DIRECTIVE

NO: D-B6 100604 1

LOW PRESSURE THERMAL FLUID PLANT AUTOMATED CONTROL SYSTEMS

Date of Issue: June 4, 2010

General Details

This directive is being issued to owners, licensed contractors, consulting engineers, manufacturers and designers of low pressure thermal fluid plants to provide guidance on the registration of automated control systems required for the exemption for operators from certificates of qualification requirements for low pressure thermal fluid plants under the *Safety Standards Act*.

Specific Details

A low pressure thermal fluid plant is an assembly of one or more thermal fluid boilers which is protected with temperature control and safety devices that will not permit the boilers to continue to operate should the thermal fluid temperature rise to or above the vapour point of the thermal fluid at atmospheric pressure.

Section 6 of the *Power Engineers, Boiler, Pressure Vessel and Refrigeration Safety Regulation* ("the Regulation") now exempts operators of low pressure thermal fluid plants with a boiler capacity greater than 150m² from the requirement to hold a certificate of qualification to operate the plant if the plant is equipped with an automated control system that:

1) monitors performance of the plant, including all systems related to automated operation, and automatically alters the operation of the plant to ensure it is operating safely, including during start up and shut down operations, and
2) is designed so that any failure of the automated control system will cause the plant to go to a predetermined safe state.

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

FRM-1127-02 (2010-02-09)

Section 84.1 of the Regulation requires that the design of these automated control systems must be registered with a provincial safety manager and the registration of a design or an alteration to a design must be obtained before installation of the control system is commenced. To register a control system design the owner or the engineer, manufacturer or designer of the automated control system, acting as an agent for the owner, must submit, for review by a provincial safety manager, an application that includes:

1) all drawings, design specifications, calculations, information respecting safeguards, controls, interlocks, logic data, system testing and commissioning and codes of conformance as required by a provincial safety manager, and
2) an approval by a professional engineer of the automated control system's design and commissioning.

Registration Submission Requirements

The design submission must contain sufficient information and to demonstrate that the control system is capable of monitoring and automatically starting operating and shutting down a low pressure thermal fluid plant under normal, abnormal and emergency conditions. Submissions should include plans, drawings, details of the sequence of operations and operating specifications, safety device technical data, detailed plans for commissioning and verification of the control system operation after installation and the required procedures for maintaining, inspecting and testing to ensure the control system operates in accordance with its design over the service life of the plant.

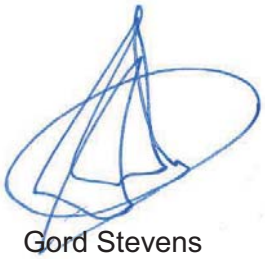
The minimum requirements for the content of an automated control system registration submission are listed in the attachment to this directive.

Upon satisfactory review of the registration submission, the control system design shall be assigned a British Columbia Limited Design Number (BCLD #). A design registration letter indicating the BCLD#, date of registration, owners name, drawing/revision numbers, registration fee and any other pertinent information will be sent to the applicant and a separate invoice for the registration fee will be forwarded on a separate cover. **No other documents will be stamped or returned to the applicant.**

After completion of the design registration and before starting the installation of the control system the plant the owner must notify a Safety Officer of the installation. The Safety Officer will make inspections during installation and commissioning as necessary to enable the Safety Officer to verify that the control system conforms to the registered design and operates as specified. After ensuring that all design and commissioning requirements have been satisfactorily completed and the training or qualifications of the individuals designated to operate the plant are adequate the Safety Officer can approve the plant for operation in accordance with the exemption Section 6(l).

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

If, in the opinion of a provincial safety manager, a registered automated control design is subsequently found to be defective in any detail, the design must be revised and those revisions must be approved and registered by a provincial safety manager. Until such revisions are approved staffing requirements for plants under review must meet the requirements of the regulation.



Gord Stevens
Acting Provincial Safety Manager – Boiler Technology

References:
Relevant Legislation

Power Engineers, Boiler, Pressure Vessel & Refrigeration Safety Regulation

Definitions and interpretation for this regulation

2 (1) In this regulation:

"low pressure thermal fluid plant" means an assembly of one or more thermal fluid boilers that do not contain an expansible fluid and are protected with temperature control and safety devices that will not permit the boilers to continue to operate should the temperature rise to or above the vapour point of the contained thermal fluid at atmospheric pressure;

Exemption from certification requirement to operate certain equipment

6 An individual is not required to hold a certificate of qualification to operate any of the following:

(l) a low pressure thermal fluid plant with a boiler capacity greater than 150 m^2 if the plant is equipped with an automated control system that

(i) monitors performance of the plant, including all systems related to automated operation, and automatically alters the operation of the plant to ensure it is operating safely, including during start up and shut down operations,

(ii) is designed so that any failure of the automated control system will cause the plant to go to a predetermined safe state, and

(iii) has been registered by a provincial safety manager in accordance with section 84.1.

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

Registration of control systems

84.1 (1) In this section, automated control system means an automated control system described in section 6 (l) (i) and (ii) and includes the commissioning programs, functional testing programs and maintenance programs for the system.

(2) The design of all automated control systems, including all alterations of previously registered designs, must be registered with a provincial safety manager.

(3) To register a design or an alteration to a design, the owner of the automated control system or the engineer, manufacturer or designer of the automated control system, if the engineer, manufacturer or designer is acting as an agent for the owner, must submit, for review by a provincial safety manager, an application that includes

(a) all design specifications, including information respecting safeguards, controls, interlocks, logic data and system commissioning and testing,

(b) an approval by a professional engineer of the automated control system's design, and

(c) any additional information with respect to the automated control system required by a provincial safety manager.

(4) Registration of a design or an alteration to a design must be obtained before installation is commenced.

(5) If, in the opinion of a provincial safety manager, a design registered under subsection (2) is subsequently found to be defective in any detail, the design must be revised by the person who submitted the design and those revisions must be approved by the provincial safety manager.

(6) The registration of a design or an alteration to a design does not relieve the professional engineer or equipment manufacturer of liability for the design and the installation of the automated control system.

Automated Control System Requirements

The automated control system shall be designed based on the operations of the low pressure thermal oil plant. The plant, its complete thermal oil system and its operation must be analyzed for all possible hazards and the associated safety risks. Strategies to manage these safety risks shall be addressed by the applicant and controls implemented in the system design to address these safety risks. Not all of the aspects outlined in these guidelines may be applicable to a particular control system however during development every factor must be reviewed; if it is deemed not to be applicable then a justification should be provided in the registration submission. Conversely there may be other aspects unique to specific plant operations that are not outlined in these guidelines which must be considered by the system designer.

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

The submission shall document all possible hazards in the plant operations that could lead to equipment failure or incidents. Hazard identification should take into account the primary causes and system failure modes such as equipment deterioration, operating conditions, environmental conditions and human interaction (operator or system user) which could result in safety incidents. Measures for monitoring conditions that could lead to incidents should be implemented and automated control routines incorporated into the design to eliminate or mitigate the hazardous conditions which can lead to incidents.

Registration submissions should include the following:

1. **Plans, drawings or other documentation** that show all essential plant details with regard to equipment and piping location, configuration and construction including:

    - the operating conditions for which the fluid heater was designed including type of fuel, pressure, temperature and type of thermal fluid including specifications such as fluid volume, mass, fluid viscosities, densities, and velocities at given temperature
    - a list of all combustion, control, and safety equipment giving manufacturer, type, model and number:
    - all safety devices should be listed for the service intended or approved by the Safety Manager if listed devices are not available
    - safety devices should be installed, used, and maintained in accordance with the manufacturer's instructions, located or guarded to protect them from physical damage and shall not be bypassed electrically or mechanically except for testing purposes.
    - purge, ignition trials and other burner safety sequencing should be performed using either devices listed for such service or programmable controllers
    - a description of plant design features used to minimize fire or explosion hazards, prevent released fluid leaks from flowing into adjacent areas or floors below fluid heaters, pumps and piping joints and details of how personnel are protected from fire or explosion hazards such as non-combustible construction, clearances, containment, explosion relief, location, explosion suppression, damage limiting construction.

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

- **A listing of possible hazards and the associated safety risks** as determined by hazard analysis and the conditions monitored by the control systems including the limits which will initiate a shutdown or cause the plant to go to another safe state. As a minimum the following conditions should be addressed:
    - pre-ignition purging to remove flammable gases prior to start-up
    - trial for ignition period to prevent build-up of unburned fuel and explosive conditions in the combustion chamber
    - proving combustion air flow prior to ignition or interlocks during operation
    - fuel pressure is within specified limits for safe combustion
    - flame supervision of the burners
    - liquid fuel temperature limits for proper burner operation
    - excess temperature limits for combustion chamber, thermal fluid or flue gas stack
    - adequate thermal fluid flow to prevent thermal damage to heat exchangers
    - thermal fluid leak detection and minimization of leakage
    - thermal fluid fires in the combustion chamber or other parts of the plant
    - a manual emergency device that initiates a safety shutdown
    - loss of electrical power
    - removal of heat after emergency shut down to prevent thermal damage to heat exchanger of other critical equipment

- **Measuring instrumentation and interlocks** to initiate alarms and automatically shut down the plant should be provided for the operating conditions:
    - low thermal fluid flow through the heat exchanger
    - high thermal fluid temperature or pressure at the heat exchanger outlet
    - low thermal fluid pressure at the heat exchanger or other critical parts of the system
    - high heat exchanger tube temperature
    - high heat exchanger furnace temperature
    - low thermal fluid level in expansion tank
    - activation of plant fire sprinkler system
    - high temperature of thermal fluid entering heat exchanger
    - high differential flow between heat exchanger inlet and outlet or in expansion tank
    - burner firing controls and flame supervision

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

- **Detailed interlocks and safety equipment descriptions** of the function and sequence of operations for in the control system:
    - pressure relief devices or other devices to prevent overpressure of the boilers, heaters, pressure vessels, piping or other components in the plant
    - where combustion air is provided by a fan or blower, combustion airflow or fan discharge pressure and damper position should be proven and interlocked with the fluid heater operation so that heater is shut off in the event of combustion air failure.
    - where a burner register air adjustment is provided, adjustment should include a locking device to prevent an unintentional change in setting.
    - a remotely located shutoff valve or other device shall be provided to allow the fuel to be shut off in an emergency; location and operation of this device should be such that fire or explosion at the fluid heater does not prevent access to or operation of this device
    - where a system includes a "built-in" test mechanism that bypasses any safety device, it shall be interlocked to prevent operation of the system while the device is in the test mode
    - safety interlocks should be in hardwired without relays in series ahead of the controlled device connected to an input of a programmable controller logic system
    - electrical power for safety control circuits should be DC or single phase AC, 250 volt maximum, one-side grounded, with all breaking contacts in the ungrounded, fuse-protected, or circuit breaker–protected line.
    - programmable logic controller–based systems listed for combustion safety service should be used in accordance with the listing requirements and the manufacturer's instructions.
    - the programmable logic controller should detect failure to execute any program or task containing safety logic, failure to communicate with any safety input or output changes in software set points of safety functions, failure of outputs related to safety functions and failure of timing related to safety functions; a safety shutdown should occur if any of these failures are detected
    - the following devices and logic should be hardwired external to the programmable logic controller as follows:
        - manual emergency switch
        - combustion safeguards
        - safe start checks
        - ignition transformers
        - trial-for-ignition periods
        - excess temperature controllers

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca

- a combustion safeguard should directly control at least one safety shutoff valve between the fuel gas supply and the monitored burner.
- where airflow proving logic is performed in the programmable logic controller, the logic should include verification of a change of state in each airflow proving device during the start-up of the related ventilation equipment and initiation of a safety shutdown if a change of state in an airflow proving device is not detected
- memory that retains information on loss of system power should be provided for software
- the programmable logic controller should have a minimum mean time between failure rating of 250,000 hours.
- all safety controls should be interlocked to shutdown the thermal fluid plant.
- operation of any interlock should require a manual reset prior to restart.
-

- **Commissioning plans** to verify correct installation, instructions for critical operating functions such as start-up, alarm response or emergency shut down, and schedules for inspection, testing and maintenance:
  - commissioning should validate that all equipment is installed in accordance with the system design, any changes to the original design made during commissioning are documented, set points of all safety interlocks are confirmed, all interlocks and actuators of fire protection systems are tested for proper function, and distribution piping for the extinguishing agent is unobstructed.
  - operating instructions should include, design limits (maximum and minimum) on process parameters such as firing rate, turndown, fluid flow rates, and fluid characteristics, start-up procedures, shutdown procedures and emergency procedures
  - instructions for the inspection, testing and maintenance of the safety controls including a schedule detailing the frequency (daily, weekly, monthly, annually)
  - pressure relief devices and safety interlocks shall be tested at least annually
  - explosion relief devices, if installed, and other fire protection equipment should be visually inspected to ensure that they are unobstructed and properly labelled.

For more information on the British Columbia Safety Authority, please visit our web site at:

www.safetyauthority.ca

505 SIXTH STREET, SUITE 200, NEW WESTMINSTER, BRITISH COLUMBIA, CANADA V3L 0E1
Toll Free: 1-866-566-SAFE (7233) Fax: 778-396-2064 Web Site: www.safetyauthority.ca E-mail: info@safetyauthority.ca