PROJECT
ENG
PRO

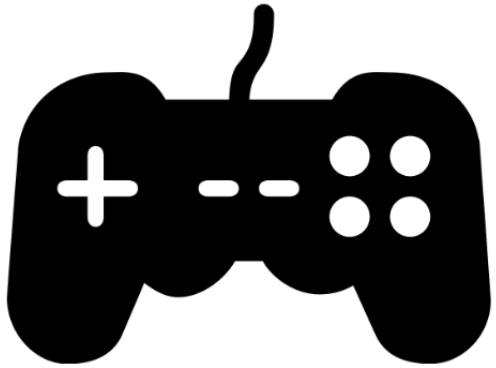
CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

FR 2 – Use Control

- FR1 – Identification, authentication and access control
- FR2 – Use Control
- FR3 – System Integrity
- FR4 – Data Confidentiality
- FR5 – Restrict Data Flow
- FR6 – Timely response to event
- FR7 – Resource Availability

FR 2 – Use Control



In essence, use control pertains to the control system's ability to generate security-related audit records for all categories shown on screen in order to ensure comprehensive monitoring and accountability.

- Access Control
- Request Errors
- Operating system event
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Access Control

Access control tracks user or software resource access (workstations, controllers, etc.). Detailed audit records are essential for monitoring, accountability, and analysis.

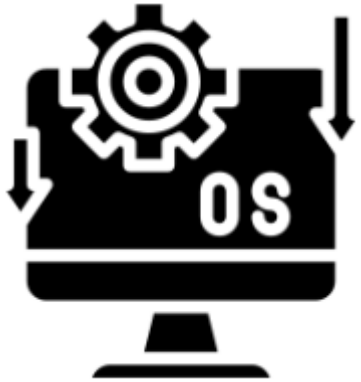
- **Access Control**
- Request Errors
- Operating system event
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Request Errors

The "request error" category pertains to instances where users attempt actions like retrieving backups. Errors such as rejected requests due to credential mismatches or corrupted files should be logged.

- Access Control
- **Request Errors**
- Operating system event
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Operating System Events



Operating System Events. These are pivotal for control system workstations. Logging activities like user access, data transfers, and system changes is essential. Audit records are vital for security and anomaly detection.

- Access Control
- Request Errors
- **Operating system events**
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Control System Events

Control system events involve application software in systems like DCS, SIS, and SCADA. Audit logs track user interactions, program changes, and errors, aiding in accountability and process integrity.

- Access Control
- Request Errors
- Operating system events
- **Control system events**
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Back Up and Restore Events

In the realm of "backup and disturbance events," maintaining audit logs is paramount for data backup, restoration, and configuration changes.

- Access Control
- Request Errors
- Operating system events
- Control system events
- **Backup and restore events**
- Configuration changes
- Potential Reconnaissance activity
- Audit Logs

Configuration Changes

Robust configuration management, along with a permit system, is crucial for maintaining system stability, security, and transparency in authorized changes.

- Access Control
- Request Errors
- Operating system events
- Control system events
- Backup and restore events
- **Configuration changes**
- Potential Reconnaissance activity
- Audit Logs

Reconnaissance Activity

To counter reconnaissance activities in industrial control systems, organizations should deploy effective detection tools for identifying both digital and physical probing.

- Access Control
- Request Errors
- Operating system events
- Control system events
- Backup and restore events
- Configuration changes
- **Potential Reconnaissance activity**
- Audit Logs

Audit Logs

In essence, use control pertains to the control system's ability to generate security-related audit records for all categories shown on screen in order to ensure comprehensive monitoring and accountability.

- Access Control
- Request Errors
- Operating system events
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- **Audit Logs**

Audit Logs

In essence, use control pertains to the control system's ability to generate security-related audit records for all categories shown on screen in order to ensure comprehensive monitoring and accountability.

- Access Control
- Request Errors
- Operating system events
- Control system events
- Backup and restore events
- Configuration changes
- Potential Reconnaissance activity
- **Audit Logs**

Wrap Up