CONTRIVE

Q SERIES

PARAMETRIC BURNER CONTROLLERS

SAFETY MANUAL

SM8000 1025

SAFETY INTEGRITY LEVEL - SIL3
SYSTEMATIC CAPABILITY - SC 3

TARGET AUDIENCE
SYSTEM ENGINEERS
SIS (SAFETY INSTRUMENTED SYSTEM) DESIGNERS
MAINTENANCE TECHNICIANS

CONTENT

1. GENERAL INFORMATION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the parametric burner controllers Q1/Q2, with the following safety functions:

- Direct and indirect flame surveillance
- Gas leakage

The purpose of this Safety Manual, drawn up in compliance with the IEC 61508-2 and IEC 61508-3 standards, Annex D, is to provide the system integrator with all the information necessary for the correct use of the Q1/Q2 devices in Safety Instrumented Systems for SIL classified applications.

The Q1/Q2 devices are certified for Functional Safety according to IEC 61508, SIL 3, by an independent body (UL Solutions GmbH), for the safety functions mentioned above.

Functional safety activities for the entire product life cycle are entrusted to QSD sistemi.

2. VERSIONS

The following table provides an overview of the different functions and their availability in the different device models. Communication interfaces are available on all versions.

		Q1		Q2			
		Q11	Q12	Q21	Q22	Q26	Q28
1st stage fuel valve		●	●	●	●	●	●
2nd stage fuel valve			●		●	●	●
2nd flame sensor			●		●	●	●
Hi temperature bypass / Flameless			●		●	●	●
UV shutter control						●	●
Safety fuel valve	Valve Proving System					●	●
Bypass fuel valve						●	●
Fuel pressure switch input						●	●
Safety valve proof of closure						●	●
Air valve						●	●
Air pressure switch						●	●
Air actuator (3 points butterfly)							●

Q2 is fully integrated into an enclosure with aluminum base and polycarbonate front, user interface providing:

- led-bar flame signal indicator
- 2 seven segment status display
- led indicators for outputs and communication
- reset/shutdown button

Q1 is fully integrated into an aluminum or polycarbonate enclosure, user interface providing:

- led-bar flame signal indicator
- 1 seven segment status display
- led indicator for communication
- reset/shutdown button

3. SAFETY FUNCTIONS

3.1. SF-1 FLAME SURVEILLANCE

The Flame surveillance safety function can be divided in two sub-functions:

a. Flame loss
b. Illegal flame

Flame surveillance can be performed via:

i. Direct surveillance

Direct surveillance of the flame can be carried out with an electrode using the principle of rectification or with a phototube sensitive to ultraviolet radiation.

An additional UV phototube can be connected to a second input for independent monitoring of the flame belonging to a different burner stage.

The two independent flame amplifiers detect the signal coming from the sensors, supplying a differential signal to both microprocessors.

When the UV phototube is used for permanent operation, it will be necessary to use appropriate sensors equipped with electro-optical shutters, alternatively 2 independent sensors can be used to monitor the same flame (redundancy).

ii. Indirect surveillance

When the burner operates at high temperatures (combustion chamber walls over 750 °C) indirect monitoring of the flame is allowed in accordance with the provisions of EN 13577-2.

Indirect flame monitoring is activated by an external safety thermoregulator connected to terminal HT, this signal is dynamic and verified by both microprocessors.

When this signal is released the direct flame surveillance is reinstated.

Flame surveillance safety function is defined as follows:

a. Flame Loss

i. During normal operation of the burner in LOW TEMPERATURE mode, the flame is detected by means of sensor(s) (direct surveillance). In case of loss of sensed flame, the burner control, depending on the configuration parameter, performs one of the following actions (EN 298 § 7.101.2.3):

a) shutdown + ignition restoration
b) shutdown + recycling
c) lock-out

ii. During normal operation in HIGH TEMPERATURE mode, the flame is detected through the HT input (HTO indirect surveillance): In case of HT input release, the burner control (EN298 § 7.101.6.2):

- Restores direct flame surveillance, returning to LOW TEMPERATURE mode
- Stops the burner in CONTROLLED SHUTDOWN

b. Illegal Flame – During the purge phase (pre-purge and post-purge) of the burner, in case of sensed flame(s), the burner control performs the following safety action:

- lock-out

Summary of safety functions enabled for each version →

			Q11 Q21	Q12 Q22	Q26	Q28
SF-1	a	i	YES	YES	YES	YES
		ii	NO	YES	YES	YES
	b		YES	YES	YES	YES
SF-2	a		NO	NO	YES	YES
	b		NO	NO	YES	YES

3.2. SF-2 GAS LEAKAGE

Gas leakage safety function is defined as follows:

a. During the tightness test, in case of leakage in the automatic shut-off valves detected in the gas burning section, the burner control performs the following safety action:
   - lock-out

b. During normal operation of the burner, in case of fuel pressure switch detecting an incoherent condition (active when VS is OFF or inactive when VS is ON), the burner control performs the following safety action:
   a) Shutdown + recycling
   b) Lock-out

3.3. SF-1 AND SF-2 GENERAL NOTES

The following NOTES applies for the Safety Functions:

1. Q1/Q2 models in which the Safety Functions are included:
   - SF-1: all models
   - SF-2: Q26, Q28 models only
2. the lock-out condition corresponds to the following:
   - de-energisation of the master relay, AND
   - de-energisation of the fuel valves, AND
   - energisation of the crowbar relay

   the lock-out condition is saved in non-volatile memory
3. the shutdown condition corresponds to the following:
   - de-energisation of the master relay, AND
   - de-energisation of the fuel valves (V1, V2, VB, VS) output relays

   in case the feedback detects a double dangerous fault, the burner control activated the lock-out condition
4. the CONTROLLED SHUTDOWN condition corresponds to the following:
   - De-energisation of fuel valves (V1, V2, VS) output relays (the behaviour of the multifunctional valve VB can be parameterised)

   in case the feedback detects a dangerous fault, the burner control activated the lock-out condition
5. for SF-1a:
   i. during normal operation in LOW TEMPERATURE mode, the flame is detected by means of sensor(s) (direct surveillance). In case of loss of sensed flame, the burner control:
      - de-energises the master relay
      - de-energises the output relays

      then, if configured for LOCKOUT:
      - energises the crowbar relay
      - saves the lockout condition in non-volatile memory

      or, if configured for RECYCLE:
      - starts a new burner ignition trial from PRE-OPERATION

      or, if configured for IGNITION RESTORATION:
      - starts a new burner ignition trial from PRE-IGNITION

   ii. During normal operation in HIGH TEMPERATURE mode, the flame is detected through the HT input (HTO indirect surveillance): In case of HT input release, the burner control:
      - Restores direct flame surveillance, returning to LOW TEMPERATURE mode
      - Stops the burner in CONTROLLED SHUTDOWN
6. for SF-1b:
   a. During the purge phase (pre-purge and post-purge) of the burner, in case of sensed flame:
      - de-energise the output relays
      - energise the crowbar relay
      - save the lockout condition in non-volatile memory

3.4. SAFE STATE

Safety function	Safe state description
SF1a – case i - Flame surveillance – Flame loss – in LOW TEMPERATURE mode	Depending on the configuration parameter: a) shutdown + ignition restoration, OR b) shutdown + recycling, OR c) lock-out Where shutdown is: 1. Master relay de-energised 2. Fuel valves relays de-energised Where lock-out is: 1. Master relay de-energised 2. Fuel valves relays de-energised 3. Crowbar relay energised - with main fuse blown as outputs are intentionally tied to neutral while in lock-out (safe state). Safety relevant outputs are shorted to neutral by means of relay contact while in lock-out NOTE: the safe state is reached when at least one of the above conditions is reached.
SF1a – case ii - Flame surveillance – Flame loss – in HIGH TEMPERATURE mode	Restoration of direct flame surveillance, return to LOW TEMPERATURE mode Stopping of the burner in CONTROLLED SHUTDOWN Where CONTROLLED SHUTDOWN is defined as (according to EN 298): • *process by which the power to the shut-off valve(s) is removed before any other action takes place as a result of the action of a controlling function* with de-energisation of fuel valves (V1, V2, VS) output relays (the behaviour of the multifunctional valve VB can be parameterised)
SF1b – Flame surveillance – Illegal flame	Lock-out, i.e.: 1. Master relay de-energised 2. Fuel valves relays de-energised 3. Crowbar relay energised - with main fuse blown as outputs are intentionally tied to neutral while in lock-out (safe state). Safety relevant outputs are shorted to neutral by means of relay contact while in lock-out NOTE: the safe state is reached when at least one of the above conditions is reached.
SF2 – Gas leakage	Lock-out, i.e.: 1. Master relay de-energised, OR 2. Fuel valves relays de-energised, OR 3. Crowbar relay energised - with main fuse blown as outputs are intentionally tied to neutral while in lock-out (safe state). Safety relevant outputs are shorted to neutral by means of relay contact while in lock-out NOTE: the safe state is reached when at least one of the above conditions is reached.

3.5. SAFE STATE RETAINING

The safe state is retained until the specified conditions are fulfilled.

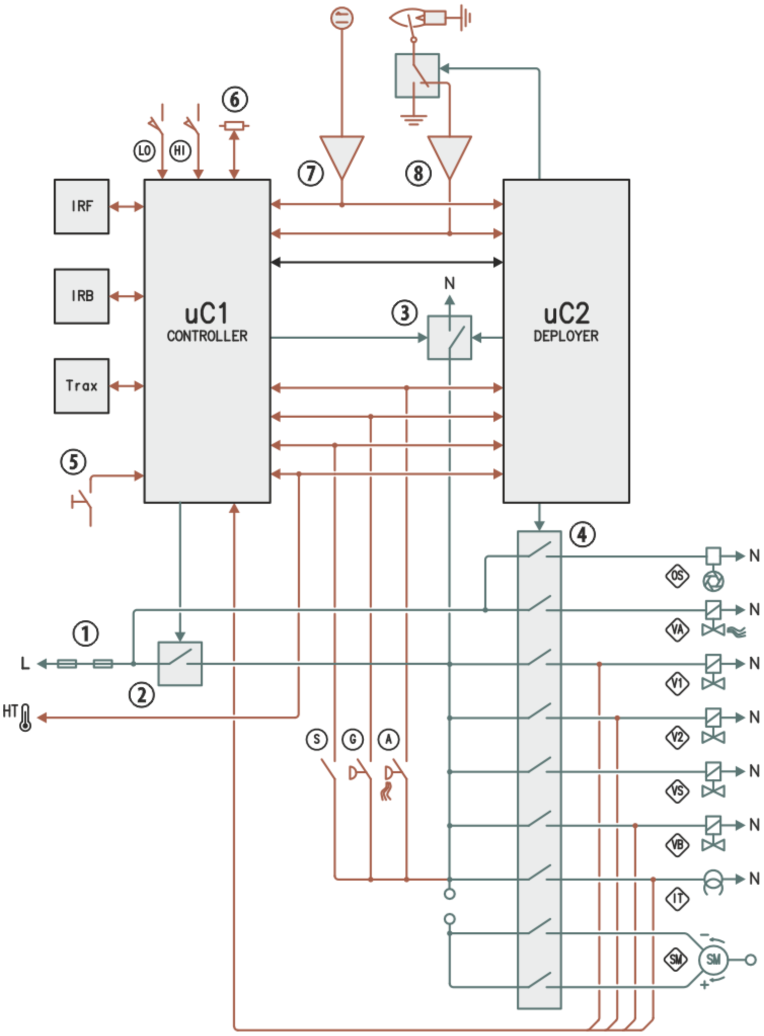
The safe state is maintained even by removing the power supply.

If no previous lock-out exists, the ability to store the non-volatile lock-out is checked as per EN 298 § 7.101.5: lock-out code written and read back (remains in lock-out in case of mismatch).

Safety function	Safe state retaining conditions
SF1 – Flame surveillance SF2 – Gas leakage	The safe state is retained until: • Reset performed by an authorised operator by means of push button or remote command • Replacement of the fuse(s) in case of destructive intervention of the crowbar relay.

4. HARDWARE ARCHITECTURE

To achieve the target SIL Capability, the device uses a redundant architecture for all safety inputs and outputs, in 1oo3 configuration.



Block diagram

1	MAIN FUSE + SAFETY FUSE
2	MASTER RELAY
3	CROWBAR RELAY
4	LOAD RELAYS
5	PUSH BUTTON
6	ACTUATOR POTENTIOMETER
7	2ND FLAME AMPLIFIER
8	1ST FLAME AMPLIFIER

S	PROOF OF CLOSURE SWITCH
G	FUEL PRESSURE SWITCH
A	AIR PRESSURE/FLOW SWITCH
LO	ACTUATOR LO SWITCH
HI	ACTUATOR HI SWITCH

IRF	FRONT IR INTERFACE
IRB	BACK IR INTERFACE
Trax	COM INTERFACE

HT	HIGH TEMPERATURE INPUT

OS	ELECTRO OPTICAL SHUTTER
VA	AIR VALVE
V1	FUEL VALVE 1
V2	FUEL VALVE 2
VS	SAFETY FUEL VALVE
VB	BYPASS VALVE
IT	IGNITOR
SM	ACTUATOR

5. APPLICATION

5.1. ENVIRONMENTAL LIMITS

Q1/Q2 are developed to operate in the following environmental conditions

	OPERATING	STORAGE AND TRANSPORT
AMBIENT TEMPERATURE	-20-60 °C (-4-140 °F)	-40-85 °C (-40-185 °F)
RELATIVE HUMIDITY	Up to 95% non-condensing	Up to 95% non-condensing
ALTITUDE	Up to 2000 m a.s.l.	-
VIBRATIONS	10 m/s^2 from 10 Hz to 150 Hz	-
PROTECTION OF HOUSING	IP54	IP54

When the device is used in different environmental conditions, it is necessary to use suitable means or to install it in suitable environments to avoid malfunctioning of the system.

The unit is not intended for explosive or corrosive environments

5.2. APPLICATION LIMITS

The installation and commissioning of the unit must be performed by a qualified flame safeguard service technician, familiar with the application environment in which the unit is installed. This expert must be familiar with the product and have received appropriate training.

The unit must be installed as specified in the instruction manual, verifying compliance with the required environmental conditions.

The device operates in "High Demand Mode" pursuant to EN 61508-4, 3.5.12.

5.3. CONFIGURATION AND SECURITY REQUIREMENTS

The modification of the safety parameters can be carried out with a special software tool and magneto-optical interface by forcing the device into Manual Shutdown.

To apply the changes, the specific password of the device must be provided for which up to 8 alphanumeric characters can be used; the factory default is 00000000 (8 zeros) and must be changed during installation.

It will be the installer's responsibility to change the password to protect the configuration by avoiding unauthorized access, keeping the password for future access.

5.4. USEFUL TIME

The useful lifetime is at least 10 years.

5.5. PROOF TEST

No proof test is required, as the device performs all diagnostic tests by itself, and the safety functions work in High Demand Mode.

5.6. PERIODIC MAINTENANCE

No specific periodic maintenance is required; however, it is recommended to check at least once a year:

- Integrity of the device and its fasteners.
- Integrity and insulation of the electrical connections, especially for the high voltage cables of the ignitor.
- Integrity of protective ground connections.
- Absence of rust and dirt.

5.7. REPAIR AND REPLACEMENT

If this unit is not working properly, it must be replaced.
Repairs are not permitted.

5.8. MANUFACTURER NOTIFICATION

Any failures that are detected and that compromise functional safety shall be reported to:

CONTRIVE S.r.l.
Via Enrico Fermi 18
24040 SUISIO (Bergamo)
ITALY
https://www.contrive.it/support

6. FAILURE MODES AND FAILURE RATES

The failure modes and failure rates are shown in the following table.

SAFETY FUNCTION	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_{S} [1/h]	SFF [%]	PFH [1/h]
Flame surveillance – with flame sensor	2,72E-09	8,21E-08	1,51E-07	98,85	2,72E-09
Flame surveillance – with HTO	2,59E-09	6,88E-08	1,79E-07	98,97	2,59E-09
Gas leakage	2,59E-09	6,88E-08	1,79E-07	98,97	2,59E-09

Table 1 - Failure rates, SFF, PFH results

The values are guaranteed for the useful lifetime defined in clause 4 with the device used under the conditions specified in clause 3.
The values for safety function “Flame surveillance” represent the worst-case between “flame loss” and “illegal flame”.

NOTE:
The following fault exclusions were taken into consideration during the evaluation:

- Short-circuits between two adjacent tracks/pads (according to IEC 60664-1 and 60664-5)
  - the clearances and creepage distances are greater than 3 mm for tracks powers by PELV power supply with pollution degree 2 / overvoltage category III
  - the clearance and creepage distances are greater than 0,1 mm for track powered by PELV power supply with pollution degree 2 / overvoltage category II
  - base material according to IEC 60893-1
  - assembled board mounted in an enclosure giving protection of at least IP54 and the printer sides are coated with an ageing-resistant protective layer covering all conductor paths.

7. DIAGNOSTICS

Q1/Q2 contains hardware and software mechanisms to detect and react to the detection of a dangerous failure.

Diagnosed block / function	Diagnostic method	Estimated DC	Diagnostic test interval TI_D	Fault reaction
Power supply (12V)	Under- and over-voltage monitoring diagnostic function performed via a voltage divider connected to a dedicated ADC on uC2	≥ 90%	Runtime (≤ 1 s)	Lock-out
Power supply (3,3 Vdc to microcontroller)	Under- and over-voltage monitoring diagnostic function performed by an HW voltage monitor	≥ 90%	Runtime (≤ 1 s)	Lock-out
Temperature	Temperature diagnostics provided by an internal sensor in both microcontrollers	--	Runtime (≤ 1 s)	Lock-out
Analog inputs - Comparison	Comparison of antivalent analog signals deriving from the same flame input – by both microcontrollers	≥ 90%	Runtime (≤ 100 ms)	Lock-out
Analog inputs - out-of-range diagnostics	Comparison of the analog input value (flame input) with an acceptance range – by both microcontrollers	≥ 90%	Runtime (≤ 100 ms)	Lock-out
Digital inputs - Comparison	Comparison of digital signals deriving from the same input (Fuel pressure switch, High temperature switch) – by both microcontrollers	≥ 90%	Runtime (≤ 100 ms)	Lock-out
Digital inputs – Diagnostics on single channel	Inputs reading by means of optocoupler transferring only half-wave of the AC voltage applied to LED emitter	99%	Runtime (≤ 100 ms)	Lock-out
Analog inputs – Diagnostics on single channel	Periodical test of flame input	99%	55 min (according to EN 298)	Lock-out
CPU	ALU self-test	90%	Runtime (≤ 60 s)	Lock-out
(Program) Invariable Flash memory	CRC of program flash memory (test performed via FW routine)	99%	Runtime (≤ 60 s)	Lock-out
Variable memory (RAM and external EEPROM)	Memory verification before use, by comparison of redundant, bit-inverted data	90%	Runtime (tested-when-used)	Lock-out

Diagnosed block / function	Diagnostic method	Estimated DC	Diagnostic test interval TI_D	Fault reaction
Program sequence	Temporal and logical monitoring of the program sequence performed via FW routine	90%	Runtime (≤ 200 ms)	Lock-out
Program execution	Reciprocal comparison by software	90%	Runtime (≤ 900 ms)	Lock-out
Fuel valves output circuitry	Feedback reading after relay contacts	99%	At the change of state of outputs	Lock-out

Diagnosed block / function, Diagnostic method, Estimated DC, Diagnostic test interval, Fault reaction (behavior at the detection of a fault)

NOTE: The flame failure response time (FFRT) is configurable between 1 and 10 seconds.
The response time of the fuel pressure switch during the tightness test is not more than 1 second.

8. DEVICE CLASSIFICATION

This unit is a type B device (complex) suitable for use up to SIL 3 with

HFT=0 for Input,
HFT=1 for Logic
HFT=2 for Output

9. SYSTEMATIC CAPABILITY

This unit is a type B device (complex) suitable for use up to SIL 3 wit The Systematic Capability is equal to 3, provided that the indications given in the User Manual and the contents of this document are complied with.

10. COMMON CAUSE FACTORS

B=βD=2% is used as Common Cause Factor for internal redundant blocks.

11. SYSTEM SOFTWARE

11.1. CONFIGURATION

Device configuration is described in detail in document B8000 – TECHNICAL INFORMATION.

11.2. COMPETENCE LEVEL OF PERSONNEL

The personnel responsible for operating the system software must be competent both with regards to combustion systems and with regards to manual parameterisation via software.

11.3. INSTALLATION INSTRUCTIONS

No software installation is required by the end user.

11.4. ANOMALIES

No known anomalies.

11.5. COMPATIBILITY WITH PREVIOUS VERSIONS

Not applicable.

11.6. MODIFICATIONS

The user of the device does not have the possibility to request a change in the functioning of the system software; he/she can only report any malfunctions due to software errors (bugs).

11.7. SECURITY MEASURES FOR SYSTEM SOFTWARE

A detailed description of the specific measures for protection against cyberattacks is given in document B8000 – TECHNICAL INFORMATION.

12. REFERENCE STANDARDS

- **IEC 61508:2010 Parts 1-7**
  Functional safety of electrical/electronic/programmable electronic safety-related systems
  considered as basic standard, and as main standard for SIL assessment
- **EN 298:2022**
  Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
  considered for functional safety requirements only
- **EN 1643:2022**
  Safety and control devices for gas burners and gas burning appliances
  Valve proving systems for automatic shut-off valves
  considered for functional safety requirements only
- **EN 13611:2019**
  Safety and control devices for burners and appliances burning gaseous and/or liquid fuels
  General requirements
  considered for functional safety requirements only, and as referenced by EN 298 and EN 1643
- **EN IEC 60730-1:2022**
  Automatic electrical controls
  Part 1: General requirements
  considered for functional safety requirements only, and as referenced by EN 298 and EN 1643
- **EN IEC 60730-2-5:2017**
  Automatic electrical controls
  Part 2-5: Particular requirements for automatic electrical burner control systems
  consolidated version
- **EN 13577-2:2023**
  Industrial furnaces and associated processing equipment - Safety
  Part 2: Combustion and fuel handling systems (ISO 13577-2:2023)
  considered as far as applicable

13. RELATED LITERATURE

All documents related to Q2 for the user are available from the following website:

https://www.burner-control.com

CONTRIVE

CONTRIVE S.r.l. I-24040 SUISIO (Bergamo) via Enrico Fermi 18

ANY ILLUSTRATIONS, PHOTOGRAPHS, OR EXAMPLES USED IN THIS MANUAL ARE PROVIDED AS EXAMPLES ONLY AND MAY NOT APPLY TO ALL PRODUCTS TO WHICH THIS MANUAL IS APPLICABLE. THE PRODUCTS AND SPECIFICATIONS DESCRIBED IN THIS MANUAL OR THE CONTENT AND PRESENTATION OF THE MANUAL MAY BE CHANGED WITHOUT NOTICE TO IMPROVE THE PRODUCT AND/OR THE MANUAL.

PRODUCT NAMES, CORPORATE NAMES, OR TITLES USED WITHIN THIS DOCUMENT MAY BE TRADEMARKS OR REGISTERED TRADEMARKS OF OTHER COMPANIES, AND ARE MENTIONED ONLY IN AN EXPLANATORY MANNER TO THE READERS' BENEFIT, AND WITHOUT INTENTION TO INFRINGE.

WHILE EVERY EFFORT HAS BEEN MADE TO MAKE SURE THE INFORMATION IN THIS DOCUMENT IS CORRECT, CONTRIVE CAN NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER FOR LOSS RELATING TO THIS DOCUMENT.