Introduction to SCADA for Operators

Supervisory Control and Data Acquisition

MONITOR

CONTROL

ALARM

ANALYZE

RELIABILITY
Ensure system reliability and safety.

AWARENESS
Improve situational awareness.

RESPONSE
Respond effectively to system events.

OPERATIONAL EXCELLENCE. | SAFE SYSTEMS. RELIABLE OPERATIONS.

VERSION 1.0

Purpose

This training guide introduces operators to the fundamentals of SCADA systems used in grid and utility operations. It explains how SCADA supports monitoring, control, and response activities in real-time operational environments.

Target Audience

- New grid operators
- Control room personnel
- Operations trainees
- Field technicians transitioning to SCADA operations

Supervisory Control and Data Acquisition (SCADA)
It is a system used to monitor and control industrial and utility processes in real time.

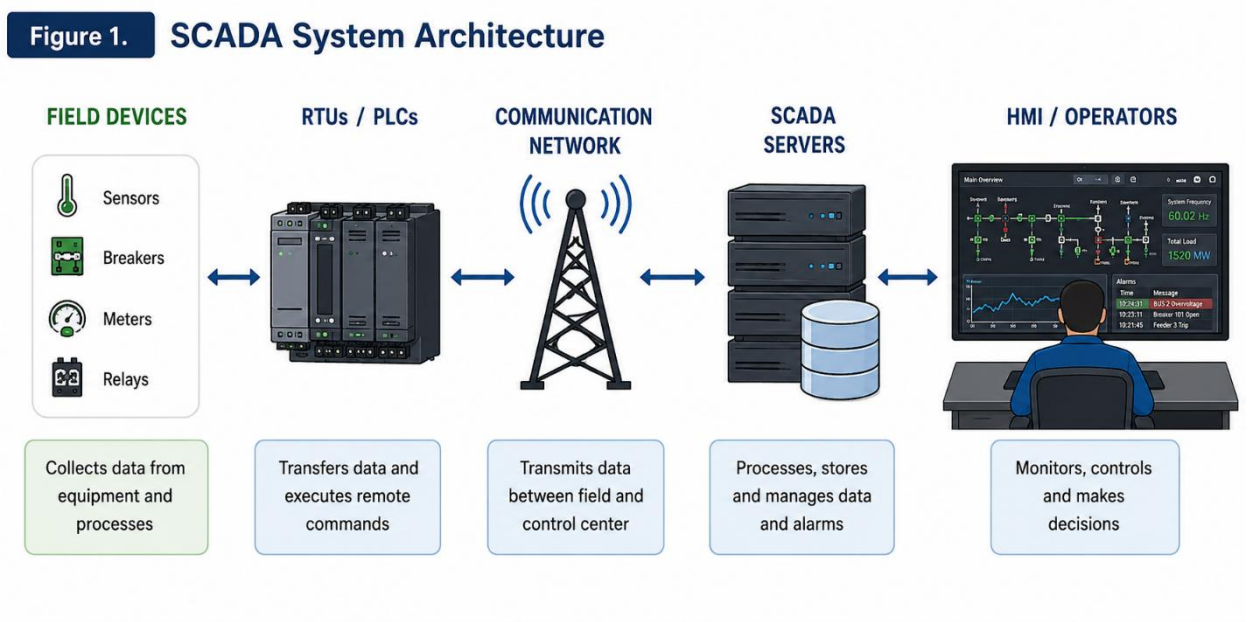
SCADA systems collect data from remote equipment and allow operators to:

- Monitor system conditions
- Respond to alarms
- Control equipment remotely
- Record operational events
- Improve grid reliability and efficiency

Why SCADA is Important?

SCADA supports critical operations by helping operators:

Function	Purpose
Real-Time Monitoring	View live system conditions
Remote Control	Operate equipment from control centers
Alarm Management	Detect abnormal conditions
Data Logging	Store historical operational data
Situational Awareness	Improve decision-making
Outage Management	Support restoration activities



SCADA System Architecture

Figure 1 illustrates the overall architecture of a SCADA (Supervisory Control and Data Acquisition) system and the flow of operational data between field equipment and the control center. The architecture begins with field devices such as sensors, breakers, meters, and relays that collect operational and electrical data from substations and industrial equipment.

The collected data is transmitted to RTUs (Remote Terminal Units) or PLCs (Programmable Logic Controllers), which act as interface devices between the field equipment and the SCADA network. These devices process field signals, execute control commands, and transmit operational information through the communication network.

The communication network enables real-time data exchange between remote sites and the central control center using technologies such as fiber optics, radio communication, or Ethernet networks. The data is then processed and stored by SCADA servers, which manage alarms, historical records, event logs, and system calculations.

Finally, operators interact with the system through the Human-Machine Interface (HMI), where they monitor system conditions, acknowledge alarms, and perform operational control actions.

Figure 2. Typical Control Room

Typical Control Room

Figure 2 presents a typical SCADA control room environment used in utility and industrial operations. The control room contains multiple operator workstations and large display panels that provide real-time visibility of system conditions.

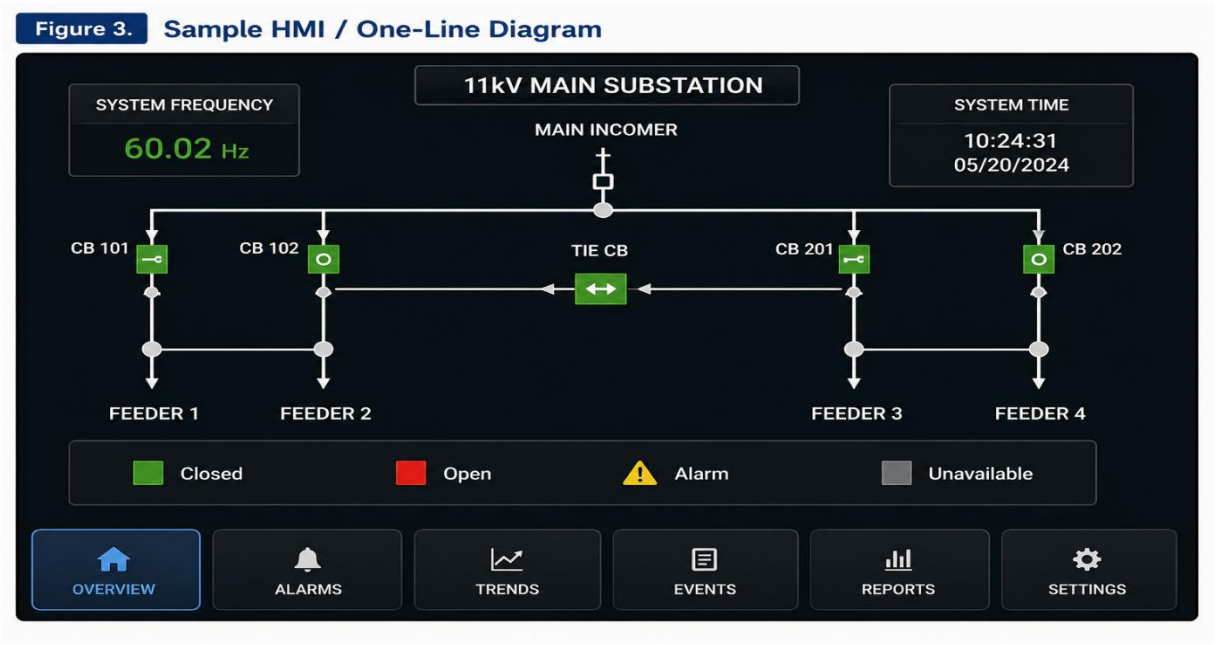
The large display wall shows critical operational information including:

- one-line electrical diagrams,
- power flow status,
- alarm summaries,
- trend graphs,
- system frequency,
- and network topology.

Operators continuously monitor these displays to maintain situational awareness and respond to abnormal conditions. The workstation monitors provide detailed operational interfaces where operators can:

- acknowledge alarms,
- review event logs, perform switching operations,
- and analyze system trends.

The control room serves as the central point for monitoring, coordination, and operational decision-making during normal and emergency conditions.



Sample HMI / One-Line Diagram

Figure 3 shows a sample SCADA Human-Machine Interface (HMI) displaying a one-line electrical diagram for an 11kV substation. A one-line diagram is a simplified representation of the electrical system that displays the relationship between breakers, feeders, buses, and switching devices. The diagram includes:

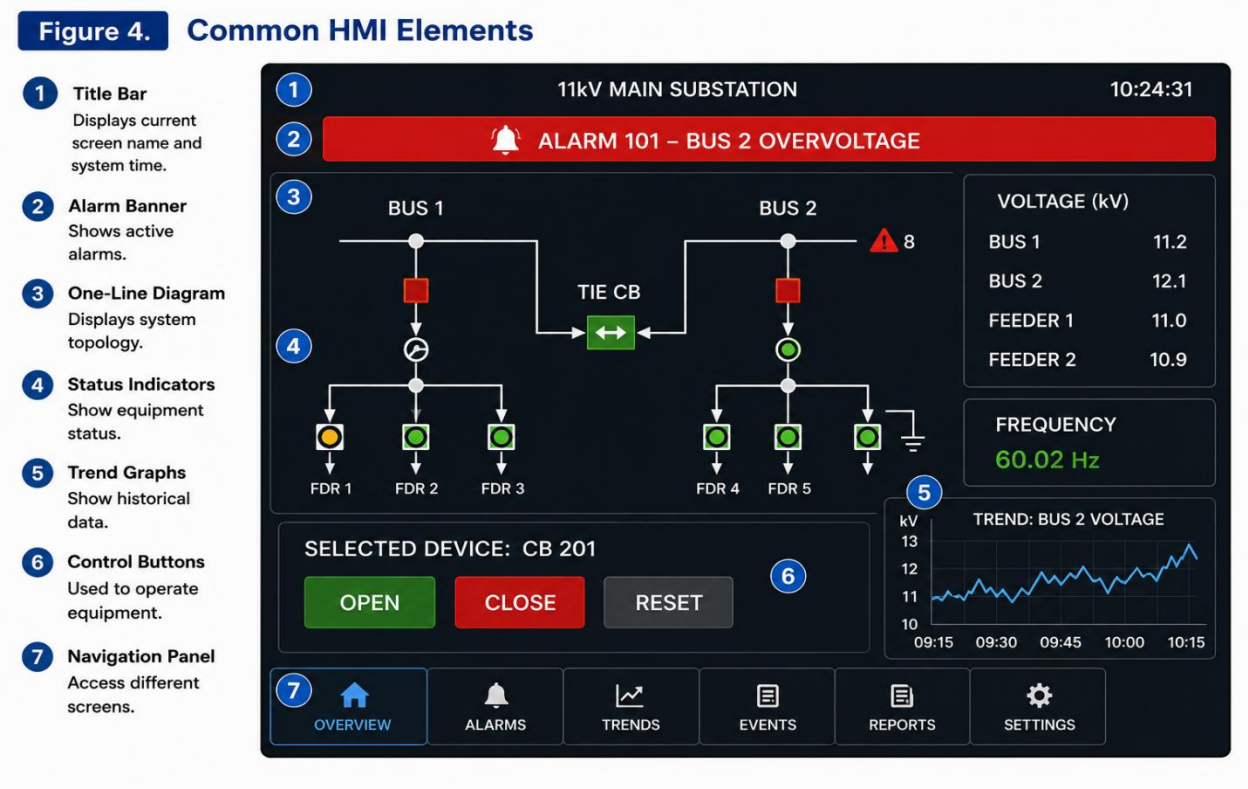
- incoming power supply,
- feeder circuits,
- circuit breakers,
- tie breakers,
- and equipment status indicators.

Color-coded symbols indicate equipment conditions:

- green indicates normal or closed status,
- red indicates open or alarm conditions,
- yellow indicates warning conditions,
- gray indicates unavailable equipment.

The HMI also displays operational parameters such as system frequency, current time, alarm conditions, and navigation controls.

Operators use this interface to monitor equipment status, verify electrical configurations, and perform remote operational control.



Common HMI Elements

Figure 4 identifies the primary components commonly found in SCADA HMI screens. Each element supports operator monitoring and operational control activities.

The title bar identifies the current operating screen and displays system information such as time and location. The alarm banner highlights active alarms requiring operator attention. The one-line diagram provides a graphical overview of the electrical system topology.

Additional interface elements include:

- status indicators for equipment conditions,
- trend graphs showing historical values,
- control buttons used for remote switching operations,
- and navigation panels for accessing different system screens.

These HMI components improve operator situational awareness by presenting operational information in a clear and organized format.

Figure 5. Alarm Priority Levels

Level	Color	Description	Required Action	Response Time	Example
Critical (Level 1)		Critical conditions that require immediate response.	Respond immediately. Notify supervisor.	Immediately (0–2 minutes)	• Bus overvoltage • Transformer trip • System blackout
Major (Level 2)		Major issues that may affect system reliability.	Investigate and take action promptly.	Within 5–15 minutes	• Feeder trip • Loss of communication • High frequency
Minor (Level 3)		Non-critical abnormal conditions.	Monitor and log. Take action if needed.	Within 15–60 minutes	• High temperature warning • Voltage deviation • Breaker mismatch
Advisory (Level 4)		Informational messages or conditions.	No immediate action required.	As needed	• Maintenance due • Parameter change • System message

Note: Response times may vary based on operating procedures and system conditions.

Alarm Priority Levels

Figure 5 categorizes alarm conditions according to severity and required operator response. Alarm prioritization helps operators identify which events require immediate attention and which conditions can be monitored routinely.

The figure defines four alarm categories:

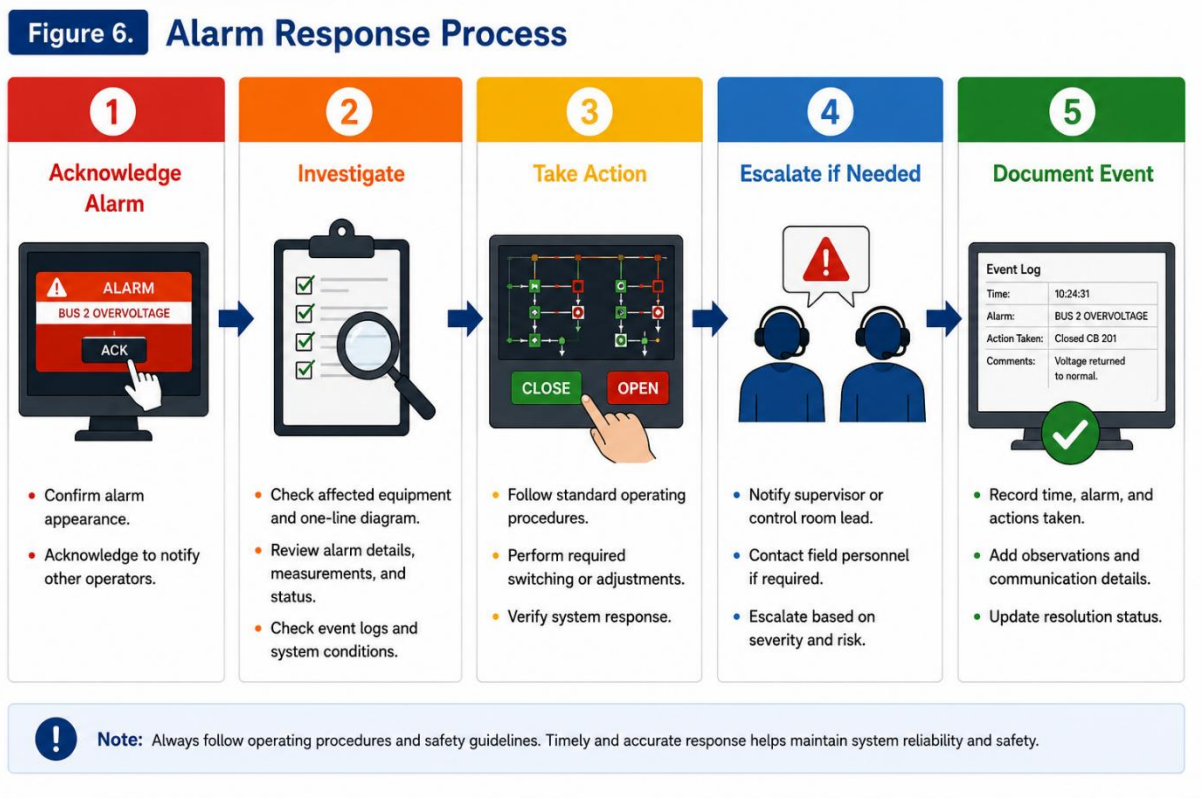
- Critical,
- Major,
- Minor,
- and Advisory.

Critical alarms represent severe conditions that may threaten system reliability or safety and require immediate action. Major alarms indicate significant abnormal conditions that require prompt investigation. Minor alarms identify non-critical issues that should be monitored and logged. Advisory alarms provide informational messages or operational notifications.

The figure also includes:

- response expectations,
- alarm color conventions,
- and example alarm conditions.

Alarm prioritization supports efficient operational response and reduces the risk of overlooking important events.



Alarm Response Process

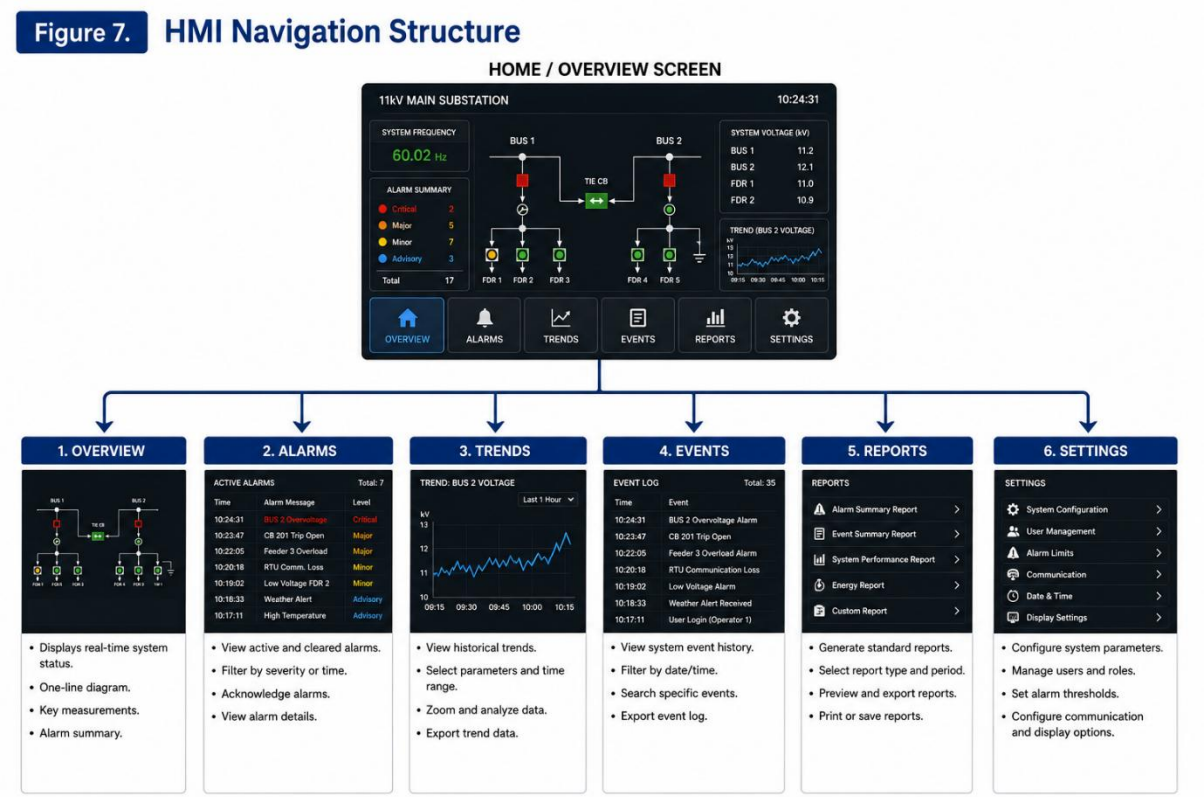
Figure 6 illustrates the standard operator workflow used when responding to alarm conditions. The process begins when an alarm is acknowledged by the operator and continues through investigation, corrective action, escalation, and documentation.

The response process includes:

1. Acknowledge the alarm,
2. Investigate the condition,
3. Perform corrective actions,
4. Escalate when required,
5. Document the event.

During investigation, operators review equipment conditions, event logs, system measurements, and operational status. Corrective actions may include switching operations, coordination with field personnel, or system adjustments.

If the condition cannot be resolved locally, the issue is escalated to supervisors or technical specialists. All operator actions and observations are recorded in the operational log for compliance and historical analysis.



HMI Navigation Structure

Figure 7 demonstrates the navigation structure of a SCADA HMI system. The diagram illustrates how operators access different operational screens from the main overview display.

The overview screen serves as the primary operational dashboard and provides:

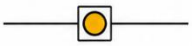
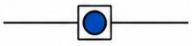
- real-time system visibility,
- alarm summaries,
- system measurements,
- and equipment status.

Operators can navigate to specialized screens including:

- alarm management,
- trend analysis,
- event logs,
- reporting functions,
- and system settings.

The navigation structure improves usability by organizing operational information into dedicated functional areas while maintaining quick access to critical data.

Figure 8. System Status Indicators

Indicator	Color	Status	Description	Example
	Green	Normal	Equipment is operating normally. No action required.	 CB 201 Closed
	Red	Open / Active Alarm	Equipment is open or an alarm condition is active. Immediate action may be required.	 CB 101 Open
	Yellow	Warning	Abnormal condition detected. Monitor the system and take action if necessary.	 FDR 2 Warning
	Gray	Unavailable	Equipment is unavailable, disconnected, or communication lost.	 FDR 3 Unavailable
	Blue	Informational	Informational message or status update. No action required.	 System Message

 **Note:** Indicator behavior may vary based on system configuration and object type.

System Status Indicators

Figure 8 explains the color-coded system status indicators commonly used in SCADA HMIs. Status indicators allow operators to quickly identify equipment conditions and operational states.

The figure defines the following indicator categories:

- Green: Normal operation,
- Red: Open or alarm condition,
- Yellow: Warning condition,
- Gray: Unavailable equipment,
- Blue: Informational status.

Each status includes:

- a graphical symbol,
- operational meaning,
- and an example device condition.

Standardized indicators improve operational consistency and reduce the likelihood of operator misinterpretation during monitoring and response activities.

Figure 9. Alarm Types and Classifications

Alarm Type	Description	Examples	Purpose	Priority Level
1. PROCESS ALARM	Related to electrical parameters and process conditions.	• Overvoltage • Overcurrent • Underfrequency • Transformer Trip	Ensure safe and reliable operation of the system.	Critical (Level 1)
2. EQUIPMENT ALARM	Related to the status of equipment and devices.	• Circuit Breaker Open • Switchgear Fault • Relay Malfunction • Communication Loss	Monitor equipment health and availability.	Major (Level 2)
3. SYSTEM ALARM	Related to system performance and operational issues.	• High System Frequency • Low System Voltage • Load Shedding • Islanding Detected	Maintain overall system stability and performance.	Minor (Level 3)
4. SECURITY ALARM	Related to security events and access violations.	• Unauthorized Access • Login Failure • Configuration Change • User Lockout	Protect the system from unauthorized access and changes.	Advisory (Level 4)

Note: Alarms are displayed based on priority levels and configured thresholds.
Refer to Figure 5 for Alarm Priority Levels and Figure 6 for Alarm Response Process.

Alarm Types and Classifications

Figure 9 classifies alarms according to their operational purpose and source. Alarm classification helps operators understand the nature of abnormal conditions and determine appropriate response actions.

The figure identifies four alarm categories:

1. Process Alarms,
2. Equipment Alarms,
3. System Alarms,
4. Security Alarms.

Process alarms relate to electrical or operational parameters such as voltage, frequency, or current deviations. Equipment alarms identify failures or abnormal conditions affecting physical devices. System alarms indicate issues affecting overall system performance or reliability. Security alarms identify unauthorized access attempts or configuration changes.

Each category includes: descriptions, operational examples, purpose statements, and associated priority levels.

Alarm classification improves troubleshooting efficiency and operational awareness.

Figure 10. Alarm Priority Levels

Alarm priorities are used to determine the severity of an alarm condition and to ensure appropriate operator response.

Priority Level	Name	Color	Description	Typical Response Time	Example Alarms
Level 1	Critical	Red	Critical conditions that may cause equipment damage, system outage, or safety hazards. Immediate action is required.	Immediate (0–5 minutes)	• Overvoltage • Major Equipment Failure • Fire / Gas Detected
Level 2	Major	Orange	Serious conditions that affect system performance or reliability. Action should be taken as soon as possible.	Prompt (5–30 minutes)	• Undervoltage • Overcurrent / Overload • Communication Loss
Level 3	Minor	Yellow	Non-critical conditions that may lead to a problem if not addressed. Monitor and plan corrective action.	Routine (30 minutes – 4 hours)	• High Temperature • Low System Voltage • Maintenance Due
Level 4	Advisory	Blue	Informational messages or low-risk conditions. No immediate action required.	As Needed (> 4 hours)	• System Message • Configuration Change • User Login

Note: Priority levels can be configured based on site requirements.

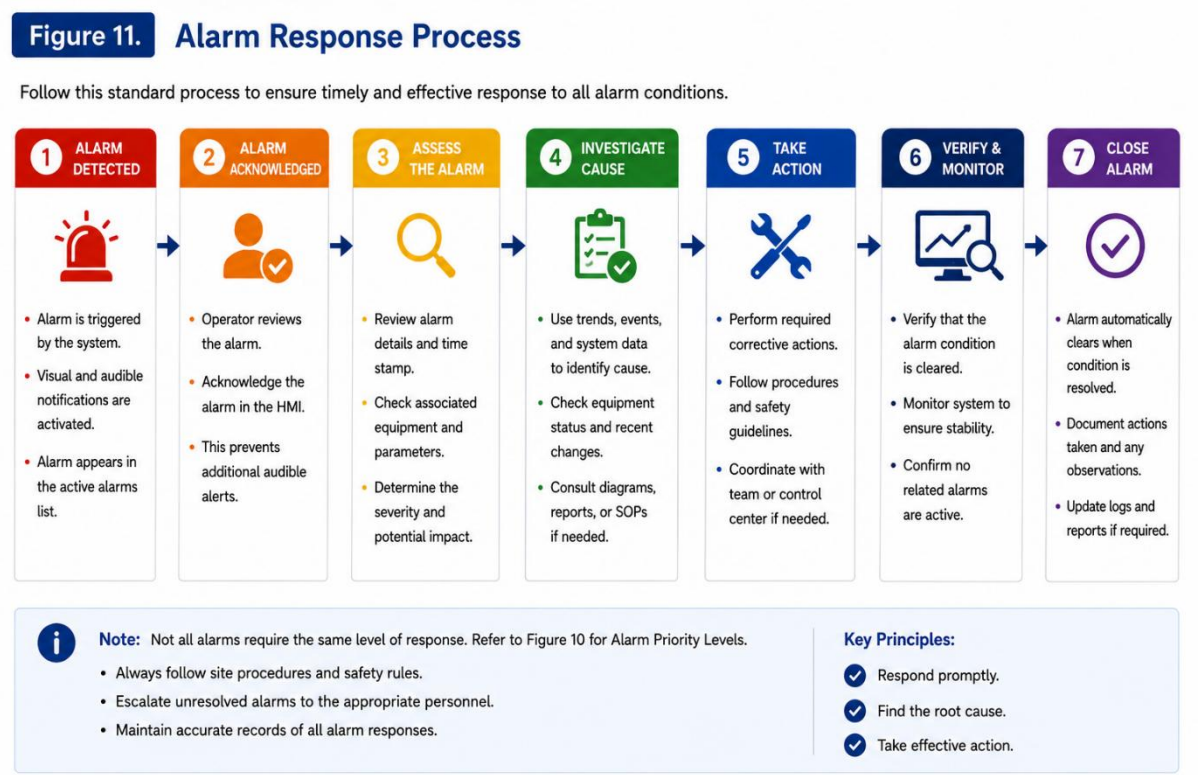
Alarm Priority Levels

Figure 10 provides a detailed overview of alarm priority management and expected operator response times. The figure associates each alarm priority with:

- severity level,
- color coding,
- response urgency,
- and example alarm conditions.

Level 1 alarms represent critical conditions requiring immediate response to prevent equipment damage or service interruption. Level 2 alarms indicate serious operational conditions requiring prompt investigation. Level 3 alarms represent routine abnormal conditions that should be monitored. Level 4 alarms provide informational notifications with minimal operational impact.

This prioritization structure supports effective alarm management and ensures operational resources are focused on the highest-risk conditions.



Alarm Response Process

Figure 11 presents an expanded alarm response workflow showing the complete lifecycle of alarm handling activities. The process begins when an alarm is detected and continues until the alarm is verified, resolved, and closed.

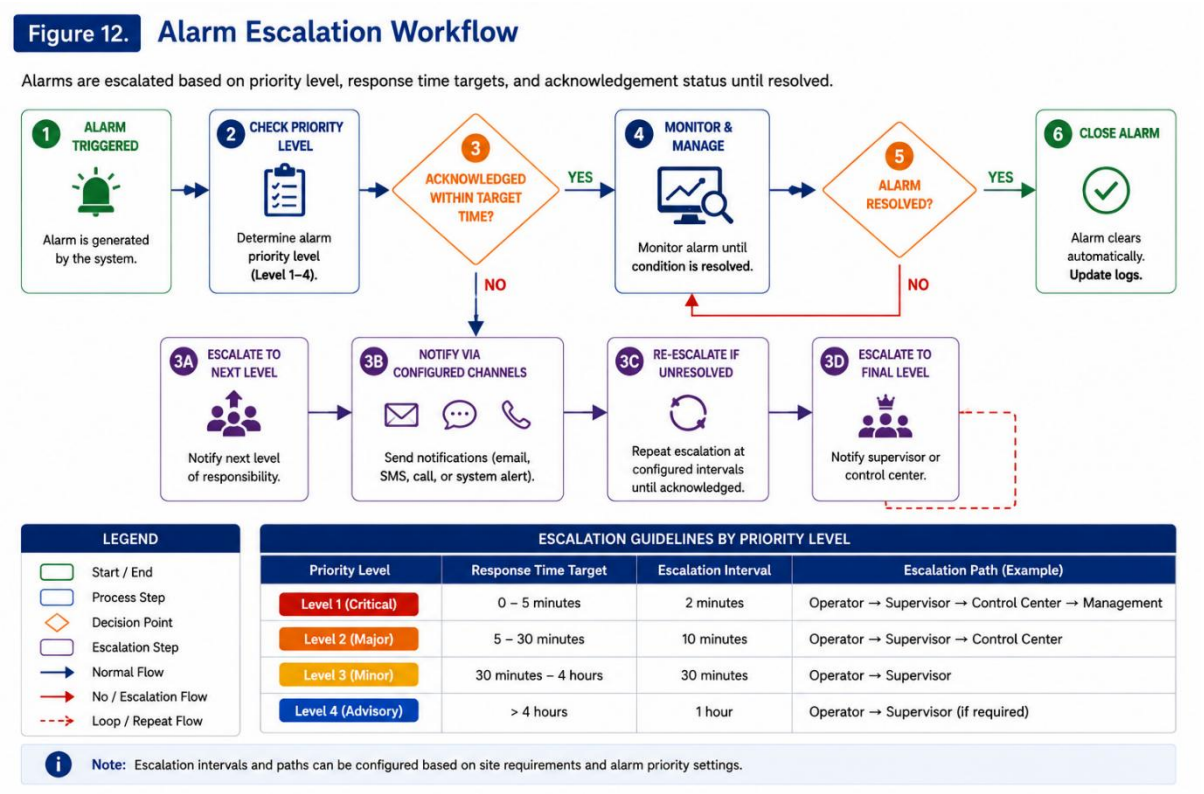
The workflow includes:

- alarm acknowledgement,
- alarm assessment,
- root cause investigation,
- corrective action,
- monitoring,
- and final closure.

The figure also emphasizes operational best practices such as:

- following site procedures,
- maintaining accurate records,
- escalating unresolved conditions,
- and verifying system stability after corrective actions.

The workflow ensures alarm conditions are handled consistently, safely, and in compliance with operational procedures.



Alarm Escalation Workflow

Figure 12 illustrates the escalation workflow used when alarm conditions are not acknowledged or resolved within established response time targets. Escalation procedures ensure critical conditions receive appropriate management attention.

The workflow includes:

- alarm detection,
- priority evaluation,
- acknowledgement monitoring,
- escalation notification,
- re-escalation procedures,
- and alarm closure.

Decision points determine whether escalation is required based on:

- alarm priority,
- acknowledgement status,
- and response timing.

The figure also includes escalation guidelines showing:

- response targets,

- escalation intervals,
- and notification paths for different alarm severity levels.

This process ensures unresolved conditions are communicated to the appropriate operational and management personnel to maintain system reliability and operational safety.