

Table of Contents

1	General	2
2	Scope	2
2.1	Terminology	2
2.2	Application Area	2
2.3	Control System Integration Process	2
3	Functional Requirements	3
3.1	Full Equipment Control by FEC during Regular Operation	3
3.1.1	Start Activities by FEC	3
3.1.2	Provide Information on States and Activities to FEC	4
3.1.3	Verification of Equipment Operation	4
3.1.4	Parameterization of Equipment	5
3.1.5	Communication Behavior and Responsiveness	5
3.1.6	Equipment Reset	6
3.1.7	Local Operation	6
3.1.8	Power-Up Notification	7
3.1.9	Notion of Time	7
3.2	Support Beam-Multiplexing Operation	8
3.3	Equipment Protection and Equipment Interlocks	8
3.4	Equipment Warnings	9
3.5	Service Access to Equipment Interface	9
4	Attached Documents	10
5	Related Documentation	10

1 General

Almost all accelerator equipment (e.g. power converters, RF systems, beam diagnostic systems, vacuum valves and pumps, etc.) is connected to the GSI/FAIR Accelerator Control System to be remotely controlled or at least monitored.

Several types of interfaces are supported to connect equipment to the Control System. Electrical and mechanical aspects of the interfacing, like connector types, layout of connector pins, voltage levels, and signal shapes as well as mechanical outline are addressed in [2].

However, only fixing the electrical and mechanical parameters is not sufficient. Seamless integration in the controls environment further requests a basic functionality to be supported by the equipment. In addition to [2], this document focuses on the functionality equipment has to provide for seamless integration into the control system.

2 Scope

2.1 Terminology

The control system corresponds to work package 2.14.10 in the FAIR project. It is comprised roughly of the full electronics, hardware and in particular common software infrastructure base for all accelerators and beam-lines of FAIR and GSI that are needed to control, commission, run and operate the GSI/FAIR accelerator complex.

In the context of the control system, accelerator **Equipment** is the umbrella term for all physical systems to be controlled and/or monitored by the control system which is needed to facilitate the production and delivery of beam to the designated destinations.

An **equipment supplier** is whoever develops and/or provides equipment under the terms stated above.

The **control system supplier** is responsible for the development and delivery of the FAIR work package 2.14.10 (technical subsystem "control system"). The **FAIR control system coordinator** will be responsible for the technical follow-up of the work package 2.14.10, taking care of technical and organizational coordination between equipment and accelerator control system supplier(s).

2.2 Application Area

This guideline holds for all equipment which is controlled or monitored by the control system by dedicated **Front-End Controllers (FEC)**, as described in [2]. Design and construction of such equipment must ensure to provide the functionality as specified in this document.

2.3 Control System Integration Process

Providing a detailed description, strictly fixing all functional aspects, would be far to rigid to cover all potential usage of equipment in the accelerators. Therefore functional aspects are specified only on a rather general level. This guideline has to be taken more as a check list than as detailed instructions for equipment development.

It is absolutely mandatory to contact the control system coordinator to check for compliance to the needs of the control system when design or purchase of equipment is started.

3 Functional Requirements

Equipment in the accelerator is connected to the control system by a local Front-End Controller (FEC), supplemented with optional control system front-end hardware like an interface to the timing system (see [2] and [1]). The front-end controller runs the FESA front-end control software, sometimes supplemented by hardware-implemented basic control functions like ramp generation. Supported FEC types are specified in the FAIR technical guideline [2].

3.1 Full Equipment Control by FEC during Regular Operation

The control system implements a strict top-down control strategy. FECs are the master for the equipment. This implies that set-up of equipment, providing set-point data and start of activities are handled by the FEC. Respectively, the FEC needs access to all actual data and must be able to monitor states and activities of the equipment.

However, intrinsic equipment control functionality like internal close-loop controls in general don't need to be under control of the FEC.

3.1.1 Start Activities by FEC

Activities in the equipment which are relevant to the operation of the accelerators must be initiated by the FEC of the control system.

However, some activities like handling of fault conditions are to be handled autonomously by the equipment. Moreover, in specific cases it may be unavoidable to start actions in the equipment not by the FEC, but e.g. by external trigger signal inputs.

The top-down control strategy results in:

- Activities in the equipment, like setting a power converter to another current (set to another setpoint-value) or starting a beam diagnostic measurement must be initiated by command from the FEC.
- Start of activities in the equipment by external triggers, e.g. by signals directly decoding signals from the timing system, shall be avoided whenever possible. They are tolerated only if there are substantial reasons and must be limited to specific tasks.
- When start of activities in the equipment by external trigger signals cannot be avoided, the FEC must be able to
 - control the use of the external triggers. The FEC must be able to enable and disable external trigger inputs,
 - detect the occurrence of a trigger (see section 3.1.2),
 - generate (simulate) external trigger signals for testing and diagnostic purposes if possible.
- Autonomous activities (not under control of the FEC) which change the behavior or state of the equipment are limited to interlock handling: detecting faulty states and switching the equipment to a safe state (see section 3.3). The equipment must provide the occurrence and the reason of the equipment interlock to the FEC (see section 3.1.2 and also [3]).

3.1.2 Provide Information on States and Activities to FEC

FECs must be able to monitor and track what is happening in the equipment. This includes equipment activities as well as internal states of the equipment.

Equipment must provide all information on states which are relevant for accelerator or equipment for operation. As a minimum, the following state information must be provided to the FEC:

- Power status (on/off), separately for all parts which can be switched on/off independently. While performing power-up or power-down sequences equipment must not signal power on.
- The control system must be able to determine when the equipment is fully operational, which is power-on and ready for operation. When equipment is ready for operation after power up, providing only power-up information will be sufficient.
- Control system access. The control system must be able to sense when equipment or part of it is under local control (see section 3.1.7).
- Equipment interlock condition occurred (see section 3.3).
 - In case of an equipment interlock condition, equipment must provide detailed information about the cause of the interlock condition.

Additional state information is often required to allow monitoring of the equipment:


- Equipment should provide state information which allows checking proper behavior of the equipment during regular operation.
- For all activities which are not directly initiated by the FEC, equipment must provide information that the activity has started (e.g. external trigger received).
- For equipment activities which are lasting either rather long or when its duration may vary, equipment must provide information when the activity has ended. As a rule of thumb, this holds for activities which extend, or may extend, a time of about 1 ms. However, depending on the application, in accordance with the control system coordinator, often much longer times can be tolerated. Examples for long lasting activities are
 - Power-up or power-down sequence has finished,
 - Data collection process, e.g. integration of a signal, is completed.

Preferably, state information should be provided as bit pattern in status registers which can be read by the control system.

3.1.3 Verification of Equipment Operation

Equipment in the accelerator must provide adequate means to allow for checking correct operation in the facility. Equipment must at least provide actual data for all output signals which are relevant for beam production. Analysis of output signals provides a good check for equipment operation, covering the full chain from data generation, front-end control and equipment itself.

- Equipment must provide actual data for all relevant equipment outputs. Such actual data should allow verifying proper operation of the equipment.
- Actual data must be available with adequate rate for the fastest proposed use.
- Equipment must provide reading of setpoint values by the FEC.
- In case setpoint values provided by the FEC are modified by dedicated external feedback systems (e.g. magnetic field regulation or closed orbit feedback system acting on beamline

	<h1>Technical Guideline</h1>	Number	F-TG-C-04e
Controls Department	<h2>Equipment Functional Requirements</h2>	Status	Version 3.0 03. Aug. 2012
<p>magnet power converters) within the equipment, the equipment must provide adequate means to the FEC to read-back such correction values or modified setpoint values. The need for this function shall be resolved with the accelerator control system coordinator.</p> <ul style="list-style-type: none"> Equipment should provide diagnostic data to check internal functionality. <h3>3.1.4 Parameterization of Equipment</h3> <p>Equipment often needs to be specifically adjusted or to be configured during set-up. Such specific settings must be known to the accelerator control system. In addition to adjustment and configuration the revision state of the equipment must be accessible by the FEC.</p> <ul style="list-style-type: none"> Configuration of equipment preferably should be done by the control system. Parameterization data should be set by the FEC. In case adjustment and parameterization are done by other means, equipment must provide configuration data to the control system. FEC must be able to read such configuration data. Equipment must provide revision information to the FEC. Especially when firmware can be updated in the equipment, information on the firmware version must be provided. <p>Parameterization and initialization of equipment is often not hold permanently in the equipment and being lost or potentially corrupted when power goes down. In such cases, it is vital that occurrence of a power-down condition can be reliably detected (see section 3.1.8) to renew the settings.</p> <h3>3.1.5 Communication Behavior and Responsiveness</h3> <p>The master / slave relation between FEC and equipment implies:</p> <ul style="list-style-type: none"> Equipment must be able to receive commands from the FEC at any time. In particular, equipment must provide full state information at any time when requested by the FEC. Dropping a request from the FEC cannot be tolerated in any case. <ul style="list-style-type: none"> At least the information that a command momentarily cannot be executed must be provided. The FEC must be able to detect when equipment cannot execute a command which is sent by the FEC (equipment must provide means that the FEC can check when it has sent an erroneous command). Equipment must response to requests from the FEC without delay. Tolerable response time depends on application area. As a rule of thumb, reaction to a command must be completed well below 1 ms. If reasonable short times cannot be assured, then: <ul style="list-style-type: none"> Split the read request in two commands: initiate request command and read result commands. Equipment must indicate that the result to a request can be read. <p>State information can be read from the FEC by request. State change may also be indicated by interrupt. Both mechanisms cannot track rapidly changing state information. As a rule of thumb</p> <ul style="list-style-type: none"> To detect a state change by request (polling), the state information must be stable for at least 10 ms. In case of reporting state changes by interrupt, interrupt rate should be below 100 Hz. Anyhow, state information must be stable until it is evaluated by the FEC. 			
Prepared by:	R. Bär	Doc. Name:	F-TG-C-04e_Control-System-Equipment-Functional-Requirements_v3.0.pdf
Date:	2011-05-27	Version:	3.0
Page 5 of 10			

- For higher rates of state changes, equipment must provide at least some summary information.

For rapid changes of state, which can not be reliably tracked neither by polling nor by interrupts, summary information must be provided. Two strategies are suggested:

- State changes must be latched by the equipment for later read-out by the FEC. A common mechanism for state information, represented by one bit, is:
 - Set the bit when the state information occurs. Further changes in the state keep the bit set.
 - Provide a command to reset the bit. Such a clearance can be combined with the state read-command (clear the bit when it is read by the FEC).
- Provide a counter, increased every time the state is set, for read-out by the FEC. Provide a flag (status bit) indicating a non-zero counter.
 - Capability to reset the counter by the FEC must be provided.
 - When possibility of counter overflow cannot be excluded, means must be provided that the FEC reliably can detect the overflow.

3.1.6 Equipment Reset

The control system must be able to set equipment to well defined initial state (start-up conditions) in all cases. This implies:

- Equipment must provide reset functionality to the FEC.
- FEC must be able to abort ongoing activities in the equipment. This includes stopping timers, abort switching sequences, and other ongoing activities.
- Reset should preferably be implemented as a single reset command. Splitting reset functionality to several commands is also possible if there are substantial reasons

The FEC needs to know when the equipment reset is completed. This implies:

- When equipment completes the reset-action in short time (as a rule of thumb within 1 ms), confirmation of the reset-action is encouraged but not strictly requested.
- When reset-action in the equipment takes longer, the equipment must provide means that the FEC can detect the end of the reset action.

3.1.7 Local Operation

Equipment installed in the facility will be remotely operated by the control system only. However, during maintenance it should be possible to operate equipment by other means. To clarify the terminology of the accelerator control system:

- Equipment is remotely controlled (in the **remote** control state) when it is controlled by the accelerator control system FEC.
- Equipment is locally controlled (in the **local** control state) when it is controlled by other means than by the accelerator control system FEC. Local control can be by front-panel knobs and switches as well as by control channels other than the accelerator control system.

When local control is possible:

- Equipment must implement explicit switching between remote control by the control system and local control.

- Equipment must present to the FEC when equipment is in local control state. Information can be presented as bit in a general status register.
- During local control, equipment should support read access by the FEC to further state information and data like actual values. It is expected that write access by the FEC is disabled.
- In case of remote control, any local operation which may change the state or setting of the equipment must be blocked, with the exception of switching the equipment to local operation. Read access is possible when interference with the control system is excluded.
- Providing control channels in parallel to the control system (control by the FEC) needs explicit clearance by the control system coordinator.
 - Sufficient precautions must be taken to exclude accidentally switching to local control during regular operation of the accelerators.

3.1.8 Power-Up Notification

Modern equipment often is highly configurable and needs specific set-up information. It is even possible to constitute equipment functionality at start-up by loading EPLD settings. It must be assured that such settings are restored when they are lost.

If equipment depends on specific settings:

- Equipment should hold its settings permanently, also when power goes down.
- When equipment settings can be lost or corrupted during power-down and have to be restored at power-up by the control system, it is mandatory:
 - Equipment must reliably notify the FEC about a power-down condition, which means the FEC is to be notified when power-up is detected.
 - Since even very short power-down drops can lead to loss of configuration data, equipment must be able to detect even short power-down conditions.
 - Any power-up information must be latched by the equipment until it is explicitly cleared by the FEC.
 - Power-up must be signaled if power-up is detected at least for one component in case of compound equipment, consisting of multiple parts.

3.1.9 Notion of Time

Equipment is often equipped with internal clocks, displaying the time of day. To achieve coherent time information all over the accelerator facility, equipment shall use the same notion of time as the accelerator control system.

- Equipment which has its own internal clock must ensure that such internal clock is set to the time base of the accelerator control system.
- Equipment must provide appropriate means for clock time adjustment to synchronize with the time base of the accelerator control system.

The control system will distribute the time base by the timing system, provided by FEC and by timing receivers, and with reduced accuracy by NTP on the communication network.

3.2 Support Beam-Multiplexing Operation

The GSI/FAIR facility will support several experiments in parallel which may use different beams. Many areas of the facility will be switched between different beams from cycle to cycle. Equipment must be designed to support such beam multiplexing operation.

All equipment which takes part in beam production or beam diagnostics and will be operated in multiplexed mode must be designed such that:

- Equipment must react to new set point values and perform data acquisition fast enough to follow beam switching for all proposed operation modes.
- Equipment must be fast enough to handle every successive beam pulse. Therefore shared elements, time multiplexed between different pieces of equipment, must not be used.
- Equipment must not be limited in the total number of setpoint value changes (multiplexing changes). Beam multiplexing operation must not use mechanical elements like relays with limited number of switching cycles.

3.3 Equipment Protection and Equipment Interlocks

The control system will account for reliable operation of the equipment under control as well as for the facility as a whole. However, the control system cannot take strict responsibility to exclude harm of the connected equipment. Therefore equipment must be built intrinsically safe, monitoring its functionality and its vital environment conditions by itself.

An equipment interlock is an asynchronous condition usually resulting from an equipment internal fault (abnormal behavior). In addition, external signals like safety shutdown signals might also lead to equipment interlocks. Equipment must detect and handle interlocks autonomously.

- Equipment must detect equipment interlocks autonomously by monitoring potential dangerous conditions. Detection of equipment interlocks is an intrinsic activity of the equipment which must not depend on explicit action by the FEC.
- Detection of equipment interlock must autonomously lead to a safe state of the equipment which must not depend on explicit action by the FEC.
- Equipment interlocks must require explicit acknowledgement (interlock reset) before resuming normal operation. Equipment must not resume operation autonomously when the cause of the equipment interlock is no longer present.
- Equipment must provide interlock reset functionality for the FEC. Resetting equipment interlocks by a general equipment reset function is sufficient.

While equipment must detect interlock conditions autonomously, including setting the equipment to a safe state, the accelerator control system needs to be notified. Equipment must provide detailed information about the cause of the interlock (interlock conditions).

- Equipment must provide summary interlock conditions to the interlock system as specified in [3].
- Equipment must provide detailed information about the cause of the interlock (the interlock condition) to be read by the FEC. Typically, the various interlock conditions are coded as bits in state registers.
- Interlock conditions must be latched by the equipment. Clearing notification on interlock conditions must be done by an explicit reset command only.

3.4 Equipment Warnings

Equipment interlocks will usually stop all accelerator operation which makes use of the respective equipment. Often shutting down accelerator operation can be avoided by taking early action. As an example, notification when temperature of cooling water is well above the normal level (but not yet critical) allows to take preventive action in case of slowly rising temperature of cooling water.

- Equipment should not only handle interlock conditions but should notify on warning conditions.
- A warning condition indicates states which are not yet critical but well apart from normal operational states. A warning condition does not trigger an equipment interlock.
- Notification on warning conditions to the FEC is similar to interlock conditions:
 - Warning conditions may be indicated by bits in state registers
 - Warning conditions are latched in the equipment. Equipment must provide reset functionality to the FEC.
 - Reset of warning condition notification must be possible other than by general equipment reset.

3.5 Service Access to Equipment Interface

To monitor the status of the facility, the control system needs access to the equipment also during maintenance periods, requesting that at least the interfacing electronics is powered.

- The equipment controls interface shall be powered independently from the power part of the equipment if possible. Thus, the control part can be still powered even if the power part of the equipment is switched off.
- It is strongly encouraged to provide means in the equipment to safely switch off the power part of the equipment, excluding potential harm for personnel working in the facility, while still keeping the equipment's control interface powered. The FEC should have read access to the equipment.

Maintenance of control system installations should be possible by personnel which are not specifically trained for the respective equipment (e.g. not familiar with equipment specific safety regulations).

- When control system components are installed as part of the equipment, access to these components must be possible for personnel which are not specifically trained for the equipment. For maintenance on the control system components any hazard by the equipment itself (e.g. electrical power parts) must be excluded.
 - Independent cabinet or crate doors for control system components and power parts of the equipment are strongly encouraged.
 - Equipment must provide means for control system maintenance personnel to safely switch off power of control system components. Therefore decoupled power supplies for interfacing electronics, including accelerator control system components, and for the equipment's power parts are strongly recommended.

4 Attached Documents

List of abbreviations for controls (Abbreviations_Controls.pdf).

5 Related Documentation

- [1] F-TG-C-01e, Technical Guideline "Ethernet Network Connectivity"
- [2] F-TG-C-02e, Technical Guideline "Control System Equipment Control Interfaces"
- [3] F-TG-C-03e, Technical Guideline "Control System Equipment Interlock and Status Signal Interface"