Instrumentation, Control, and Protective Systems for Fired Heaters

API RECOMMENDED PRACTICE 556

July 2010 Ballot Version.

In accordance with API ballot policy only Sections with substantive changes as recommended by the committee are included.

Note: During a 9 month review period of the balloted and approved document multiple editorial comments have been incorporated.

The committee is re-balloting only the sections with substantive changes as included in this document.

1. A modification to sections 3.4 to 3.4.4.1 that alters the technical discussion of these sections is recommended by the committee. Although still focused on the process hazard of unburned fuel within the heater the new language attempts to clarify the technical challenges due to the multiple paths to this hazardous situation. (See pages 2-20)

2. A new section 3.4.7 Pre-Ignition Purge Cycle has been added (see pages 21-22)
New Language for Re-Ballot

3.4 Protective Systems

The purpose of protective systems is to maintain safe operation or to achieve safe state in response to unacceptable process deviations.

Protective actions include:
- Process Control System (a.k.a. Basic Process Control System (BPCS)) Action - control overrides
- Operator Action - operator response to alarms, including emergency response
- SIS Action – startup permissives and interlocks, close safety shutoff valves, open dampers

Protective functions include:
- Input Devices - process measurements (e.g. analytical sensors, analog transmitters, or discrete switches), manual input devices (e.g. hard or soft hand switches/pushbuttons), and status indications (e.g. position transmitters or limit switches).
- Logic Solver - programmable electronic systems, hardwired relays, solid state systems
- Output Devices - solenoid or relay interface to final elements (e.g. safety shutoff valves, combustion air dampers, stack damper, or natural draft dropout doors), and status indicators (e.g. panel lights, or Human Machine Interface (HMI) display graphics)

The diversity in the design of fired heaters requires that each heater be independently evaluated to ensure that each hazard scenario is effectively mitigated. Since each heater may have unique features or operational modes, it is critically important that those responsible for assessing the availability and reliability of a protective function understand all of the possible equipment failure modes and the potential impact to the operating unit and personnel.

The diversity of issues that may impact the protective function requirements include:
- type of process, operating temperature and pressure
- type and size of the heater
- type and number of burners
- type and reliability of the pilots
- turndown requirements
- operating and safety criteria from the burner manufacturer
- variability in fuel gas composition and supply pressure
- fuel supply reliability and filtration requirements
- length and cross sectional area of air ducts (velocity, turbulence, flow conditioning)
- mechanical integrity of air, preheater, and stack dampers
- location of taps for process measurement
- line size and pressure drop in the fuel gas manifold to the burners
- redundancy requirements for availability and reliability
- scheduled outage or turnaround intervals

Additional considerations for protective functions include:
- Operational Modes - Consideration must be given to all equipment modes of operation (e.g. start-up, process change, minimum firing and shutdown operations) to ensure there is adequate protection in all of these modes. Conditions such as sulfiding, hydrogen sweep, decoking, spalling, catalyst regeneration, and switching from forced to natural draft operations are examples of process change operations.
— Independence - It is recommended practice to maintain separation between the control and protective systems. For example, a control device that malfunctions to create an unacceptable process deviation is no longer available to detect or mitigate the process hazard it has created.

— Loss of Utility - When loss of electrical power or instrument air occurs, it is essential the final elements are designed to fail safe. For example, solenoids should be de-energized to trip and the springs in the safety shutoff valves should fail in the direction required to achieve safe state.

— Reliable Power Source – It is recommended that all protective instrumentation be sourced from a reliable power source, e.g. Uninterruptible Power Supply (UPS) per API-554.

— System Reset - Once activated, the SIS should keep the process in the safe state until the unsafe condition is corrected and the SIS is manually reset.

A Protective Instrumented Function (PIF) may be applied to both the process side (tube) and combustion side of heaters. PIFs are implemented to detect hazardous conditions and either achieve or maintain a safe state. When a PIF is implemented to prevent a hazardous event that could result in personnel injury or fatality, the PIF is classified as a Safety Instrumented Function (SIF).

A Safety Instrumented Function (SIF) assigned a Safety Integrity Level (SIL) of 1, 2, 3 or 4 shall comply with the requirements of ANSI/ISA 84.00.01-2004 (IEC-61511 MOD). Although this standard is accepted good engineering practice and is recommended for the protection of personnel and the environment, the work process may be applied to asset protection. While these PIFs may have an assigned Integrity Level (IL) they should be clearly identified as non-safety applications.

### 3.4.1 Response Time Considerations

Each protective function has a maximum permissible time for corrective action to mitigate a hazardous event.

#### 3.4.1.1 Process Safety Time

Process safety time is the interval between the initiating event leading to an unacceptable process deviation and the hazardous event.

#### 3.4.1.2 Process Response Time

Process response time (dead time, delay time, or lag time) is the time required for a process variable to start changing after an initiating event.

For example, the extent of a change in the air/fuel ratio may not be fully detectable by an oxygen analyzer for several tens of seconds even if the oxygen measurement at the top of the firebox is instantaneous.

There may also be process response time between corrective action to safe state and the time at which safe state is achieved.

#### 3.4.1.3 Measurement Lag Time

Measurement lag time is the time required for an instrument to provide feedback to the control or safety system in response to a change in a process variable.

Measurement lag times are typically associated with temperature and analytical measurements.
The response times for analytical measurements are frequently represented as a percent of final value to a process step change. For example, T90 < 10 seconds represents a sensor response to 90% final value of the process deviation in less than 10 seconds.

### 3.4.1.4 Time Delays

Input time delays are frequently implemented to minimize spurious trips caused by transient conditions that do not create a process hazard. Due to the fast scan capability of PLC’s and other logic solvers, small variations or short term process impulses may be detected which may yield a spurious trip when hazardous conditions are not present. Therefore, an input time delay of 0.5 second to 1.0 second is frequently implemented as an input filter.

Delay trip timers may be used to confirm the presence of a hazardous condition for a sustained period prior to activating a trip; however, a thorough knowledge of the process safety time and time to safe state is required.

### 3.4.1.5 Time to Safe State

Time to safe state is the time difference between alarm or trip setpoint activation and the time required to achieve a safe state, thus mitigating the hazardous event. Setpoints should be selected to detect the unacceptable process deviation as early as possible in the process hazard timeline. For a protective function to be effective, safe state must be achieved within the process safety time.

- For operator response to an alarm, this includes diagnosis time, field travel time, corrective action time, and the process response time to achieve safe state and for the operator to confirm safe state.
- For an automated protective function, this includes delay trip timers in the logic solver, time to close the safety shutoff valve(s), and the process response time to achieve safe state.

### 3.4.1.6 Operator Response to Alarms

Alarms may be configured to notify the operator of abnormal process conditions, allowing the operator to take corrective action prior to an automated response by the safety shutdown system.

- The basis for alarm setpoints, the correct operator actions in response to the alarms, and the response time requirements to safe state should be documented during the design phase. Alarms that do not have a clear operator response should be avoided. It is important to identify which alarms require immediate response to assign them an appropriate priority. The operator response to each alarm should be defined in the process unit's operating procedures.

- A sequence of events alarm system functionality is recommended to support a shutdown system.

See 3.4.8 for the alarm summary table.

### 3.4.2 Overrides and Limits

A startup override is an automated bypass of a startup trip condition that is automatically enabled in the startup sequence when the trip condition is no longer present. If protective functions must be temporarily overridden to start up a heater, visual indication and/or alarm that the protective function is overridden should be provided to the operator. It is recommended that devices which are automatically overridden by the logic (even though manually initiated) be automatically returned to service (latched or activated) when the startup trip condition is cleared. It is recommended that startup overrides are designed as part of the logic to avoid inadvertently leaving a startup bypass active after startup.

- As an example, a startup override of the low fuel gas burner pressure trip is typically required to permit opening of the fuel gas block valves. Otherwise, the low pressure condition at startup below the trip setpoint would not...
allow the block valves to be sequenced open. Once the burner pressure is confirmed above the low pressure trip setpoint for a fixed time interval, the logic solver will typically activate the low pressure protective function.

- Startup override alarm and status indications should be provided to the operator interface.

A control override does not bypass a protective function. Instead, a control override is designed to keep the heater within operational limits and prevent a spurious trip (where applicable). A control override permits one controller to take control of the signal output from another controller. The output from two or more controllers is typically combined into a high or low selector, and the output from the selector controls the signal output to the final element.

- As an example, suppose the fuel gas controller is in temperature-to-flow cascade. A fuel gas pressure controller may be configured to monitor the burner pressure. At the low (or high) setpoint limit, the pressure controller may override the flow controller to keep the heater in a safe operating region and prevent a spurious trip on low (or high) burner pressure. Once the burner pressure is within the setpoint limits of the pressure controller, control is automatically returned to the flow controller via the high or low selector.

- Startup override alarm and status indications should be provided to the operator interface.

A setpoint or output limit(s) are configurable options at the controller to keep the heater within operational limits and prevent a spurious trip (where applicable).

- As an example, if the fuel gas controller is in temperature-to-pressure cascade, limits may be configured in the pressure controller to prevent a spurious trip on low (or high) burner pressure. Although generally referred to as a control override, the controller output is not externally controlled via a high or low selector. Instead, a soft clamp is configured into the controller.

- Setpoint or output limits are not typically annunciated at the operator interface.

### 3.4.3 Bypasses and Permissives

A bypass refers to a manually initiated action to bypass the input device(s) of a protective function and typically involves a keyed bypass or other manual initiation. A protective function that is bypassed is not available to trip until the bypass is manually removed and the protective function is returned to service.

- During normal operation, bypassing an input measurement device temporarily for maintenance, calibration, and testing is permissible where governed by trained personnel, applicable maintenance and operating procedures, and any emergency response procedures to the measurement under bypass. The associated control system alarm for the measured process variable cannot be bypassed at the same time as the protective device.

- Bypass alarm and status indications should be provided to the operator interface.

- It is recommended that a startup bypass is managed via a startup override.

Permissives are conditions which must be satisfied to progress to the next step in a sequence.

- As an example, fuel gas header pressure above a minimum light off pressure may be a permissive to open the pilot gas and/or fuel gas safety shutoff valves. Once the sequence has progressed to the next step, a permissive does not typically trip. For example, fuel gas header pressure (not burner pressure) may fall below permissive limits with no trip action once the pilots and/or burners are in service. At this point in the sequence, low fuel gas header pressure would typically alarm only.

- The status of permissives is typically indicated at the operator interface.

### 3.4.4 Process Hazards Protection

Recommended protective functions for process hazards related to fired heaters are provided below. These protective functions consist of a measurement and an action, usually operating valves, dampers, or motors. Each process deviation lists the process hazard, considerations, control overrides, alarms, and protective functions.

In each case, consideration should be given in regards to the redundancy required, both from an availability and reliability perspective. Accessibility to maintain and test on-line should also be reviewed. For redundant process
measurements, process tap locations and potential for common mode failure due to plugging or compromised measurement should be evaluated.

3.4.4.1 Accumulation of Combustibles within the Firebox (Loss of Flame, Substoichiometric Combustion, or Tube Leaks)

3.4.4.1.1 Process Hazards

Loss of flame, substoichiometric combustion or tube leaks may lead to the accumulation of combustibles within the fired heater.

Potential hazardous events include:

— afterburning in the radiant, convection, or stack sections which may result in the overheating and failure of tubes, tube supports and/or refractory systems;

— an explosion which may result in the partial or total destruction of the fired heater and which may be hazardous to personnel in the operating area.

These hazardous events may develop if the following occur:

— combustible material accumulates in the fired heater;

— oxygen is either present prior to the accumulation of combustible materials or oxygen is reintroduced after the accumulation of combustible materials;

— sufficient time passes to allow the combustible material and oxygen to meet and mix and thereby reach a flammable mixture condition;

— the flammable mixture is either hot enough to auto ignite or it encounters an ignition source such as a section of hot refractory, a heated analyzer sensor/cell, an operating pilot, or an operating burner.

3.4.4.1.2 Considerations

a. The hazard associated with a specific concentration of combustibles in the firebox mixing with fresh air and igniting may be estimated using thermodynamic calculations. The severity level posed by such an event depends on the amount of energy released as pressure\(^1\).

b. At startup conditions, the accumulation of combustibles within the firebox should not be permitted to exceed 25% of the lower explosion limit (LEL) before corrective action is initiated. The LEL may be calculated at laboratory conditions using Le Chatelier's formula and LEL data for pure components as listed in NFPA 325, Guide to Fire Hazard Properties of Flammable Liquids, Gases, and Volatile Solids, 1994 edition.

c. At operating conditions, it is possible for a heater to accumulate combustibles at firebox temperatures above the auto-ignition temperature if there is insufficient air to consume all of the fuel. Fuel-rich combustion produces hot flue gas with residual combustibles that can explode if mixed with fresh air.

---

too quickly. This is most likely to occur when a furnace transitions suddenly from rich combustion to lean combustion\(^2\).

d. Process deviations that precede flameout are typically associated with operational limits. Approaching or exceeding operational limits can lead to rapid accumulation of combustibles within the firebox. For example, loss of flame may result in the rapid accumulation of combustibles to an unacceptable hazard level in less than 10 seconds. Process deviations that precede flame out include:

- low fuel gas burner pressure (see 3.4.4.2),
- high fuel gas burner pressure (see 3.4.4.3),
- low combustion air flow (see 3.4.4.4),
- failure of dropout doors to open (see 3.4.4.5),
- low draft (high firebox pressure) (see 3.4.4.6),
- failure of stack damper to open (see 3.4.4.7),
- rapid change in fuel gas composition with uncompensated fuel flow (see 3.2.3.1),
- slug of liquid in fuel gas system that causes loss of flame

e. Process deviations that occur within operational limits may lead to substoichiometric combustion and a gradual accumulation of combustibles within the firebox. These process deviations include:

- a small hydrogen and/or hydrocarbon tube leak into the firebox;
- an increase in fuel gas flow rate to the burners without a corresponding increase in combustion air flow rate to the burners;
- a decrease in a combustion air flow rate or flue gas damper position in automatic control, (e.g. due to the malfunction high of an oxygen analyzer or the failure of a draft transmitter) without a corresponding decrease in fuel gas flow to the burners;
- burner tip plugging in one or more burners;
- partially closing a block valve on a fuel gas line to an individual burner;
- partially closing or fully closing the air register on an individual burner;
- changes in ambient conditions;
- changes in fuel gas composition;
- a reduction in firebox temperature (see 3.4.4.8);

\(^2\) Hawryluk, A., ibid.
f. Excessively fuel lean combustion with low firebox temperature may lead to gradual accumulation of combustibles within the firebox.

3.4.4.1.3 Control Overrides

Consider the following additional control overrides to keep the heater within operational limits and prevent a spurious trip (where applicable).

- Low fuel gas burner pressure override to the fuel gas controller (see 3.4.4.2).

- High fuel gas burner pressure override to the fuel gas controller (see 3.4.4.3).

- Reduce firing rate to established turndown condition during transition from balanced or forced draft to natural draft (see 3.4.4.5).

- Low draft (high firebox pressure) override (see 3.4.4.6).

- Low oxygen override to the fuel gas controller (see 3.4.4.9).

- High combustibles override
  a. For forced or balanced draft heaters, the combustibles measurement may be used as a control override to increase combustion air flow if combustibles levels are below a specified threshold, typically 500 ppm. Above that specified threshold, fuel gas flow should be reduced before combustion air flow is increased.
  b. For natural draft heaters, the combustibles measurement may be used as an override to the fuel gas controller to reduce fuel gas flow if combustibles levels are above a specified threshold.

- A design consideration is to adjust the rate of change of the controller output to the fuel gas control valve or stack damper such that a process step change may be detected within the overall response time of the control loop. For example, an oxygen analyzer located at the top of the radiant section may have an inherent process delay on the order of 60 to 90 seconds to T90.

- To be effective, control overrides should:
  a. be independent of the initiating cause (e.g., control loop malfunction) of the hazard scenario
  b. operate continuously in response to the process deviation creating the hazard scenario.

3.4.4.1.4 Alarms

- Alarms may be set to alert operators of abnormal process conditions that are approaching operational limits which may lead to flameout and the rapid accumulation of combustibles within the firebox. The alarms may be triggered by the following:
  a. low fuel gas burner pressure (see 3.4.4.2),
  b. high fuel gas burner pressure (see 3.4.4.3),
  c. low combustion air flow (see 3.4.4.4),
  d. low draft (high firebox pressure) (see 3.4.4.6),
This document is not an API Standard; it is under consideration within an API technical committee but has not received all approvals required to become an API Standard. It shall not be reproduced or circulated or quoted, in whole or in part, outside of API committee activities except with the approval of the Chairman of the committee having jurisdiction and staff of the API Standards Dept. Copyright API. All rights reserved.

b. Alarms may be set to alert operators to abnormal process conditions that occur within operational limits which may lead to substoichiometric combustion and a gradual accumulation of combustibles within the firebox. The alarms may be triggered by the following:
   — low oxygen (see 3.4.4.9),
   — high CO/combustibles,
   — partial loss of flame (loss of one or more burners with sufficient heat release and air from the online burners to sustain combustion in the firebox),
   — flooding alarm (a drop in process outlet coil temperature with an associated increase in firing rate when in temperature cascade mode).

3.4.4.1.5 Protective Functions

To mitigate process deviations at operational limits that precede flameout, close the fuel gas shutoff valves in response to:
   — low fuel gas burner pressure (see 3.4.4.2),
   — high fuel gas burner pressure (where applicable, see 3.4.4.3),
   — low combustion air flow (where applicable, see 3.4.4.4),
   — failure of dropout doors to open (where applicable, see 3.4.4.5),
   — low draft (high firebox pressure) (where applicable, see 3.4.4.6),
   — failure of stack damper to open (where applicable, see 3.4.4.7)
   — high liquid level in an upstream fuel gas drum (optional).

Note - The basis for tripping in response to process deviations that precede flameout is to prevent a rapid accumulation scenario. Once a rapid accumulation event is initiated, it may be challenging to achieve safe state within the process safety time.

c. Consider the following options in response to process deviations that occur within operational limits which may lead to substoichiometric combustion and a gradual accumulation of combustibles within the firebox.

Option 1 – Operator Response to a Fuel Rich Environment – This is the traditional option for refinery process heaters where operators are trained to recognize the signs of substoichiometric combustion such as:
   — alarms
   — a huffing sound associated with pressure pulsations in the furnace
   — elevated convection section or stack temperatures due to afterburning
   — smoke in flue gas leaving the stack
   — smell of unburned fuel
As long as combustion is sustained, operators should clear the area of personnel and slowly reduce fuel gas flow to avoid a hazardous situation. For example, if an operator responds to a fuel-rich furnace by completely shutting off the fuel then fresh air will mix with the combustibles inside the firebox and may ignite. Even a sudden change from 90% air to 110% air (10% excess air) could be too much for the furnace to follow safely. An understanding of the residence time is helpful to establish a safe ramp rate.\(^3\)

Potential advantage - This option reduces the number of times a fired heater is shutdown in response to substoichiometric combustion. Some facilities have operating experience to indicate that heater explosions are more likely to occur during light off, due to inadequate purge or delayed ignition, than during substoichiometric combustion.\(^4\) For those facilities, reducing the number of restarts may be an important consideration.

Potential disadvantage - The sequence of events may progress more quickly, from substoichiometric combustion to majority loss of flame, than the operator can effectively manage. Upon loss of flame the operator should close the fuel gas shutoff valves. Additional considerations in a fuel rich environment include:

- For heaters with automated snuffing steam valves or snuffing steam valves located a safe distance away from the heater, introduce snuffing steam into the firebox in conjunction with closing the fuel gas shutoff valves. With steam as a motive force, consider reducing combustion air flow or stopping the FD fan (where applicable).
- For balanced draft heaters, take into consideration that air preheaters are often corroded. To avoid a fire in the air preheater, consider shutting down the ID fan and partially open the stack damper.
- Consider removing potential ignition sources (e.g. continuous pilots and the analyzer sensor power).

**Option 2** – Prior to accumulating a hazardous gas mixture - Close the fuel gas shutoff valves at the onset of combustibles breakthrough using conventional combination oxygen/combustibles analyzers or laser based technology.

- Oxygen Analyzer (ZrO\(_2\))—90 % final response to a step change in flue gas composition is typically achieved in less than 10 seconds.
- Combustibles Analyzer (Catalytic Bead)—90 % final response to a step change in flue gas composition is typically achieved within 20-25 seconds.
- Laser based technology is capable of detecting oxygen or CO with 100 % final response to a step change in flue gas composition within 5 seconds.

Potential Advantage - For the gradual accumulation case, this option provides an opportunity to take corrective action to safe state early in the process hazard timeline. Some facilities have operating experience to indicate that heater explosions are more likely to occur as a result of improper response to a fuel-rich environment than during light off. For those facilities, reducing the likelihood of accumulating a hazardous gas mixture may be an important consideration.

Potential Disadvantage – If a gradual accumulation event progresses too quickly, the analyzers may be incapable of detecting a hazardous gas mixture prior to reaching hazardous levels. Thus, limiting controller ramp rate(s) such that a process step change may be detected within the overall response time of the control loop, and maintaining sufficient operating margin between oxygen setpoint and combustibles breakthrough, are important considerations.

\(^3\) Hawryluk, A., ibid.

Note - Ideally, the basis for selecting analytical trip setpoints at the onset of combustibles breakthrough (e.g. 1200-1500 ppm CO) is to mitigate the accumulation of a hazardous gas mixture prior to loss of flame. However, a gradual accumulation event must have sufficient process delay to facilitate detection of residual combustibles from fuel-rich combustion prior to reaching hazardous levels. In practice, the detection of low oxygen and/or high combustibles prior to loss of flame may be impacted by:

- Inherent process delay to achieve a representative sample at the sensor’s location (e.g. at the top of radiant section).

- Measurement delay due to sensor response - Typical published T90 specifications from catalytic bead and film sensors can range from < 20-30 seconds. These manufacturer specifications often do not define the concentration step change at which the T90 applies which may have a significant impact on T90 response (typically longer T90 times for lower concentration step changes). Analytical sensor test data may indicate the true T90 response time to a concentration step change of 0 - 1000 ppm and 1000 - 5000 ppm CO may be > 2 minutes. The true response time of the sensor may be determined by performing tests outlined in Section 3.2.4.1.

Option 3 - Upon Loss of Flame - Close the fuel gas shutoff valves upon loss of flame at one or more burners detected using flame scanners. Flame scanners have a configurable delay off timer that is typically configured from 0 to 4 seconds maximum to the logic solver.

Potential Advantage - This option provides the fastest response time to detect of loss of flame at one or more burners.

Potential Disadvantage - Complexity, reliability, and expense. As the number of burners is increased, resolving the correct trip voting logic can be a complex problem to resolve at different firing rates. For example, loss of a few burners at high firing rates may permit sustained combustion at higher firebox temperatures, but the same may not be true at lower firing rates. Additionally, flame scanners can be costly in relation to other protection layers and may present problems with sighting and discrimination between multiple burners.
The section above is a substantive change recommended by the committee to replace the following sections from the previous balloted version.

The September 2009 Ballot Version of the impacted sections is offered as a reference.

3.4 Protective Instrumentation and Protective Functions

The purpose of protective instrumentation and functions is to ensure safe operation (including startup and shutdown) and on-line protection for operational changes of fired heaters. The diversity in the design of fired heaters and their accompanying equipment requires each installation be studied to determine how to avoid failures that impact safety, asset loss, operability and the environment.

The complexity is dependent on several factors, including the following:

— type of process;
— operating temperature and pressure;
— type and size of the heater;
— type and number of burners;
— type of fuels;
— fuel supply reliability;
— type and reliability of the pilots;
— applicable federal, state and local regulations;
— safety integrity level requirements of the protective instrumented functions for safety, environmental and asset.

Protective Instrumentation Functions (PIF) are applied to both the process side (tube) and combustion side of heaters. PIFs are implemented to detect hazardous conditions and either achieve (shutdown) or maintain (permissive) a safe state. When a PIF is implemented to prevent hazardous events that could result in personnel or community injury/fatalities then the PIF is classified as a Safety Instrumented Function (SIF). PIFs that are implemented strictly for environmental or asset risk may be implemented using the same work process to insure the allocated risk reduction for these functions is achieved.
SIFs assigned Safety Integrity Level (SIL) of 1, 2, 3 or 4 (safety or environmental consequences) shall comply with the requirements of ANSI/ISA 84.00.01-2004 (IEC-61511 MOD). Although this standard is accepted good engineering practice and is recommended for Safety Instrumented Systems (SIS) the work process can be applied to asset and environmental PIFs. These PIFs may have an assigned Integrity Level (IL) that they should be designed to achieve but should be clearly identified as not safety related.

Protective actions include:

— control loops designed to prevent or mitigate the hazardous event,
— permissive functions and interlocks designed to prevent or mitigate the hazardous event,
— alarms followed by appropriate operator response,
— safety and protective functions in response to abnormal conditions including safety instrumented functions.

### 3.4.1 General

This section specifically addresses the following.

— Instrumentation and devices for use in protection of personnel, equipment, processes, and the environment. Instrumentation used in this manner is defined as protective instrumentation.

— Safety and loss prevention functions. These functions consist of a measurement and a response specifically designed to prevent the hazardous event from occurring.

Protective instrumentation applies to the following areas:

— alarms/indication;
— critical controls;
— safety, environmental, and asset loss protection instrumented functions;
— permissive/start up/shutdown/interlocks;
— manual intervention.

Protective instrumentation includes devices used for:

— process measurement (sensors, analyzers, transmitters, switches);
— actuating devices (valves, solenoid valves, relays);
— indicating devices (pilot lights, annunciators, visual indicators);
— control devices (Basic Process Control System (BPCS), Programmable Logic Controller (PLC), relays);
SIS logic solvers (including programmable electronic systems, hardwired relays, solid state systems);

— manual intervention devices (hard or soft hand switches/pushbuttons);

— Human Machine Interface (HMI) display graphics;

Protective System Considerations—General

— Automatic shutdown or operation to a safe state is recommended where abnormal conditions can cause a hazardous situation.

— Consideration must be given to all equipment modes of operation (e.g., start-up, process change, minimum firing and shutdown operations) to ensure there is adequate protection in all of these modes. Conditions such as sulfiding, hydrogen sweep, decoking, spalling, catalyst regeneration, and switching from forced to natural draft operations are examples of process change operations.

— If protective functions must be temporarily bypassed to start up a heater, visual indication and/or alarm that the protective function is bypassed must be provided to the operator. It is recommended that devices that are automatically bypassed by the logic (even through manual initiation) be automatically returned to service when the start up condition is cleared. It is recommended that any startup bypasses be designed as part of the logic (vs operator initiated) to avoid inadvertently leaving them active after startup.

— When loss of electrical power or instrument air occurs, it is essential that the BPCS, as well as the SIS, function in the way that has been determined to be the most favorable for overall safety. Once activated, the SIS should keep the process in the safe state until the unsafe condition is rectified and the SIS is manually reset.

3.4.2 Alarms

Alarms can indicate abnormal operation of process or equipment and allow the operator to take corrective action prior to automatic response by the safety shutdown system.

— The basis for alarms, setpoints of alarms, and the required operator response should be documented during the design phase. Alarms that do not have a clear operator response should be avoided. It is important to identify which alarms require immediate response to assign them an appropriate priority. The operator response to each alarm should be defined in the process unit's operating procedures.

— A sequence of events alarm system functionality is recommended to support a shutdown system.

See 3.4.7 for the alarm summary table

3.4.3 Time Response

Each safety function has a maximum permissible time for corrective action to mitigate a hazardous event.

3.4.3.1 Process Measurement Lag Time

Process measurement lag time is the time difference between a process deviation occurring and the time required for the instrument to detect it. Measurement lag times are typically associated with temperature and analytical measurements.
This document is not an API Standard; it is under consideration within an API technical committee but has not received all approvals required to become an API Standard. It shall not be reproduced or circulated or quoted, in whole or in part, outside of API committee activities except with the approval of the Chairman of the committee having jurisdiction and staff of the API Standards Dept. Copyright API. All rights reserved.

The response times for analytical measurements are frequently represented as a percent of final value to a process step change. For example, T90 < 10 seconds represents a sensor response to 90% final value of the process deviation in less than 10 seconds.

### 3.4.3.2 Process Safety Time

Process safety time is the time difference between the unacceptable process deviation and the hazardous event.

### 3.4.3.3 Time to Safe State

Time to safe state is the time difference between detecting the unacceptable process deviation and the time required to achieve a safe state, thus mitigating the hazardous event. This includes process response time, process measurement lag time, logic solver delay time, and time to close the safety shutoff valves. For a safety function to be effective, safe state must achieved within the process safety time.

### 3.4.3.4 Time Delays

Time delays are frequently implemented to minimize nuisance trips caused by transient conditions that do not create a process hazard. Due to the fast scan capability of PLC’s and other logic solvers, small variations or short term process impulses may be detected which may yield a nuisance trip when hazardous conditions are not present. Therefore, a time delay of 0.5 second to 1.0 second is frequently implemented as an input filtering time delay.

Delay trip timers may also be implemented to allow time for corrective action by the control system or operator response to alarm where the safety impact is not immediate; however, a thorough knowledge of the process safety time and time to safe state is required.

### 3.4.4 Process Hazards Protection

Recommended protective functions and safety functions for fired heaters are provided below. These safety and/or protective functions consist of a measurement and an action, usually operating valves, dampers, or motors. Each process deviation lists the potential process hazard, the recommended protective or safety functions, and options for consideration.

In each case, consideration should be given in regards to the redundancy required, both from an availability and reliability perspective. Accessibility to maintain and test on-line should also be reviewed. For redundant process measurements, process tap locations and potential for common mode failure due to plugging or compromised measurement should be evaluated.

#### 3.4.4.1 Flame Instability, Loss of Flame or Small Tube Leak leading to a Flammable Mixture within the Firebox

##### 3.4.4.1.1 Process Hazards

Flame instability, loss of flame or tube leaks may lead to the accumulation of carbon monoxide, hydrogen or hydrocarbon within the fired heater.

Potential hazardous events include:
afterburning in the radiant, convection, or stack sections which may result in the overheating and failure of refractory systems, tube supports and/or tubes;

— an explosion which may result in the partial or total destruction of the fired heater and which may be hazardous to personnel in the operating area.

These hazardous events may develop if the following occurs:

— combustible material accumulates in the fired heater;

— oxygen is either present prior to the accumulation of combustible materials or oxygen is reintroduced after the accumulation of combustible materials;

— sufficient time passes to allow the combustible material and oxygen to meet and mix and thereby reach a flammable mixture condition;

— the flammable mixture is either hot enough to auto ignite or it encounters an ignition source such as a section of hot refractory, a heated analyzer sensor/cell, an operating pilot, or an operating burner.

3.4.4.1.2 Considerations

1. LEL data is commonly available at laboratory conditions therefore the lower explosion limit (LEL) should be calculated at these conditions. To account for differences between laboratory conditions and actual firebox conditions, the accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox should not be permitted to exceed 25% of the laboratory based LEL before corrective action is initiated. Calculate LEL using Le Chatelier’s formula and LEL data for pure components as listed in NFPA 325, Guide to Fire Hazard Properties of Flammable Liquids, Gases, and Volatile Solids, 1994 edition.

2. Process safety time for an accumulation event is determined by the rate of accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox and the time required to reach the hazardous event.

a. For the total flameout case at maximum heat release, the process safety time may be in the range of 5 to 15 seconds depending upon fuel gas composition and the heater volume. This range is based on assuming the hazardous event is defined at the LEL and modeling the radiant section as a well stirred vessel with constant volumetric flow and no reaction.

b. Rapid accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox is defined as having a process safety time < 15 seconds (Note 1). Flameout at all burners may occur nearly simultaneously if a rapid accumulation event is allowed to progress.

c. Gradual accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox is defined as having a process safety time > 15 seconds (Note 2). Flameout at one or more burners may occur during a gradual accumulation event.

Note 1 - To construct a conservative basis, the process safety time for rapid accumulation to the LEL was estimated assuming total flameout at maximum heat release with a typical bridgewall temperature of 1450°F. A reduction in firing rate or loss of fewer burners may extend the process safety time depending upon the hazard scenario.

Note 2 - Although the transition point may be estimated at > 15 seconds, the true process safety time for a gradual accumulation event is more subjective. In practice, the capability to detect this
scenario is limited by the inherent process delay to achieve a representative sample at the top of the radiant section and/or the sensor response time.

3) Process deviations that precede flameout are typically associated with operational limits. Approaching or exceeding operational limits can lead to rapid accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox. Process deviations that precede flame out include:

a. low fuel gas burner pressure (see 3.4.4.2),
b. high fuel gas burner pressure (see 3.4.4.3),
c. low combustion air flow (see 3.4.4.4),
d. failure of dropout doors to open (see 3.4.4.5),
e. low draft (high firebox pressure) (see 3.4.4.6),
f. slug of liquid in fuel gas system that causes flame loss in one or more burners.

4) Process deviations that occur within operating limits may lead to a more gradual accumulation of carbon monoxide, hydrogen or hydrocarbon. These process deviations include:

a. hydrogen and/or hydrocarbon tube leak into the firebox;
b. an increase in fuel gas flow rate to the burners without a corresponding increase in combustion air flow rate to the burners;
c. a decrease in a combustion air flow rate or flue gas damper position in automatic control, because of the failure of an oxygen analyzer or draft gauge, without a corresponding decrease in fuel gas flow to the burners;
d. burner tip plugging in one or more burners;
e. partially closing a block valve on a fuel gas line to an individual burner;
f. partially closing or fully closing the air register on an individual burner;
g. changes in ambient conditions;
h. changes in fuel gas composition;
i. a reduction in radiant floor temperature (see 3.4.4.8).

3.4.4.1.3 Control Overrides

Consider the following additional control overrides to keep the heater in a safe operating region without putting a demand on the safety system.

1. Low fuel gas burner pressure override to the fuel gas controller (see 3.4.4.2).
2. High fuel gas burner pressure override to the fuel gas controller (see 3.4.4.3).
3. Reduce firing rate to established turndown condition during transition from balanced or forced draft to natural draft (see 3.4.4.5).

4. Low draft (high firebox pressure) override (see 3.4.4.6).

5. Low oxygen fuel gas override to the fuel gas controller (see 3.4.4.9).

6. High combustibles fuel gas override to the fuel gas pressure controller. The combustibles measurement may be used as an override variable to the fuel gas and/or combustion air flow controller if combustibles levels exceed a specified threshold (typically 500 ppm). Fuel gas flow or pressure should be reduced before combustion air flow is increased as high combustibles (and/or low oxygen) is typically the first indication of a potential firebox flooding situation. This indication may be followed by a rapid drop in coil outlet temperatures and/or firebox bridgewall temperatures.

7. A design consideration is to slow the rate of change of the controller output to the fuel gas control valve or stack damper such that a process step change may be detected within the overall response time of the control loop. For example, an oxygen analyzer located at the top of the radiant section may have an inherent process delay on the order of 90 seconds to T90.

3.4.4.1.4 Alarms

1. Alarms may be set to alert operators to abnormal process conditions that are approaching operational limits which may lead to rapid accumulation of carbon monoxide, hydrogen or hydrocarbon within the firebox. The alarms may be triggered by the following:
   
   d. low fuel gas burner pressure (see 3.4.4.2),
   
   e. high fuel gas burner pressure (see 3.4.4.3),
   
   f. low combustion air flow (see 3.4.4.4),
   
   g. low draft (high firebox pressure) (see 3.4.4.6),
   
   h. low firebox floor temperature (see 3.4.4.8),
   
   i. high liquid level in an upstream fuel gas drum,

2. Alarms may be set to alert operators to abnormal process conditions that occur within operational limits and that may lead to a more gradual accumulation of carbon monoxide, hydrogen or hydrocarbon. At less than 25 % LEL, the alarms may be triggered by the following:

   a. low oxygen (see 3.4.4.9),
   
   b. high combustibles detected using a convectional combustibles analyzer,
   
   c. high CO detected using laser based technology,
   
   d. loss of flame at one or more burners detected via flame scanners,
   
   e. high methane detected using laser based technology.
3. Proof of Closure Valve Diagnostic Alarm—If a block valve fails to close during a trip to main fuel gas within the prescribed time (e.g. 5 seconds to 10 seconds) it is recommended the operator take corrective action by isolating fuel gas at the battery limits.

### 3.4.4.1.5 Protective Functions

1. To mitigate process deviations at operational limits that precede flameout, close the fuel gas shutoff valves in response to:
   
   - low fuel gas burner pressure (see 3.4.4.2),
   - high fuel gas burner pressure (optional, see 3.4.4.3),
   - loss of combustion air (optional with trip to natural draft mode, see 3.4.4.4),
   - failure of dropout doors to open (see 3.4.4.5),
   - low draft (high firebox pressure) (optional, see 3.4.4.6),
   - high liquid level in an upstream fuel gas drum (optional).

   Note - The basis for tripping in response to process deviations that precede flameout is to prevent a rapid accumulation scenario. Once a rapid accumulation event is initiated, it may be challenging to achieve safe state (process delay, measurement delay, logic solver delay, and valve stroke time) within the allowable process safety time.

2. Consider closing the fuel gas shutoff valves in response to process deviations that occur within operational limits -that may lead to a more gradual accumulation of carbon monoxide, hydrogen or hydrocarbon. Response to these process deviations may take place prior to loss of flame, upon loss of flame or after loss of flame depending on the choice of instrumentation and the trip setpoint (not to exceed 25 % LEL).

   **Option 1—Prior to Loss of Flame**—Close the fuel gas shutoff valves at the onset of low oxygen and/or high combustibles detected using conventional combination oxygen/combustibles analyzers.

   - Oxygen Analyzer (ZrO2)—90 % final response to a step change in flue gas composition is typically achieved in less than 10 seconds.
   - Combustibles Analyzer (Catalytic Bead)—90 % final response to a step change in flue gas composition is typically achieved within 20-25 seconds.
   - Laser based technology is capable of detecting CO with 100 % final response to a step change in flue gas composition within 5 seconds.

   Note - To be actionable, a gradual accumulation event must be sufficiently slow such that the inherent process delay, sample location, and sensor response will permit detection prior to reaching 25% of the LEL and corrective action to safe state prior to reaching the LEL. In practice, the detection of low oxygen and/or high combustibles prior to loss of flame may be impacted by:

   - Inherent process delay to achieve a representative sample at the sensor’s location (e.g. at the top of radiant section).
Measurement delay due to sensor response - Typical published T90 specifications from catalytic bead and film sensors can range from < 20-30 seconds. These manufacturer specifications often do not define the concentration step change at which the T90 applies which may have a significant impact on T90 response (typically longer T90 times for lower concentration step changes). Analytical sensor test data may indicate that the true T90 response time to a concentration step change of 0-1000 ppm and 1000 - 5000 ppm CO may be > 2 minutes. The true response time of the sensor can be determined by performing tests outlined in Section 3.2.4.1.

Option 2—Upon Loss of Flame—Close the fuel gas shutoff valves upon loss of flame at one or more burners detected using flame scanners. Flame scanners have a configurable delay off timer that is typically-configured from 0 seconds to 4 seconds maximum to the logic solver.

Option 3 - After Loss of Flame - Close the fuel gas shutoff valves at the onset of high methane detected using laser based technology. This technology is capable of detecting methane with 100% final response to a step change in flue gas composition within 5 seconds. The response time is a configurable option and may be reduced to within 1 to 3 seconds as desired. This option may not be viable when firing refinery fuel gas as it may be difficult to resolve the methane concentration and the corresponding trip setpoint.
Section 3.4.7 Pre-Ignition Purge Cycle – (new) therefore also part of the ballot.

3.4.7 Pre-Ignition Purge Cycle

Prior to each fired heater startup, provision shall be made for the removal of combustible gases which may have entered the heater during the shutdown period. A timed pre-ignition purge cycle shall be repeated after every shutdown of all fuel sources (main fuel gas, waste gas and pilot gas).

When continuous pilots (where applicable) are operating, restart may be performed without the requirement for a full purge cycle. This restart should not be immediate but should include time to allow a minimum of one volume change of the firebox to post-purge the heater.

3.4.7.1 Purging a Firebox – Heated Analyzer Sensors as Ignition Source

When purging a firebox provisions should be made to prevent a heated oxygen, combustibles, or methane sensor from becoming an ignition source. Options include:

— Turn off the sensor power for 30 to 60 minutes prior to initiating the purge cycle to allow the sensor to cool below the fuel gas ignition temperature. Upon restoring power, an oxygen sensor may require 15 to 30 minutes to completely stabilize to published accuracy. A cold combustibles or methane sensor at ambient conditions may have a warm up period of 4 to 6 hours for the sensors to stabilize to published accuracy.
— For close-coupled extractive systems, blowback (reverse flow) instrument air or nitrogen through the sample probe during the purge cycle. Upon purge complete, standard sample flow is resumed with no sensor stabilization time due to interruption of power.
— Install flame arrestor(s); however, they add lag time (estimated 10 seconds extractive and 1 minute for in-situ probe systems) which is a consideration for process control or process safety applications where response time is critical.

3.4.7.2 Purging a Natural Draft Heater

Purge options:

a. Air purge a hot firebox (e.g. greater than 600°F)
   — The default purge timer is typically 15 minutes for five heater volume changes.
   — A bridgewall temperature indication may assist with shortening the purge time requirements as a hot firebox will draft more air.

b. Steam purge a cold firebox
   — Inject low pressure steam into either the radiant section or the base of the stack for at least 15 minutes for three heater volume changes.
   — It is difficult to calculate purge volumes with a steam medium. Therefore the purge timer should not start until steam is visually confirmed exiting the stack. The steam valve must be sufficiently opened to establish sufficient purge velocity, with a minimum of 50% open recommended.
   — Steam purging a radiant section can be a problem in cold weather locations due to the condensing of the steam in the firebox. A slow heat up rate is recommended to insure this water is re-evaporated and the refractory dried.
   — Using the base of the stack as the injection point may improve pilot reliability by keeping igniters and flame rods dry (where applicable).

Especially for a cold firebox, use a portable analyzer to check the firebox for combustibles through openings in the burners and/or observation doors at several locations.

3.4.7.3 Purging a Forced Draft Heater
Purge airflow shall reach no less than 70 percent of the airflow required at maximum continuous capacity of the unit. Confirm the purge interlock by satisfying either:

a. combustion air pressure (see 3.2.2.2) and all dampers in the flow path fully open

b. combustion air flow transmitter.

Purge for a period of not less than five minutes or five heater volume changes, whichever is greater, prior to being placed into service.

Consider the use of a portable analyzer to check the firebox for combustibles through openings in the burners and/or observation doors at several locations.

3.4.7.4 Purging the Air Preheater

If the firebox is fuel rich, a consideration is to purge the flue gas side of the preheat system by starting the ID fan, closing the stack damper, and purging the firebox in balanced draft mode. However, the ID fan does not typically have sufficient turndown to light the burners in balanced draft mode.

----------------end of section 3.4.7----------------