



Exploration & Production

GENERAL SPECIFICATION

INSTRUMENTATION

GS INS 150

**Design method for system configuration
standard functions**

01	10/04	Revised as per marking
00	11/03	First issue
Rev.	Date	Notes



Contents

1. Scope	3
2. Reference documents.....	3
3. Glossary.....	4
4. Definitions.....	4
4.1 Standard Function	4
4.2 Modes and Controls.....	6
5. Main Commands from HMI and Controls	7
5.1 Commands of valves	7
5.2 Motor Interfaces.....	7
5.3 Packages control	8
6. Access levels.....	8
7. Alarm and event management	8
7.1 Alarm and event levels	8
7.2 Alarm acknowledgement management	9
7.3 Events and values	10
8. General principles	10
8.1 Discrepancy	10
8.2 Fault status	10
8.3 Redundant analogue inputs (RAI)	10
8.4 Maintenance inhibition	10
8.5 Start-up inhibition.....	11
8.6 Maintenance commands.....	11
8.7 Safety bar Isolating	11
9. List of Standard Functions	12

1. Scope

The purpose of this document is to define the Design Methodology for Control and Safety System Configuration Standard Functions. The principle of this methodology is the development of Standard Functions which are re-usable within a hierarchical structure.

These Standard Functions shall define the operating and control requirements of equipment in both normal and degraded conditions, along with its operator interface definition.

A set of Standard Functions Specifications, listed in §9, has been prepared and detailed, based on the general principles defined in this document. It is believed that these Standard Functions cover the majority of cases. However, each project shall review its specific requirements and prepare supplementary Standard Functions as necessary. Company subsidiaries may use their own library of Standard Functions when available.

This specification requires that the methodology of using Standard Function when configuring instrument systems is maintained in all cases. These shall always be fully tested early in the software lifecycle to prove their operation meets the required functionality. This will therefore assist in reducing the overall configuration development time, while at the same time improving overall quality.

All such Standard Functions shall be fully documented.

2. Reference documents

The reference documents listed below form an integral part of this General Specification. Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the EFFECTIVE DATE of the CONTRACT.

Standards

Reference	Title
Not applicable	

Professional Documents

Reference	Title
Not applicable	

Regulations

Reference	Title
Not applicable	

Codes

Reference	Title
Not applicable	

Other documents

Reference	Title
Not applicable	

Total General Specifications

Reference	Title
GS SAF 261	Pressure protection and relief, emergency shut-down and depressurisation
GS INS 134	Design and supply of integrated control and safety systems

3. Glossary

DCS	Distributed Control System.
FGS	Fire and Gas System
ICSS	Integrated Control and Safety System
MCC	Motor Control Centre
HMI	Human Machine interface
PCS	Process Control System
PDS	Process Data Server
PSS	Process Safety System
UCP	Unit Control Panel (package)
SSS	Safety Shut-down System

4. Definitions

4.1 Standard Function

A Standard Function describes all logic and calculation functions that characterise either process equipment (transmitter or actuator), or control algorithm management (pressure/temperature compensated flow, totalized flow, duty/backup/standby, etc...).

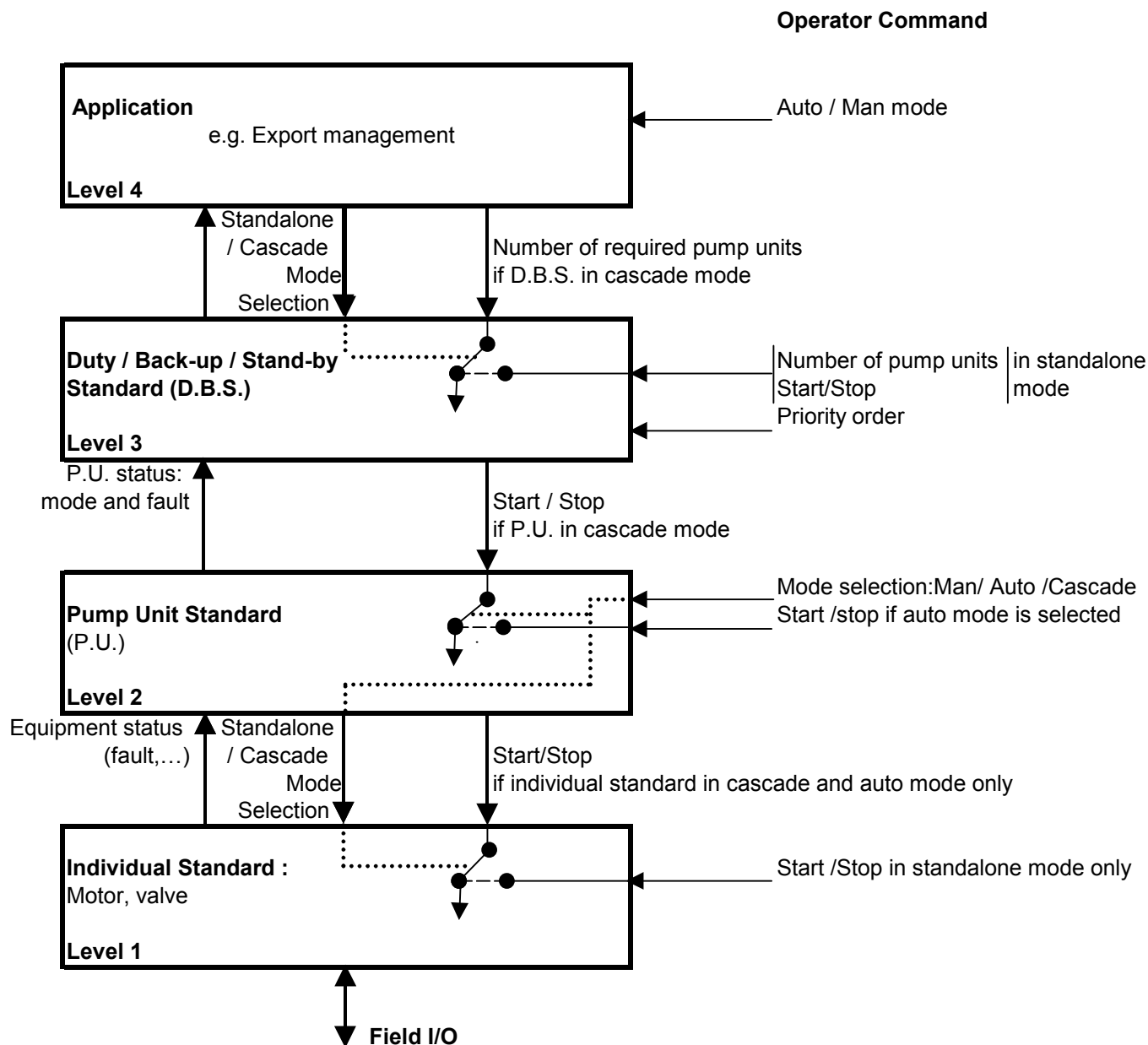
These functions may be carried out by the Distributed Control System (DCS), the safety system (ESD, PSS and FGS), or the package control panel (UCP).

It also describes the associated Human Machine Interface (HMI) representation. Access to operator commands or specific faceplates (pop-up) are detailed in the different Standard Functions, but may be changed in function of Systems features.

The following diagrams show how individual Standard Functions can be linked in a hierarchic way to create more complex functions.

Data may be exchanged in both ways between consecutive levels.

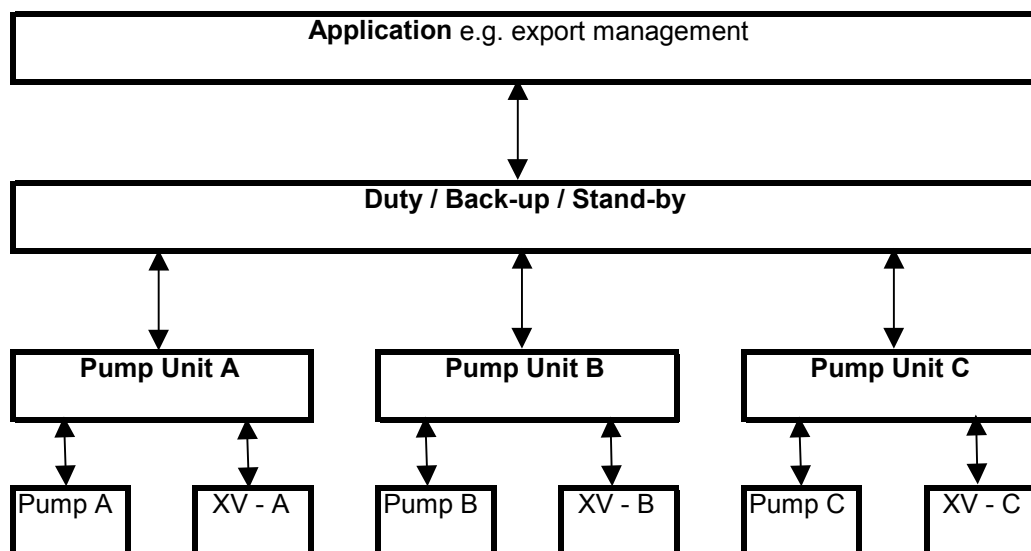
Example of Standard arrangement



To simplify the representation, this arrangement shows one Pump Unit and one individual Standard Function only.

In principle, as many individual Standard Functions as primary elements (e.g. pump (motor), upstream and downstream valves) may be connected to each Pump Unit Standard Function.

Likewise, as many Pump Unit Standard Functions as pump runs may be connected to Duty / Back-up / Stand-by Standard Function.



4.2 Modes and Controls

Two different modes may be implemented within each Standard Function:

- Auto / Man
- Standalone / Cascade

When it exists, Auto / Man mode is selected by the operator, whereas Standalone / Cascade mode of a Standard Function at level N may be either forced by the Standard Function at level N+1, or selected by the operator.

Standalone / Cascade mode determines whether the corresponding Standard Function runs on its own or is interlocked with a higher level Standard Function.

In order to avoid process upsets during transitions (auto/man, standalone / cascade, etc), DCS status and commands will be systematically tracked and aligned to those currently present, except if specified differently within the functional analysis.

Consider the example shown above with 3 pump runs (A, B and C):

- When the operator switches the Pump Unit A to manual mode, the different individual Standard Function will run in standalone mode, which authorises the operator's command (start/stop of the pump, open/close of the valve...). Likewise the operator can not remotely operate any equipment (mainly valves and motors) when the cascade mode is active.
- At the same time, if both Pump Units B and C are set to cascade mode, they will be operated by commands issued from the Duty / Back-up / Stand-by Standard Function. The corresponding valves and motors will be operated without any operator intervention.

5. Main Commands from HMI and Controls

Operator commands such as AUTO/MAN, START/STOP, OPEN/CLOSE, SELECTION, SETPOINT, OUTPUT VALUE ... are available at the HMI.

However, they may be overridden by process control or safety control. Each Standard Function description defines this possibility.

5.1 Commands of valves

Valve Standard functions shall be able to handle the control functions as described below.

For more details about ON/OFF valves general functional requirements, see [GS SAF261](#).

	ESDV	SDV	BDV	XV
Control signal failure action	Close	Close	Open	(1)
Power fluid failure action	Close	Close	Open	(1)
Open/Close local command	Yes	Yes	Yes	(1)
Local Reset after ESD	Yes	No	Yes (2)	No
Partial stroking facility	Yes	Yes (1)	No	No
ESD signal test facility	Yes	Yes (1)	Yes	No
Open remote control	No	(1)	Yes (3)	Yes
Close remote control	Yes	(1)	No (2)	Yes

(1) as per project requirements.

(2) automatic reset or reset from control room may be envisaged in specific cases.

(3) interlocked with “permissive” to blow down operations

For more details about on/off safety valves functional requirements and accessories, see [GS SAF 261](#).

In addition, the project Standard Functions will have to cope with specific project control requirements.

5.2 Motor Interfaces

The motors Standard Functions shall enable the controls and monitoring as below:

	Start/Stop command	Safety trip command	Status feedback	Unavailable
Low voltage	Yes	Yes	Yes	Yes
High voltage	Yes	Yes	Yes	Yes

Details relative to signals types are given within individual Standard Functions.

Usually electrical interface is achieved through hardwired links. But if cost effective, smart high and low switchboards may be selected. In this alternative, all data and commands will be exchanged via digital links, except safety trip commands which shall always be hardwired.

Tracking between Power Distribution Control System, handling load shedding function, and DCS may be required to avoid discrepancies.

5.3 Packages control

Unless specified differently within the project specifications, a LOCAL/REMOTE selection is available from the DCS HMI for each package.

Packages operated in local mode are still monitored from the DCS.

If the DCS and the package are connected via a digital link, this command will be automatically switched to LOCAL mode in case of link failure.

This link shall be monitored by a watch-dog system in both DCS and package control panel.

When switching from LOCAL to REMOTE mode, the DCS data will be re-aligned on the package states.

6. Access levels

Five access levels from MMI are identified:

- Visitor: no accessible command
- Operator: normal process control
- Maintenance: first level of intervention
- Method: process parameters modifications
- Engineer: all system modifications including system configuration modifications by using the Engineering software tool.

If not requested by the application, the method level may not be implemented.

Levels of access to the different functions are defined individually in each Standard Function.

7. Alarm and event management

7.1 Alarm and event levels

Alarms described hereafter are those associated with the process. Standard Function system alarms and status such as redundancy failure, I/O module failure, system, etc, have their own system management.

Alarms and events are arranged according to four levels. These priority levels are defined according to the source of the alarm and its degree of urgency:

Level 0: indicates that this event shall be only logged on the DCS with no alarm

Level 1: indicates that this event is alarm linked to the process control and consequently issued by the Process Control System (PCS) or packages control panels

Level 2: indicates that this event is alarm linked to the process safety and consequently issued by the Process Safety System (PSS) or packages control panels

Level 3: indicates that this event is alarm linked to the Emergency Safety functions and consequently issued by the Safety Shutdown System (SSS) or the Fire and Gas Systems (main FGS or package FGS in case of turbo-generators for instance).

The level is specified individually for each alarm within each Standard Function.

All alarm information shall be time stamped and recorded.

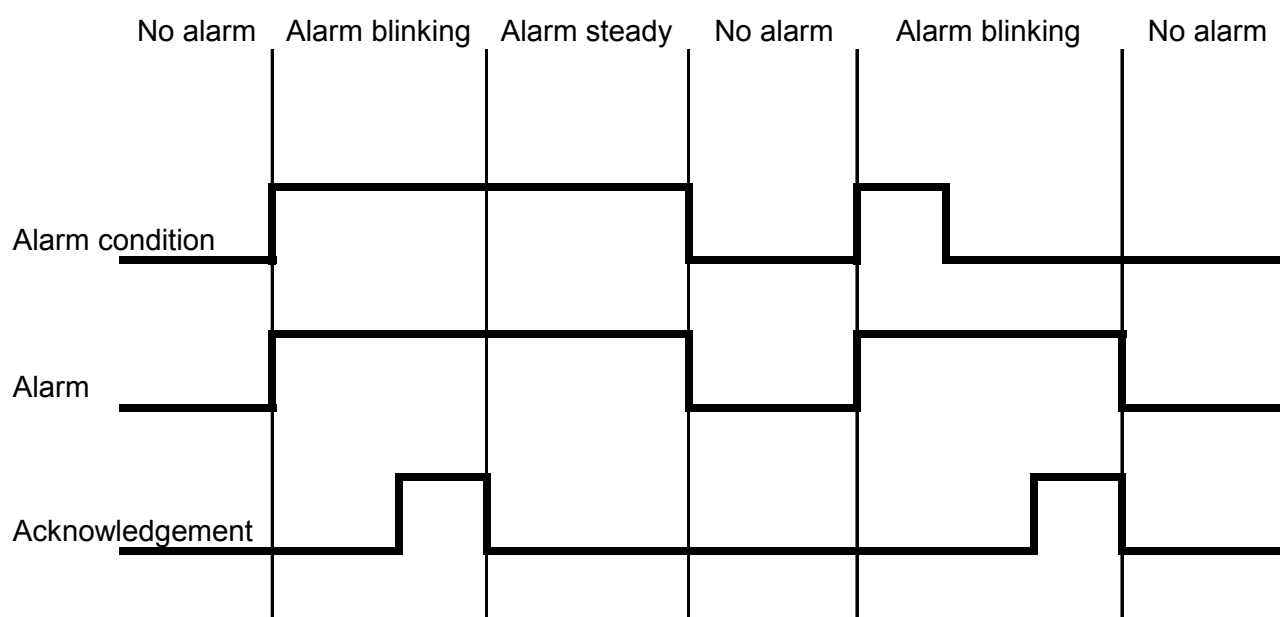
They shall be available to the operator either in chronological order of occurrence, priority level or according to other criteria defined through by the HMI.

These alarm lists shall be printed upon the operator request. No automatic alarm printing is required.

7.2 Alarm acknowledgement management

Each alarm remains active, until it is acknowledged and the alarm condition has disappeared.

It applies to both display and automatic control. Each alarm operates as shown in the diagram below.



Acknowledgement on a process view leads to the individual acknowledgement of all active alarms on the same process view.

Moreover the alarm acknowledgement leads to the acknowledgement of the same alarm on all views and top header where the alarm is present.

Generally no acknowledgement of alarm is possible from alarm list, except when in maintenance access.

Any automatic alarm priority level change or masking shall be as defined within the specific project's functional analysis: e.g. a PALL alarm at pump outlet shall be active only if the pump is running. In this case, the start-up inhibition will be activated by the pump restart (see § 8.5 - Start-up inhibition).

7.3 Events and values

Events and values to be recorded are defined individually within each Standard Function.

8. General principles

8.1 Discrepancy

Motor: The detection of a discrepancy between the command and status leads to lock automatically the "Start/Stop" command on "Stop".

Valve: In general, the detection of a discrepancy between the command and status of the valve will not affect the command state which remains unchanged.

8.2 Fault status

8.2.1 Definition

Fault status of a signal corresponds to:

- A fault loop: transmitter or loop itself
- A faulty I/O module.

Consequences of fault status are specified individually within each Standard Function.

8.3 Redundant analogue inputs (RAI)

For the same process measurement, two similar transmitters may be used: one is connected to the PCS and the other one to the PSS.

When PSS functions are processed by the same type of controllers as PCS, then the specific Standard Function (RAI) may be applied: if the PSS transmitter loop becomes invalid, PCS transmitter will be automatically used for PSS duty to prevent any process shut-down. Specific MMI representation and report are described within the corresponding Standard Function.

8.4 Maintenance inhibition

8.4.1 General points

Access level: MAINTENANCE.

The consequences of maintenance inhibition are specified individually in each Standard Function.

The maintenance inhibition is classified as a level 0 alarm/event.

Report and dedicated display shall be generated periodically and upon operator request showing all current inhibitions, including packages ones.

8.4.2 Process instrument

Maintenance inhibition of the process transmitters (PCS) leads to the inhibition of all corresponding thresholds. Therefore, only one command is necessary.

8.4.3 Safety instrument

Activation of maintenance inhibit will defeat the safety logic relevant to this input.

When several thresholds are used in the safety logic diagram, each threshold shall be individually inhibited.

8.5 Start-up inhibition

Access level: OPERATOR or performed automatically.

The purpose of this command is to allow the temporary inhibition of some inputs in ALARM, in order to defeat the safety logic and reset the associated safety bar (e.g.: low pressure safety threshold at the pump outlet).

The start-up inhibition function is described in detail within the Safety Bar Standard Function.

8.6 Maintenance commands

Report and dedicated display shall be generated periodically and upon operator request showing all current isolating, maintenance input trip and test commands.

8.6.1 Specific equipment Test

Access level: Maintenance

Test command shall be available for testing specific equipment (e.g. fire extinguishing skids, safety valves, deluge valves control circuits).

Details are given within each Standard Function.

8.6.2 Maintenance input trip

Access level: Maintenance

Such function will be implemented for all detectors used in voting logic (e.g. gas detector). The purpose is to maintain the integrity of the safety function while working on one detector (for calibration for instance).

When the maintenance input trip is active for one detector, the corresponding input of the voting logic will be forced to fault status, so that the logic will process healthy detectors only.

8.7 Safety bar Isolating

Access level: Engineer

Isolating facility will be implemented in each safety bar function. This shall primarily be used as a commissioning tool. This functionality shall also be reviewed to assist in testing and verification of software modifications, which may be required during the operating life of the facilities. This function should be removed at the end of this stage.

9. List of Standard Functions

This list has not to be considered as exhaustive; refer to the scope of this document (§1)

LIST OF STANDARD FUNCTIONS				SUB-FUNCTIONS			
GS INS	NAME	Option	Description	PCS	PSS	ESD	FGS
151	DI		Digital input without alarm	X	X		
		_AL	Digital input with alarm	X	X	X	X
152	DI-LM		Line monitored digital input		X	X	X
153	AI		Process analogue input	X			
154	AIS		Safety analogue input		X	X	X
155	RAI		Redundant analogue inputs	X	X		
159	DO	_D	Digital output logic (De energise to trip)	X	X	X	X
		_E	Digital output logic (Energise to trip)	X	X	X	X
160	HIC		Analogue output command	X			
161	PID		PID controller	X			
		_MR	cascaded PID controllers (master)	X			
		_SR	cascaded PID controllers (slave)	X			
		_SPR	split range PID controller	X			
		_RD	PID controller with redundant valves	X			
		_ON/OFF	PID controller with flip/flop analogue output	X			
		_1DC	PID Controller with a digital output	X			
162	GCF		Pressure / temperature compensated flow (linear)	X			
		_SQ	Pressure / temperature compensated flow (square root extraction)	X			
163	TOT		Total flow (daily)	X			
		_AV	Average flow (daily)	X			
165	MOT		Low voltage motor and High voltage motor with fuse contactor ($P \leq 1500$ kW)	X			
		_BK	High voltage motor with circuit breaker ($P > 1500$ kW)	X			

LIST OF STANDARD FUNCTIONS				SUB-FUNCTIONS			
GS INS	NAME	Option	Description	PCS	PSS	ESD	FGS
		_ST	Status monitoring only	X			
167	PU	_CENT	Centrifugal pump unit	X			
		_CENT_1SDV	Centrifugal pump unit with SDV	X			
		_CENT_1XV	Centrifugal pump unit with discharge valve (XV)	X			
		_CENT_2XV	Centrifugal pump unit with suction and discharge valves (XV)	X			
		_RECIP	Reciprocating pump unit	X			
169	D/B /S		Duty/backup/standby	X			
170	XV		XV (ON-OFF process valve) with 2 limit switches	X			
		_2B	XV with 2 digital outputs and 2 limit switches	X			
171	HV		Manual valve with 2 limit switches	X			
172	SDV		Safety control SDV with 2 limit switches		X		
173	ESDV		ESDV(emergency shutdown valve) with 2 limit switches			X	
174	BDV		BDV (blow down valve) with 2 limit switches			X	
178	SBAR		Safety bar		X	X	X
180	GD		Point gas detection				X
181	GDB		Infra-red beam gas detector				X
185	RD		Flame detector				X
186	RDH/RDIS		Heat / Smoke detector				X
190	DELUGE		Deluge system (without foam)				X
		_F	with foam				X
		_Water curtain	Water curtain system				X
191	fire Ext.		Fire extinguishing system logic				X
195	2ooN		Two out of N voting logic		X	X	X