NUCL SCI TECH (2021) 32:39
https://doi.org/10.1007/s41365-021-00875-1

Design of a personnel safety interlock system for proton therapy

Shou-Yuan Wang[1,2,3] · Yun-Tao Song[1,3] · Han-Sheng Feng[1,3] · Shi Li[1,3] · Hai-Lin Cao[3] · Jing Zhang[3] · Ou-Wen Huang[3] · Zhu Li[3]

Received: 9 November 2020 / Revised: 4 February 2021 / Accepted: 19 February 2021 / Published online: 17 April 2021

Abstract Proton therapy is the most advanced radiotherapy approach in the world, and causes less damage to normal human tissue than traditional radiotherapy. Because the treatment process produces a high-energy proton beam, the personnel safety interlock system mainly considers measures to protect personnel from radiation hazards during beam preparation and the beam release process. Unlike other safety interlock systems, the personnel safety interlock system designed in this study focuses on the safety and stability of the system itself. The hardware and software of important interlock control loops are designed and developed according to the requirements of Safety Integrity Level 3 specified by IEC61508. A set of redundant ring networks was developed to ensure that damage to a certain network line does not affect the normal operation of the system. A set of friendly operation interfaces and data storage systems were developed to ensure that the operator can monitor the data in real time and trace the data. The personnel safety interlock system mainly includes a beam enabling function, clearance function, and emergency stop function. The system was put into actual use and successfully ensured personnel safety.

Keywords Personnel safety · Radiation protection · Interlock system · Safety integrity levels

1 Introduction

Compared with other radiotherapy methods, proton therapy has the advantages of a better dose distribution and higher local dose. Clinical treatment data show that the 5-year survival rate is as high as 70% [1]. The proton therapy system includes an accelerator system, an energy selection system, a beamline system, and a treatment room. A high-energy proton beam is generated by the accelerator, adjusted to a pre-set energy level by the energy selection system, and then transmitted to the treatment room by the beam line system to treat the patient tumor.

A superconducting cyclotron was developed and built by the Hefei proton therapy project with an energy level of 200 MeV and a beam current of 400 nA. During the system operation, along with high radiation fields, measures need to be taken to ensure the safety of on-site workers. Based on radiation safety and the reliability requirements of the interlock system, in this paper, the design and development of a personnel safety interlock system (PSIS) depending on the safety requirements of IEC 61508 is introduced. The safety integrity level (SIL), a key concept in functional safety standards, is a performance metric used to measure the reliability of safety systems that conduct specific safety functions [2]. The SIL is widely used in high-risk industries, such as the nuclear, petroleum, chemical, and steel industries. In the system design stage, the SIL design must be carried out at the hardware and software levels to ensure that the entire control loop meets the safety requirements. The system safety that satisfies the SIL is mainly embodied

✉ Han-Sheng Feng
hansheng.feng@hfcim.com

[1] Institute of Plasma Physics, Chinese Academy of Sciences, Hefei 230031, China

[2] University of Science and Technology of China, Hefei 230026, China

[3] Hefei CAS Ion Medical and Technical Devices Co. Ltd, Hefei 230088, China

in two aspects. On the one hand, it has a lower probability of failure, and on the other, it has a series of failure protection measures in the event of failure. SIL1, SIL2, and SIL3 are commonly used SIL levels. The higher the level is, the higher the safety factor [3]. In this project, because proton therapy is a high-risk industry, its personnel safety interlock system needs to meet the application requirements of SIL3. Some of the terms used to describe the safety level of the control loop are listed below, and Table 1 shows the criteria correspondence between PFDSIF and SIL:

PFDS: average failure probability on sensor demand.

PFDL: average failure probability on logic controller demand.

PFDA: average failure probability on actuator demand.

PFDSIF: average failure probability on safety interlock function demand.

PFDSIF = PFDS + PFDL + PFDA.

In PSIS, the main functions are the beam enable function, clearance function, and emergency stop function [4]. The key control loop of the interlock function, such as the beam enable function and emergency stop function, meet the requirements of SIL3. In addition, a friendly graphical user interface (GUI) was developed for operators to remotely monitor the safety system.

There are two treatment rooms in the project, and the workplace depending on the radiation intensity is divided into a control area and a supervision area to meet the requirements of the China National Standard GB18871-2002 (basic international standards for protection against ionizing radiation and for the safety of the radiation sources) [5]. The control area is shown in the dotted area in Fig. 1, and focus needs to be on radiation safety management.

2 System requirements

According to the requirements mentioned in the introduction to ensure the radiation safety of personnel in the control area, the safety interlock system of proton therapy personnel mainly needs to consider the safety requirements of the system from two aspects: readying the beam release and the actual beam release itself. During the preparation of the beam release, it is necessary to consider the possible radiation risks of workers and take necessary measures to avoid these risks, and in the process of beam release, measures should be taken to shut off the beam in time to prevent or reduce the harm caused by radiation.

Table 1 Correspondence between PFDSIF and SIL

SIL	PFDSIF
4	$\geq 1.00 \times 10^{-5}$ to $< 1.00 \times 10^{-4}$
3	$\geq 1.00 \times 10^{-4}$ to $< 1.00 \times 10^{-3}$
2	$\geq 1.00 \times 10^{-3}$ to $< 1.00 \times 10^{-2}$
1	$\geq 1.00 \times 10^{-2}$ to $< 1.00 \times 10^{-1}$

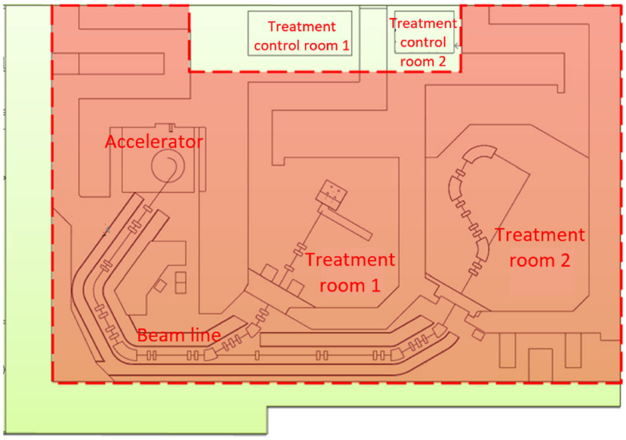


Fig. 1 (Color online) Control and supervision areas

Therefore, it is necessary to arrange a large number of interlock devices to collect field data and use the controller to process the data. To realize the safety function, it is necessary to select the hardware according to the requirements of the safety interlock system first, and then arrange the devices in various areas of the site. Next, it is necessary to carry out safety programming in the controller and collect real-time data of the devices through the controller. In addition, a GUI was developed to remotely monitor the key parameters of the interlock system [6].

2.1 Beam enable requirements

The interlock system requires a series of measures to confirm the beam-enabled conditions before the beam is released, and attempts to avoid the risk of radiation accidents. Therefore, the requirements for enabling a beam release are as follows:

1. A series of measures are needed to confirm that no personnel are within the radiation area before the beam is released to prevent injury in such personnel from the radiation [7, 8].
2. It is necessary to confirm the states of all emergency stop interlocks on site, and that all emergency stop interlocks have been reset.
3. Radiation monitoring equipment must be ready to confirm the radiation status of the site.

4. To avoid an accidental operation of the beam, a key switch should be set in the control room to confirm the beam-enabled condition.
5. It is necessary to confirm the states of the interlock system itself, and the interlock system should be opened and operated normally.

2.2 Interlock requirements of emergency stop

During the process of beam release, it is necessary to consider the risk of workers staying in the radiation area or entering the radiation area by mistake, and a series of measures should be taken by the safety interlock system to stop the beam. The requirements of the emergency stop interlock are as follows:

1. If an emergency occurs during the beam-out process, the personnel in the control or supervision areas can press the emergency stop button to stop the beam.
2. During the beam release process, a beam stop interlock is required to detect whether the clearance door is open.
3. During the beam release process, if the interlock system fails, a beam-stop interlock is required.

2.3 Device requirements

Hardware is needed to realize the software function of the beam enabling and emergency stop interlock. A controller is needed to realize the interlock logic, and a field sensor is required to collect the field signals.

1. A controller is needed to implement the safety interlock program, and a series of input and output modules are required to monitor and control the safety equipment [9].
2. The safety system needs to know whether the area dose has been exceeded, and it is therefore possible to arrange the radiation monitoring equipment in the control and supervision areas to monitor the radiation dose.
3. To prevent people from staying in the site when the accelerator is running, clearance buttons and clearance doors must be arranged in the control area. The interlock system needs to monitor the clearance button and the position switch signal of the clearance door for the personnel in the control area to clear the site before leaving the field. Sound and light alarms are required during the process to remind us that the site is currently being cleared.
4. Emergency stop buttons need to be arranged in the control and supervision areas for interlock protection under emergency conditions, and the personnel safety interlock system needs to monitor whether the emergency stop button has been pressed.
5. To prevent the accelerator from being turned on accidentally, a key switch for the accelerator beam needs to be set in the supervision area, and the personnel safety interlock system needs to collect the signal of the key switch for the interlock logic.

2.4 System safety requirement

The system includes two parts: hardware and software. To meet the safety requirements of the safety interlock system and enable the system to operate safely and stably [10], it is necessary to select safety devices and ensure safe communication. It is also necessary to select appropriate programming software for the safe programming of the key program blocks.

1. In the hardware selection, it is necessary to fully consider the system safety. For the key safety interlock function, it is necessary to select the controller and sensor meeting the SIL3 level according to the requirements of the safety standard. For a general logic function, a normal device is simply needed.
2. In software programming, it is necessary to apply a program according to different security levels. The security program needs to use the program block of the security program library, and the general program uses the program block of the general program library.

2.5 Interface requirement

Users need to obtain the safety interlock parameters conveniently and quickly, and judge whether the current beam output conditions have been met or whether there is an interlock trigger. Therefore, a friendly interlock interface is required. The system states can be monitored at the interface, and the state history can be queried. The specific requirements are as follows:

1. It is necessary to remotely monitor the main safety signals, such as the radiation value of the area, area clearance states, emergency stop states, and beam enable states.
2. It is necessary to trace the historical information. In the case of an emergency stop, it is necessary to determine the cause of the fault for maintenance.

3 Design principles

Considering the safety and reliability, the overall design of PSIS adopts a control loop that meets the SIL in the design of an important interlock control loop [11], as shown in Fig. 2.

The interlock control loop represents a complete control link, including the sensor used to monitor the field status, the signal acquisition module, the logic processing module, the signal beam output module, and the actuator to execute the interlock command. In the SIL3 control loop, the device selected, hardware wiring, and communication methods all need to meet SIL3.

Programs with low safety levels are called general programs, and programs with high safety are called safety programs. Their programming is relatively independent, each of which having its own set of program libraries that meet the safety requirements.

General procedures typically apply general sensors and actuators, and safety equipment uses safety sensors and actuators to meet the SIL requirements. The general program and the safety program operate together in the safety controller, although the controller distinguishes two programs and runs them in different processing layers [12].

The difference between safety hardware and general hardware lies mainly in two aspects: failure probability and failure protection. Manufacturers will test the failure probability of the safety hardware in a specific environment. The lower the failure probability, the higher the reliability and the higher the SIL level. When the safety sensor fails, it can send a fail-safe signal to the controller, and the controller can generate an interlock to protect the safety of the personnel. When the safety controller fails, it can send a fail-safe signal to the actuator, and the actuator can generate interlocking actions to protect the personnel. When the safety actuator fails, it interlocks to protect the safety of the personnel. General hardware only needs to perform routine inspections and does not need to test the failure probability. It is generally only used for process control and does not trigger an interlock action when it fails.

The safety software was programmed in the safety logic controller to match the safety sensors and safety actuators. Hardware devices that meet SIL3 are generally redundant. The safety program can determine whether the interlock protection program will be triggered according to whether the redundant circuit is abnormal. However, safety programs are fail-safe. When there is an abnormality in the controller device or communication, or when a power failure occurs, a fail-safe signal is sent to the actuator to generate interlocking actions to protect the safety of the personnel.

General software is only used for process control, with a lower security level, such as field clearance control and alarm light control, and when such software fails, there is no effect on personnel safety, and thus no corresponding failure protection measure is required.

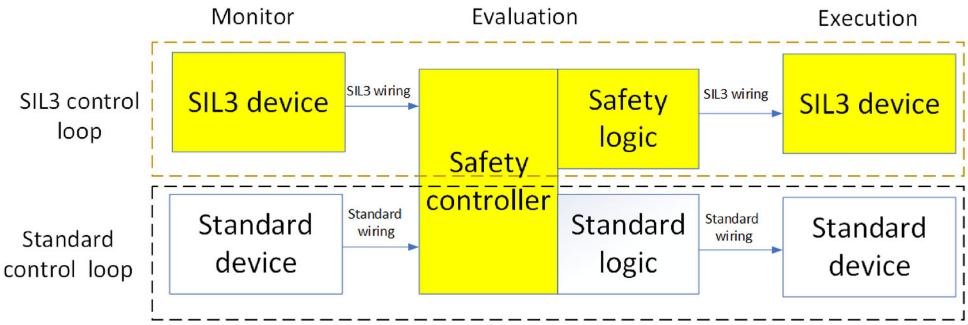
Consider an emergency stop when the area is cleared as an example. After the area is cleared, the door position switch monitors whether the interlock door is opened. If the interlock door is opened, it sends an interlock signal to the controller, and the controller executes the beam-off command. If the cable of the door position switch is disconnected, the controller will detect the abnormality of the door position switch and execute the beam-off command. When the controller fails, the fail-safe is activated, and the relay receives the fail-safe signal and executes the beam-off command. When the relay fails, it will also activate the fail-safe system to shut off the beam.

4 Architecture design

To realize a personnel safety interlock system, the system architecture was first designed. This system is divided into four layers according to their functional characteristics: the display, data service, function, and device layers [13], as shown in Fig. 3. In the architecture, the safety and general parts are distinguished. The yellow background in Fig. 3 is the safety part, which is designed based on SIL3.

The display layer is the GUI of the PSIS, which runs independently in the control room, and is only used to

Fig. 2 Control loop



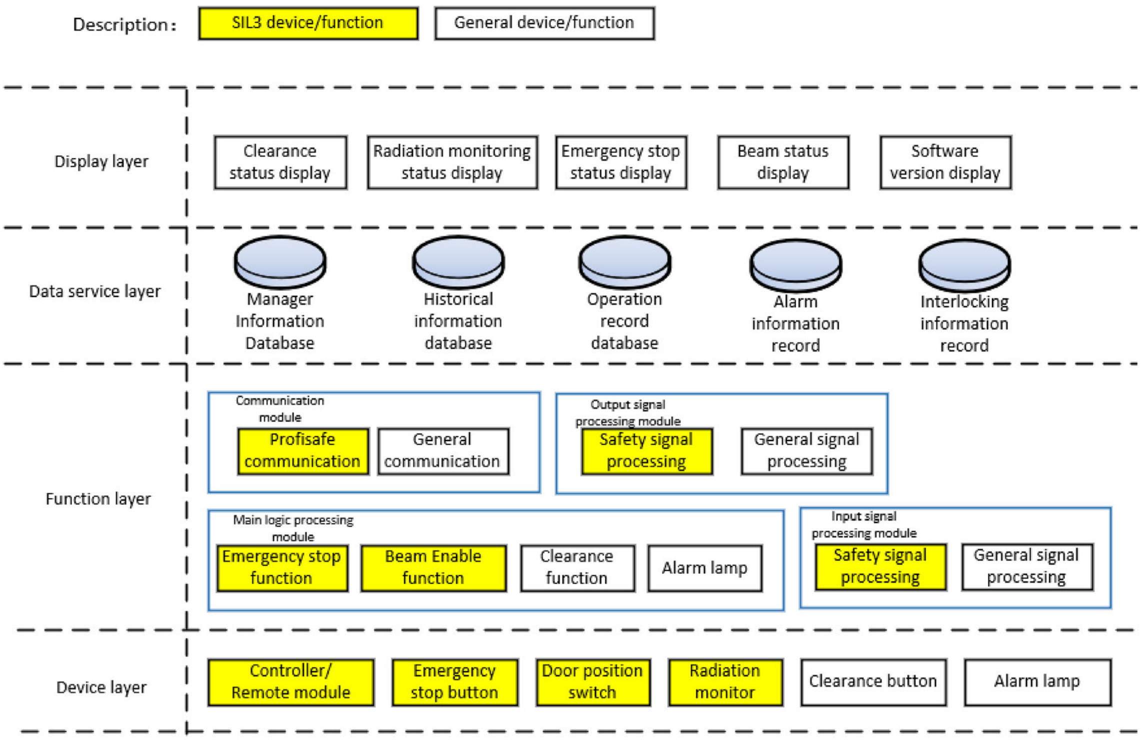


Fig. 3 System architecture

display the state. When the GUI fails, the program will still be executed in the underlying controller without affecting the safety program. The GUI includes the clearance information, radiation monitor information, emergency stop information, and beam ready/release information. The operator can easily obtain the system operation information from the GUI and proceed to the next step.

The main function of the data service layer is to store historical data, including manager information, historical data information, operation records, alarms, and interlock information. The data service layer of the safety interlock system archives and records all information generated during operation, such as radiation monitoring system operation records, emergency stop button information, site clearing information, site clearing door switch states, and enabled key switch states. When needing to retrieve data for analysis, operators can extract storage information from the database.

The logic of the personnel safety interlock system is realized in the functional layer, and the PSIS consists of four main functional modules: the communication module, input signal processing module, main logic processing module, and output processing module [14]. In each function module, the PSIS distinguishes between the safety functions and general functions. The safety program uses the safety function block, which can self-check the input signal, internal communication, and output signal of the program. When the self-inspection is abnormal, the interlock command is executed. The safety functions include PROFIsafe communication, safety signal processing, an emergency stop function, and a beam enable function. A safety library that satisfies SIL3 with a series self-check functions is included in the safety controller programming platform. The safety program was developed using programs of the safety software library. The general function is the general action flow because the auxiliary program of the safety system does not directly participate in the interlocking process, and sound and light alarms or necessary logic signals for the safety program are provided on-site. General functions include general communication, general signal processing, a clearance function, and an alarm lamp function.

The device layer also distinguishes general and safety devices according to the actual application requirements. SIL3 devices were selected as the key interlock control loop hardware. As the main difference between the SIL3 device and the general device, the failure probability is lower; however, when the equipment fails, it can send safety signals to trigger an interlock. The safety devices include an interlock controller, emergency stop button, and door position switch to conduct an interlock function with a high level of safety. General equipment includes a clearance button, alarm lamp, low security level logic, or alarm function.

The average failure probability on the demand of the safety control loops is shown in Table 2, and the

Table 2 Safety interlock function PFD

No	Safety loop	Sensor	PFDS	Controller	PFDL	Actuator	PFDA	PFDSIF
1	E-stop button function	Emergency stop button	1.00×10^{-8}	F-CPU	1.00×10^{-5}	Relay	1.43×10^{-4}	1.53×10^{-4}
2	Clearance destroyed function	Door position switch	2.50×10^{-8}	F-CPU	1.00×10^{-5}	Relay	1.43×10^{-4}	1.53×10^{-4}
3	Beam enable function	Key switch	1.00×10^{-8}	F-CPU	1.00×10^{-5}	Relay	1.43×10^{-4}	1.53×10^{-4}

calculation indicates that the designed safety control loops meet the requirements of SIL3.

5 Hardware design

As shown in Fig. 4, the field interlock devices are relatively scattered, although the interlock functions are relatively centralized. One main controller and three remote modules are selected to realize the interlock function in the personnel safety interlock system. The remote module was used to monitor and control the personnel safety interlock device on-site. The personnel safety interlock equipment can be divided into SIL3 safety devices and general devices according to the safety functions conducted. Safety devices include emergency stop buttons, door position switches, key switches, relays, radiation monitors, and accelerator beam-off devices. Common equipment includes a clearance button and an alarm lamp. The remote modules connect with the device through a hard wire to ensure the signal transmission rate and reliability. For safety devices, the remote module adopts the SIL3 level redundant wiring mode, which can identify a series of line faults, such as a short circuit and open circuit, and prevent a safety function failure [15]. For the general module, the remote module adopts single-channel wiring mode to meet the functional requirements. The main controller collects the signals uploaded by all remote modules as the judgment condition of the interlock logic and executes the safety interlock program. The main controller identifies the safety program and the general program, and then runs them separately. If the general program is abnormal, the operation of the safety program will not be affected. The communication protocol between the main controller and the remote module uses a PROFIsafe protocol meeting the SIL3 level. In addition, PSIS designs and develops a set of ring networks for data communication. The PROFIsafe protocol and ring network meet the failure requirements. The controller and remote module of the PSIS include two network ports, which are connected in series individually, forming a closed-loop network. When a line in the ring network is damaged, it will not affect the network communication of the system, thereby significantly improving the reliability of the network communication. In addition, when the ring network fails, it will be detected by the safety controller, and the safety system will trigger the failsafe interlock to shut off the beam.

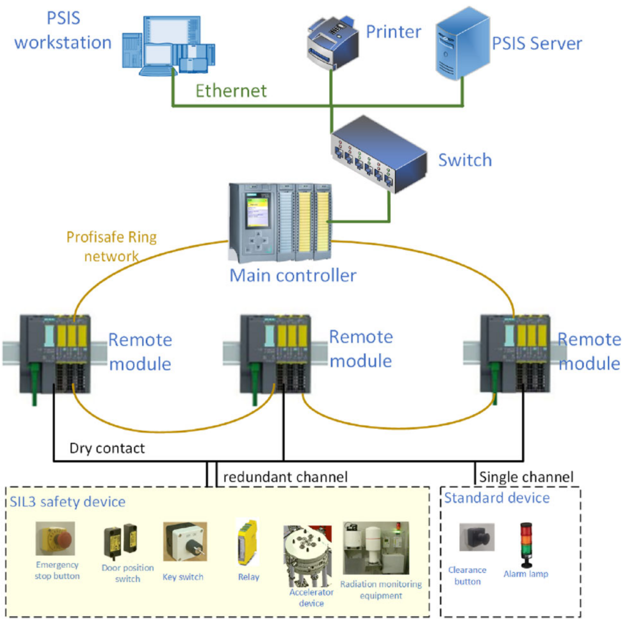


Fig. 4 (Color online) Personnel safety interlock system hardware design

The PSIS is connected to the ion source (IS), radio frequency (RF), and vertical deflection (VD). These devices are accelerator subsystems for producing a beam. When the beam-off logic is active, the HSIS interlocks the IS, RF, and VD to shut off the beam [16, 17].

The interface of the PSIS runs on a workstation used to monitor the states of the site. It has a low security level, and when the GUI fails, the personnel safety interlock logic continues running in the controller. The GUI uses the TCP/IP protocol, which is the general protocol for communication [18].

The data of the personnel safety interlock is stored on the server, and the operator can reference the historical data stored on the server for research through the system software. As a part of the auxiliary function of interlock system, the data storage function has a low safety level requirement, and uses a general network protocol for communication.

6 Logic design

The control logic of the PSIS was carried out in the main controller. The personnel safety interlock receives the signals of the clearance button, door position switch, emergency stop button, radiation monitoring, key switch, and other field devices arranged in the control area. The layout of the local interlock system device is shown in Fig. 5. The signals are logic inputs, and the controller applies the logic through the program. The logic output devices are IS, RF, and VD, which are used for beam-off logic. The logic function can be divided into the clearance function, enable function, emergency stop function, and a series of signal processing functions.

The clearance function is realized by the clearance button and clearance door. As shown in Fig. 5, the clearance function of the proton therapy system is divided into five routes, and each route is an independent area. The main purpose of the clearance is to ensure that no people are in the control area before the accelerator is released. Therefore, it is necessary to establish a clearance route that can cover the control area. According to the characteristics of this project, a clearance route is set, which can guide the worker in clearing the control area. As shown in Fig. 5, the accelerator and transportation line areas consist of routes 1, 2, and 3. When routes 1, 2, and 3 are all cleared, the interlock system judges that the accelerator and transportation line areas are cleared. The clearing of the treatment room 1 area is route 4, and when the clearance of route 4 is completed, treatment room 1 is cleared. Route 5 is used for the clearance of treatment room 2. When the route 5 area is cleared, the treatment room 2 area is cleared.

A series of area-clearance logic approaches were designed. Each area is relatively independent, and the destruction of the clearance area does not destroy the clearance of the other areas. When clearing the radiation areas, the staff only need to clear the uncleared area, which significantly improves the efficiency of the site clearance.

Inside the control and supervision areas, a large number of emergency stop buttons are arranged for beam-off operations during emergency situations to protect the safety of the personnel. The personnel safety system monitors the states of the emergency stop buttons in real time. When an emergency stop button is pressed, the interlock action is activated.

Radiation monitoring equipment is used to monitor the on-site radiation value to prevent radiation from exceeding the standard. The PSIS needs to determine whether the radiation monitoring equipment operates normally before the beam is released. If it is abnormal, the beam is not allowed. During the beam output, it is also necessary to determine whether the radiation on site exceeds the threshold value. If the threshold value is exceeded, it means that the personnel may be at risk of radiation exposure, and the beam flow needs to be interrupted.

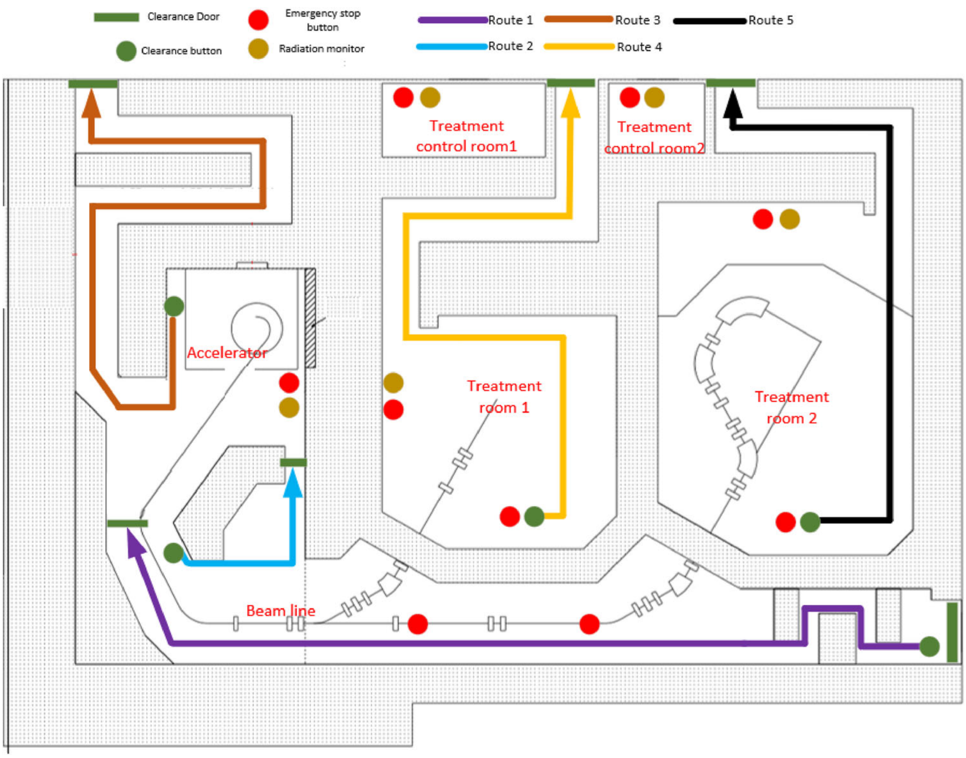


Fig. 5 (Color online) PSIS local device layout

6.1 Clearance function

The staff must clear the site according to the path indicated by the arrow. First, the operator needs to go to the starting point of the path to photograph the clearance button, and the clearance door needs to be closed within the time specified by the system. The route-clearance logic for the program is shown in Fig. 6. The interlock system monitors in real time whether the clearance button and clearance door are pressed or closed within the specified time. When the logic is correct, the interlock system judges that the route clearance has been completed. When all routes are cleared, the PSIS determines that all areas are cleared.

6.2 Beam enable function

To prevent human radiation hazards caused by the accelerator beam under unexpected situations, the safety interlock system needs to determine a series of prerequisites before releasing the beam, including the following: all control areas have been cleared, the emergency stop button has not been pressed in any areas, and the radiation monitoring system works normally without an alarm sounding.

However, on-site staff members require management methods to confirm whether the external environment is normal, such as some necessary signing procedures, confirming whether the personnel in the control room are ready, and whether the server and GUI are working normally. When all external conditions are met, the staff needs to turn on the key switch to allow the beam to be released.

The safety interlock system activates the interlocks of IS, RF, and VD when the beam release conditions are not met. At this time, the IS, RF, and VD will be interlocked, and the proton therapy system cannot release the beam. When the safety interlock system detects that all beam conditions are met, it releases the IS, RF, and VD interlocks, and the proton therapy system can release the beam.

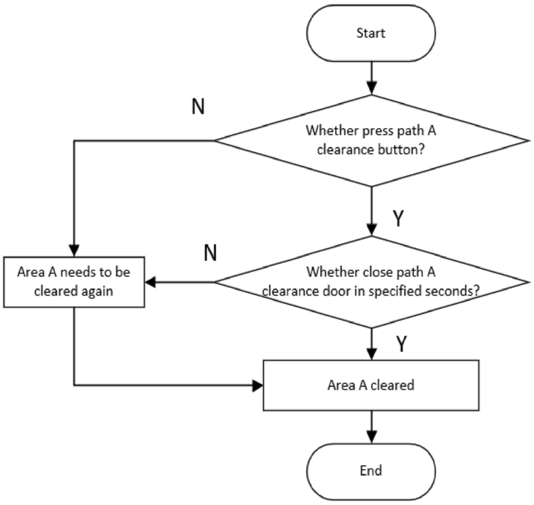

Start
Whether press path A clearance button?
N
Y
Whether close path A clearance door in specified seconds?
N
Area A needs to be cleared again
Y
Area A cleared
End

Fig. 6 Clearance logic

6.3 Emergency stop function

The emergency stop function means that, during the beam release process, the personnel safety system executes the beam-off emergency stop after detecting the beam-off condition. During the beam release process, the PSIS monitors the states of the emergency stop button, the states of the radiation monitor equipment, and whether the clearance door is open in real time. If the emergency stop button is pressed, it means that the staff has found an abnormality at the scene, and the emergency stop will be manually interrupted. To ensure the safety of the on-site staff, the proton therapy system arranges a large number of emergency stop buttons in the control area and the supervision area, and the staff can press any emergency stop button for beam stop logic. Radiation monitoring equipment is used to monitor the radiation situation in a specific location. If the radiation exceeds the limit, the equipment is deemed abnormal, or the radiation shielding fails [19], an emergency beam-off stop button is required. During the beam release process, if the clearance door is opened, it means that someone might have entered the control area by mistake. To ensure the safety of the personnel, the personnel safety interlock system needs to shut off the beam [20].

The execution devices of the beam-stop interlock are the IS, RF, and VD. When the beam stop interlock is triggered, the interlock system sends the beam stop signal to these three devices simultaneously through a hard wire and redundantly shuts the beam flow down.

7 Software development

The system block is used for software development. The system block mainly includes the function block and data block. The system blocks are divided into general function blocks and safety function blocks, and safety programs and general programs are stored. The enable function and emergency stop function belong to the safety program and are programmed in the safety function block. The clearance function and the alarm light function belong to the general function and are programmed in the general function block. Data blocks are also divided into safety data blocks and general data blocks, which store the safety variables and variables, respectively, and the safety program calls the data in the safety data block for a logical execution. In the case of a system failure, the safety program automatically activates the fail-safe interlock function to interrupt the beam. As shown in Fig. 7, the yellow background color belongs to the safety system block, and the other colors belong to the general function block.

8 GUI development

In proton therapy systems, the interface of the PSIS plays an important role. The staff cannot directly obtain the information they want from the controller, and thus a human–computer interaction interface is necessary. The GUI was developed according to the requirements of the PSIS (see Fig. 8).

In the GUI, the operator can directly obtain detailed information on the area clearance. The situation of each clearance route on the GUI interface is clearly displayed. The clearance button is green when pressed and orange when it is not pressed. The clearance door is green when it is closed and orange when it is not closed. The clearance route indicates the clearance state of the current area: clearance is complete when it is green, and incomplete when it is orange. Before the beam is enabled, the operator can determine the areas that need to be cleared on the interface and move to the corresponding area to conduct the clearing process.

The operator can obtain emergency stop information for each area on the interface. Many emergency stop buttons are arranged in each area. When an emergency stop button is not pressed, it is displayed in green. When an emergency stop button is pressed, the display of the emergency stop button in this area is changed to red. An emergency stop button area is mainly divided into the accelerator area, beam line area, treatment room 1, treatment room 2, treatment control room 1, and treatment control room 2. The operator can determine the reason for the pressing of the emergency stop button according to the area where the emergency stop button is pressed, and reset the emergency stop button in this area after confirming whether the system is functioning normally.

The system state represents the key signals of the safety interlock system. These key signals are summarized signals processed by the controller. When the beam enable indicator is green, it means that the external conditions of beam release have been met and a beam release is allowed, and when it is red, it means that the external conditions of beam release have not been met. When the emergency stop indicator is red, it means that the system has an emergency stop triggered; when it is green, it means there is no emergency stop. If the radiation alarm indicator is red, it means that the radiation is abnormal, and when it is green, it means that the radiation is normal.

The operator can obtain the beam information on the GUI, check which conditions have not been met, and view the beam logic in the GUI. When all areas have been cleared, no emergency stop button has been pressed in any area, and the radiation monitoring equipment is not in an abnormal state, the beam key switch is turned on, and all red lines of the beam logic in the GUI will change to green lines. When the beam enable signal is green, it means that the beam-release conditions have been met and the beam release is allowed.

The operator clicks the radiation monitor on the operation interface to view the specific data of the radiation monitor in each area, and clicks the History Record button to view the historical data of the interlock system, such as the time when the emergency stop button was pressed, the time of the clearance completion or failure, and the time record of the beginning and end of the beam.

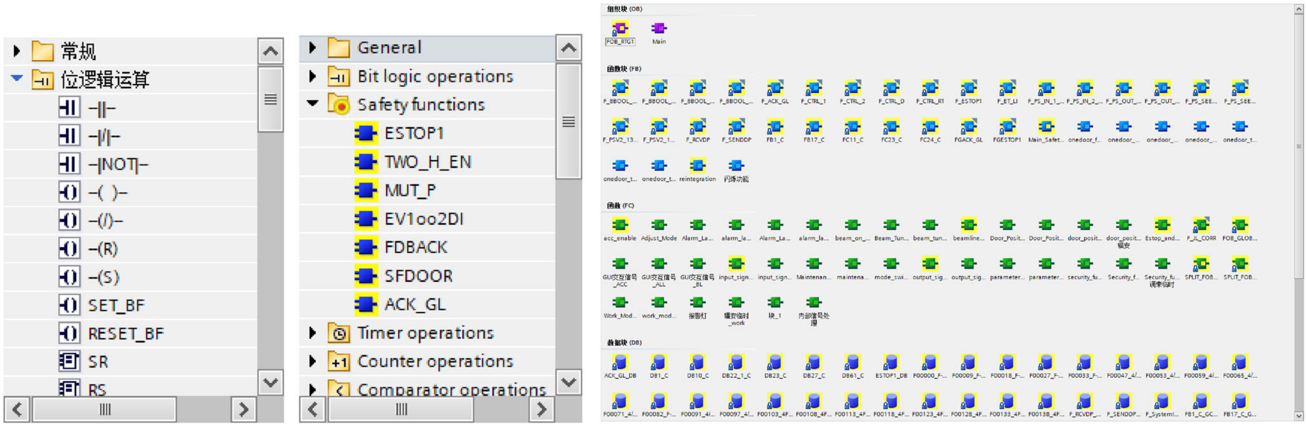


Fig. 7 (Color online) Software development

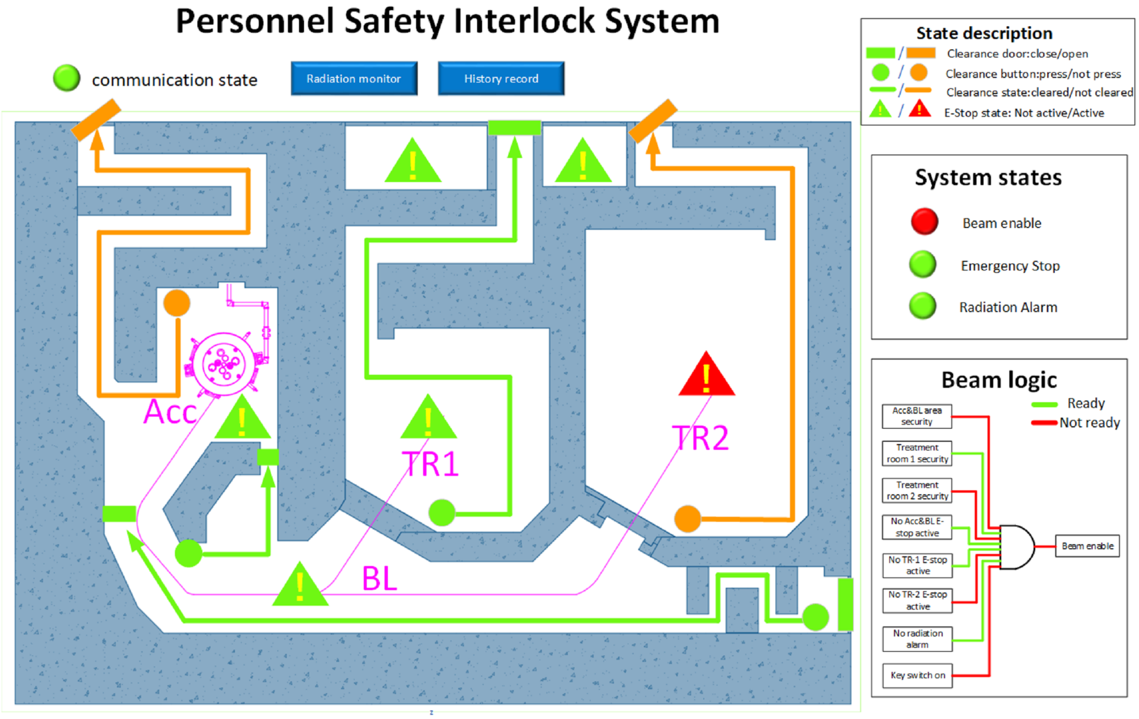


Fig. 8 (Color online) Personnel safety interlock system GUI

9 Conclusion

To protect personnel from the radiation field during the operation of the proton therapy system, a personnel safety interlock system was designed and developed. The safety interlock system of this project provides a wealth of safety interlock functions to ensure the safety of the personnel within the radiation area. However, the safety interlock system of this project fully considers the safety requirements of the system, and the key interlock control loops are designed based on SIL3, which meets the requirements of the IEC61508 standard. To obtain the SIL3 control loop, SIL3 bottom equipment and a controller are selected, the SIL3 wiring mode is used, the communication protocol applies the SIL3 PROFIsafe protocol, and a set of safety ring network systems designed for the bottom equipment communication are used. As an advantage of the SIL3 design it reduces the failure probability of the system and provides fail-safe protection; in the case of equipment failure, interlock actions can be applied to protect the personnel.

At present, the designed safety interlock system has passed a fail-safe test and has been used in the project. The safety interlock system can trigger a fail-safe protection in the case of a network failure or disconnection of the equipment signal line, effectively ensuring the safety of the personnel. Although the system was developed for specific facilities and used to protect on-site personnel during proton therapy, the data collection, data processing, site cleaning, emergency stop, and activation functions in the system can still be widely used in most radiological experimental sites. Because the PSIS is extremely important for protecting field personnel in the radiation industry, it is necessary to continue recording the problems that occur during the operation of the existing equipment, optimize the safety interlock system, and improve the overall stability of the safety interlock system operation.

Author contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Shou-Yuan Wang, Jing Zhang, Ou-Wen Huang, Zhu Li. The first draft of the manuscript was written by Shou-Yuan Wang and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

1. S. Frisch, B. Timmermann, The evolving role of proton beam therapy for sarcomas. Clin. Oncol. **29**(8), 500–506 (2017). https://doi.org/10.1016/j.clon.2017.04.034
2. International Electrotechnical Commission (IEC). Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Geneva, Switzerland: IEC; 2010. Standard No: IEC 61508:2010.
3. F. Tao, J. Murphy, E. Carrone et al., Safety integrity level (SIL) verification for SLAC radiation safety systems. In: The 15th international conference on accelerator and large experimental physics control systems, ICALEPCS 2015, Melbourne, Australia,

pp. 561–564 (2015). doi:https://doi.org/10.18429/JACoW-ICALEPCS2015-TUC3O07

4. W. Wang, Y. Song, J. Wang et al., Design of the personnel radiation safety interlock system for high intensity d–t fusion neutron generator. J. Fusion Energ. **34**(2), 346–351 (2015). https://doi.org/10.1007/s10894-014-9807-1
5. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China. Basic standards for protection against ionizing radiation and for the safety of radiation source. Beijing, China: Standards Press of China; 2002. Standard No: GB 18871:2002 (in Chinese)
6. A. Luchetta, N. Pomaro, G. Manduchi et al., Progress in the design of MITICA control and interlock systems. Fusion Eng. Des. **146**, 1528–1532 (2019). https://doi.org/10.1016/j.fusengdes.2019.02.121
7. M. Mansouri, S. Birch, A. Nordt, et al., New concepts for access devices in the SPS personnel protection system. In The 16th international conference on accelerator and large experimental physics control systems, ICALEPCS 2017. Barcelona, Spain, pp1608–1612 (2017). doi:https://doi.org/10.18429/JACoW-ICALEPCS2017-THPHA099
8. M. Hron, R. Sova, R. Siba et al., Interlock system for the COMPASS tokamak. Fusion Eng. Des. **85**(3–4), 505–508 (2010). https://doi.org/10.1016/j.fusengdes.2010.03.054
9. P. Bohm, M. Hron, J. Kovar et al., Personnel protection during the operation of Thomson scattering laser system on COMPASS tokamak. Fusion Eng. Des. **86**(6–8), 699–702 (2011). https://doi.org/10.1016/j.fusengdes.2011.02.073
10. J. Hawkins, C. Seaver, J. Stein et al., Personnel safety system for the beamlines at the advanced photon source. Rev. Sci. Instrum. **67**(9), 3370–3370 (1996). https://doi.org/10.1063/1.1147477
11. E. Barrera, M. Ruiz, A. Bustos et al., Implementation of ITER fast plant interlock system using fpgas with CompactRIO. IEEE Trans. Nucl. Sci. **65**(99), 796–804 (2017). https://doi.org/10.1109/TNS.2017.2783243
12. H. Tyagi, J. Soni, R. Yadav et al., Preliminary design of safety and interlock system for indian test facility of diagnostic neutral beam. Fusion Eng. Des. **112**, 766–770 (2016). https://doi.org/10.1016/j.fusengdes.2016.05.017
13. J. Kieffer, B.V. Golceff, A modular safety interlock system for high energy physics experiments. IEEE T. Nucl. Sci. **28**(1), 634–637 (1981). https://doi.org/10.1109/TNS.1981.4331254
14. Z.Y. Huang, K. Xuan, C. Li et al., Novel design of a personnel safety system for Hefei Light Source-II. Nucl. Sci. Tech. **30**, 99 (2019). https://doi.org/10.1007/s41365-019-0610-6
15. J. Cinnamon, K. Mahoney, Modular reliability modeling of the TJNAF personnel safety system. IEEE. **3**, 3678–3680 (1998). https://doi.org/10.1109/PAC.1997.753382
16. M. Suzuki, T. Iwasaki, T. Sugawaraa, A study of startup and shutdown procedure of accelerator-driven system. Nucl. Instrum. Methods Phys. Res. Sect A **562**, 867–869 (2006). https://doi.org/10.1016/j.nima.2006.02.174
17. Y.G. Song, Interlock system for machine protection of the KOMAC 100-MeV proton linac. J. Korean Phys. Soc. **66**(3), 449–453 (2015). https://doi.org/10.1007/s41365-019-0610-6
18. V. Drndarevic, Control of Gamma Irradiation Facility with Improved Safety System. J. Nucl. Sci. Technol. **45**, 361–367 (2008). https://doi.org/10.1080/18811248.2008.9711445
19. R.K. Reed, J.C. Bell, Safety systems and access control in the National Ignition Facility. Health Phys. **104**(6), 563–570 (2013). https://doi.org/10.1097/HP.0b013e31828cfb46
20. V. Drndarevic, Safety systems in gamma irradiation facilities. Health. Phys. **73**(2), 383–41997 (1997). https://doi.org/10.1097/00004032-199708000-00012