benefits and challenges noted necessitate refinement. Standards such as NERC CIP, IEC 62351, and IEC 62443 establish criteria for technologies like syslog in operational settings, encouraging asset owners' deeper adoption. Syslog’s versatility allows its application to various components within OT networks, given the abundance of devices capable of generating logs.

As mentioned previously, locally installing a syslog server in OT environments enables log forwarding to enterprise security tools. Additional benefits include staying ahead of future security requirements, such as those from NERC, and alleviating constraints on OT personnel with cybersecurity expertise. Asset owners can benefit from syslog deployment irrespective of compliance mandates, utilizing solutions based on regulatory frameworks or standards as reference. Integration of syslog in OT environments eases the burden on personnel lacking cyber threat awareness or mitigation skills, bridging the gap until adequate training is provided [10].

Observing events via syslog is crucial for both system admin and security monitoring. However, responsible personnel must discern critical information and devise action plans. Deviating from security standard guidelines may hinder the effective outcomes. Not all utilities have the capability to fully implement standards due to resource constraints [11], highlighting
syslog deployment’s role in enhancing security posture despite limitations. Syslog tools offer scalability and customization to meet asset owners’ specific needs and capabilities.

Conclusions
Since cybersecurity is becoming increasingly important in OT environments, we suggest that syslog can enhance the practical application of IEC 62351. With the use of illustrative scenarios, we demonstrated the granular level of detail of events which can be acquired via syslog in the cases of cybersecurity incidents. Furthermore, we defined where syslog collection can complement other aspects of security monitoring, even in cases where there is no formal IEC 62351 compliance. We hope that this work will assist both new and experienced practitioners and researchers in OT cybersecurity.

REFERENCES

Nicolas “Nick” Trezza is Master of Electrical and Computer Engineering Graduate at University of Idaho Contact him at trez9772@vandals.uidaho.edu.

Georgios Michail Makrakis is a Ph.D. student in Computer Science at University of Idaho. Contact him at gmakrakis@uidaho.edu.

Dakota Roberson is associate professor of Electrical and Computer Engineering at the University of Idaho with a joint appointment at the Idaho National Laboratory. Contact him at dakotar@uidaho.edu.