BJRS
BRAZILIAN JOURNAL OF RADIATION SCIENCES

doi.org/10.15392/2319-0612.2026.2956
Braz. J. Radiat. Sci., Rio de Janeiro
Jul-Sep 2026, 14(3) | 01-25 | e2956
Editor(s): Dr. (Prof.) Bernardo Maranhão Dantas
Dr. (Prof.) Alfredo L. Ferreira Filho
Dr. (Prof.) Ademir de Jesus Amaral
Submitted: 2025-05-30
Accepted: 2026-03-30

Original Article

Requirements and Implementation of the Traceability System in the Sirius Accelerator

Vieira[a*], A. L. C.; Barreto[a*], G. T.; Moura[b], F. N.; Canova[a], H. F.

[a]Centro Nacional de Pesquisa em Energia e Materias - CNPEM, 13083-100, Campinas, São Paulo, Brasil.
[b]MAX IV Laboratory, Fotongatan 2, 224 84 Lund, Suécia

*Correspondence: ana.vieira@cnpem.br, guilherme.barreto@lnls.br

Abstract: This paper describes the requirements and implementation of the Traceability System at Sirius, the Brazilian synchrotron light source. The system was designed to ensure that only personnel trained by the Radiation Protection Group operate the beamlines. The solution utilizes radio-frequency identification technology to enable the "Search" procedure, a mandatory safety step for the release of synchrotron radiation. The system integrates Siemens programmable logic controllers (PLCs), C# development for data encoding, and a web infrastructure based on MariaDB, Node-RED, and PHP for real-time monitoring. Results indicate that, between June 15, 2023 and October 24, 2025, 34,099 search procedures were performed across the 15 beamlines in operation and commissioning, involving more than 200 internal and external users. This work elucidates the system's technical architecture and demonstrates its effectiveness in radiological safety management and the traceability of experimental activities at Sirius.

Keywords: Traceability, radiation safety, programmable logic controller, security procedure, Sirius.

SBPR
OPEN ACCESS
CC BY

doi.org/10.15392/2319-0612.2026.2956
Braz. J. Radiat. Sci., Rio de Janeiro
Jul-Sep 2026, 14(3) | 01-25 | e2956
Editor(s): Dr. (Prof.) Bernardo Maranhão Dantas
Dr. (Prof.) Alfredo L. Ferreira Filho
Dr. (Prof.) Ademir de Jesus Amaral
Submitted: 2025-05-30
Accepted: 2026-03-30

Requisitos e implementação do sistema de rastreabilidade no acelerador Sirius

Resumo: Este artigo descreve os requisitos e a implementação do Sistema de Rastreabilidade no Sirius, o acelerador de partículas brasileiro. O sistema foi projetado para assegurar que apenas usuários capacitados pelo Grupo de Proteção Radiológica operem as linhas de luz. A solução utiliza tecnologia de identificação por radiofrequência para habilitar o procedimento de "Procura", etapa mandatória para a liberação de radiação síncrotron. O sistema integra controladores lógicos programáveis Siemens, desenvolvimento em C# para gravação de dados e uma infraestrutura web baseada em MariaDB, Node-RED e PHP para monitoramento em tempo real. Os resultados indicam que, entre 15 de junho de 2023 e 24 de outubro de 2025, foram realizados 34.099 procedimentos de procura nas 15 linhas de luz em operação e comissionamento, abrangendo mais de 200 usuários internos e externos. O trabalho elucida a arquitetura técnica do sistema e demonstra sua eficácia na gestão da segurança radiológica e na rastreabilidade das atividades experimentais no Sirius.

Palavras-chave: rastreabilidade, proteção radiológica, controlador lógico programável, procedimento de segurança, Sirius.

1. INTRODUCTION

Sirius is a fourth-generation synchrotron light source located at the Brazilian Center for Research in Energy and Materials (CNPEM) in Campinas, São Paulo, Brazil (Figure 1). Categorized as a Class 7D facility by the Brazilian Nuclear Energy Commission (CNEN) [4, 5], Sirius operates at 3 GeV with a current of 100 mA, generating a broad spectrum of synchrotron radiation ranging from infrared to hard X-rays [17]. Within its 15 operational beamlines, researchers must perform a 'Search procedure' to establish radiological safety conditions at experimental stations. To ensure security and the integrity of user logs, a traceability system has been implemented across all beamlines.

Figure 1: Front view of the building housing the Sirius synchrotron accelerator.



Source : Authoral image

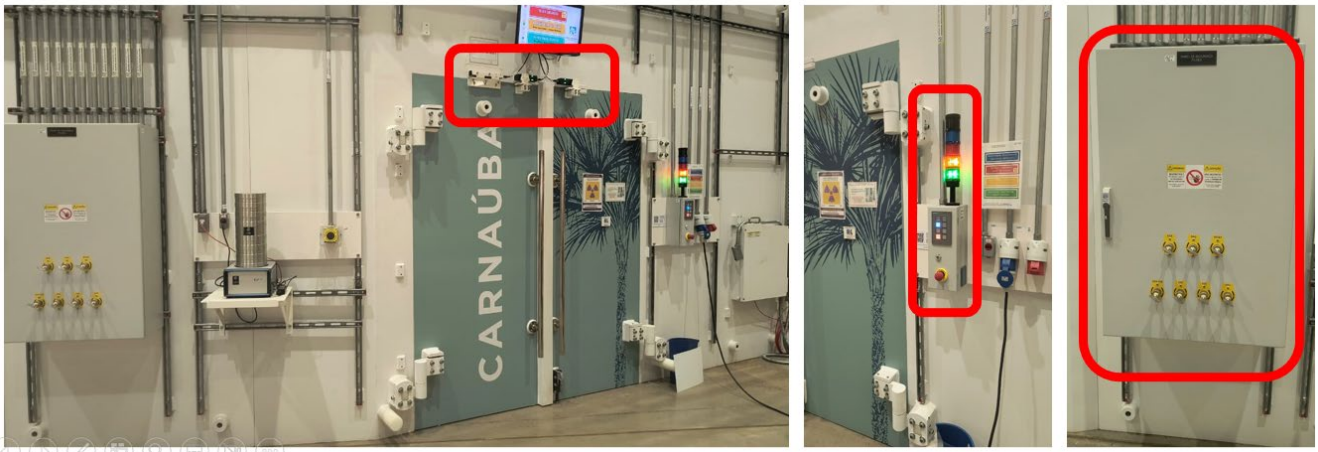
Beamlines consist of hutches, designed to accommodate the sample analysis instruments, where they will be exposed to a spectrum of the synchrotron radiation; and to ensure that the radiation generated is contained within their shielding [17,5]. Furthermore, numerous safety mechanisms have been implemented to ensure their safe and effective operation. These include safety locks and switches, light curtains, signal towers, an emergency system, the Search and a traceability system. As demonstrated in Figure 2, the elements of

OPEN ACCESS
CC BY

the PPS (Personnel Protection System) are highlighted in the Carnaúba (Coherent X-rAy NAnoprobe) beamline. Figure 2 highlights:

- Left: doors locks
- Center: Signaling tower, operation panel and external emergency button
- Right: Personnel protection panel

Figure 2: Hutch of a beamline with security elements.



Source : Authoral image

The Search procedure, carried out exclusively by trained personnel, consists of verifying that the radiation safety conditions within the hutch are satisfactory and must be completed to enable the beamline hutch for operation [12, 19, 14]. The most important condition in the search procedure is to verify that no person is inside the hutch. This verification is performed by pressing buttons strategically positioned inside the hutch. This procedure enforces the verification that no person is present inside the hutch. After the buttons are pressed, the hutch door must be closed and press a specific external button to lock the door and enable the beamline hutch for operation.

The overarching objective of the Sirius project was to cater to the global scientific community; consequently, it is reasonable to assume that thousands of researchers will utilize the beamlines for their experiments. Given the considerable number of people involved, effective registration processes are fundamental. In addition to efficient registration, the

OPEN ACCESS

implementation of a logical security barrier within the registration procedure is essential. Furthermore, the establishment of a link with a qualification granted through training, along with a traceability system, is necessary.

The traceability system, a collaborative effort between the laboratory's Radiological Protection Group (RAD) and the Infrastructure in Electrical, Electronics and Automation Group (AIS), has been developed for two primary objectives. Firstly, it is intended to serve as a safety barrier, ensuring that only authorized personnel perform specific procedures. Secondly, it is designed to record all data related to these procedures.

2. MATERIALS AND METHODS

2.1. The people involved

The traceability system integrates the daily operations of three main groups: RAD, AIS, and EdU.

The RAD group has the safety specifications that must be met to ensure compliance with regulations and radiological safety [4]. The RAD group trains and enables trained individuals to use the search cards.

The RAD group specified the implementation conditions to the AIS group. Based on this, the AIS group developed the entire system architecture and maintains it in operation.

The User office group (EdU) is responsible for receiving users from other facilities and institutions. When an external user arrives at CNPEM, they must complete a series of training sessions, which includes training provided by RAD, and EdU can, through the traceability system developed by AIS, enable the external user to access the search procedure.

This means that the three groups share a common point of convergence: the traceability system.

OPEN ACCESS

2.2. Definition of technologies used

2.2.1. User registration and authentication

The preliminary stage in defining the technologies for the traceability system was to determine the authentication method for users authorized to perform the search procedure. In the contemporary technological landscape, a wide range of authentication methods is available, including biometrics, facial recognition, passwords, and verification codes. However, to avoid handling of sensitive user data and to optimize the search procedure, possession-based authentication was chosen. In this approach, the user must be present an object to gain access to the service.

In the realm of authentication methodologies, particularly those predicated on possession, a notable contender emerges in the form of an integrated RFID (radio frequency identification) reader and transponder configuration. The use of this technology necessitates the proximity of the transponder to the reader, thereby enabling the retrieval of the transponder's data. This data can be the transponder's unique serial number or internally stored information.

The data read from the transponder is then transmitted to a control unit, such as a computer, programmable logic controller (PLC), or microcontroller. The function of this unit is to determine whether a specific user is authorized to access or perform a particular action, such as controlling access or executing specific procedures.

The implemented solution utilizes the card reader model RF1040R [19] and the transponder model MDS D200 [18]. Figure 3 shows both the card reader (left) and the transponder (right).

OPEN ACCESS

Figure 3: Card reader (ledt) and transponder (right)



Source : Adapted [19] and [18]

There are some reasons for choosing the card reader and transponder models mentioned above:

- The reader model chosen is capable of communicate directly with the PLC responsible of the search procedure and the equipment that governs the passage of synchrotron radiation between hutches. The implementation of a direct connection between the user authentication device and the PLC serves to eliminate potential failures that may be introduced by an intermediate device, thereby enhancing the reliability of the system. Additionally, the reader is manufactured by Siemens, the same company as the PLCs used in beamlines, which facilitates device integration. This integration is achieved using the RS-232 (Recommended Standard 232) communication standard and the Freeport communication protocol [6].

- In addition to the RS-232 interface, the RF1040R reader is equipped with a USB communication interface that incorporates DLL libraries (Dynamic Link Library). These libraries facilitate the reading and writing of data using the C# programming language [2]. The ability to write data on computers is crucial, as it allows the RAD and the EdU groups to register authorized users directly from their workstations, thereby streamlining the user enablement process.

OPEN ACCESS
CC BY

- The transponder design has been conceived with a resemblance to that of an identification card, thus facilitating ease of handling and storage for the user.

As the transponder is in the form of a card, it will be referred to as a card throughout the remainder of this document.

2.3. Data recording

The database management system selected for recording the data generated by the system was MariaDB [13]. The database is an SQL (relational) database and can be used without the need for a license.

The data collected is sourced from both the computer program and the PLCs. In the absence of native capabilities in Siemens PLCs to write directly to a MariaDB database, the use of an intermediary communication method is imperative. Node-RED [15] acts as the intermediary software that enables communication between the database and the PLC. The selection of Node-RED was based on its widespread adoption automation, its event-oriented programming approach, and its capacity for license-free usage.

2.4. Data display

To facilitate the presentation of the data, web technologies were employed to enable access through a standard web browser.

The web technologies employed for the retrieval of data from the database were PHP (PHP: Hypertext Preprocessor) [16] and Apache [1]. The data display was facilitated by the utilization of HTML (HyperText Markup Language) [10], CSS (Cascading Style Sheets) [3], JavaScript [11], and Bootstrap [9]. The selection of these technologies was based on the development team´s prior expertise in their use.

2.5. Traceability system specifications

To accomplish the objectives specified for the traceability system, it was necessary to satisfy certain specifications:

OPEN ACCESS
CC BY

1) It is essential that the "Search" procedure is restricted to authorized personnel only. In the context of Sirius, individuals performing this procedure can be categorized into two groups: internal users (Sirius beamline staff and support groups) and external users (researchers with approved proposals who conduct experiments at the beamlines for a limited period). Authorization for this procedure depends on successful completion of training that provides a comprehensive explanation of the procedure itself, in addition to the radiological safety elements and the necessary conditions for a beamline to be enabled to receive synchrotron radiation.

2) The system must record and display the history of "Search" procedures performed on the beamlines, as well as identify the user who performed the procedure. This information is critical for the diagnosis of potential issues associated with the "Search" procedure, as well as in emergency cases for the reconstruction of local history and maintaining a mapping of individuals who perform "Search" procedures on the beamlines.

3) The system cannot store sensitive personal information of authorized users. In the context of Brazilian legislation, the General Data Protection Law (LGPD) is the primary regulatory framework governing the protection of personal data. Notably, this legislation prohibits the storage of sensitive data, such as fingerprints and facial recognition.

4) It is necessary for the system to be developed in such a manner that the registration of authorized individuals can be conducted using a computer program. The registration of authorized individuals is a function of RAD for CNPEM users, and the Users Office (EdU) group for external users who have submitted proposals to use the facility.

5) It is imperative that the system is developed in such a manner that users are only permitted to perform the "Search" procedure on the beamlines for which they have been trained.

2.6. Approaches to recording data on the card

In the context of RFID readers and cards, two primary approaches to user authentication can be identified:

OPEN ACCESS
CC BY

- Centralized Approach: In this method, the card only provides its unique serial number to the RFID reader. This serial number has been preregistered in a database linked to the control unit. Subsequently, the control unit queries the database to ascertain whether the user is authorized to perform a specific action. The benefit of a centralized approach is that it does not necessitate the writing of data to the card. However, the necessity for constant database access by the control unit to verify card authorization constitutes a significant drawback. In the case of PLC), database access is typically only possible via an internet connection.
- Decentralized Approach: In this scenario, the card provides the RFID reader with its previously recorded internal data. This data is then transmitted to the control unit, which uses this information to determine user authorization exclusively based on these criteria.

In the Sirius system, the PLC that is employed for the search procedure has been programmed to function independently of internet network data. The operational logic of the system is contingent on the input from sensors. This design choice is critical for the system's required robustness, ensuring the search procedure remains functional for the longest possible duration. For instance, potential internet connection drops do not affect the search procedure, which is a prerequisite for experiments on beamlines.

Consequently, to maintain the search procedure's robustness, the decentralized approach for RFID readers and cards is the most suitable for Sirius. While the process necessitates the inscription of data to the card, this is substantiated by the enhanced robustness it confers in authorizing users for the search procedure without necessitating a database connection.

Therefore, the database in the traceability system records data about authorized users and completed search procedures, but it does not handle user authorization directly. The process of authorizing users in relation to the search procedure is overseen by the PLC itself.

OPEN ACCESS

2.7. System function stages

The Traceability System architecture in four distinct stages:

- The process of data recording on the card
- The process of enabling the search procedure for users
- The process of recording the search procedures status – in progress, finalized and undone
- The process of blocking cards. This process is only applied if the card has been lost, damaged, or stolen

2.8. Data recording on the card

The groups designated RAD and EdU are responsible for the data recording on the card. The process involves the use of a desktop application in conjunction with the reader. The data is encrypted after been stored on the card:

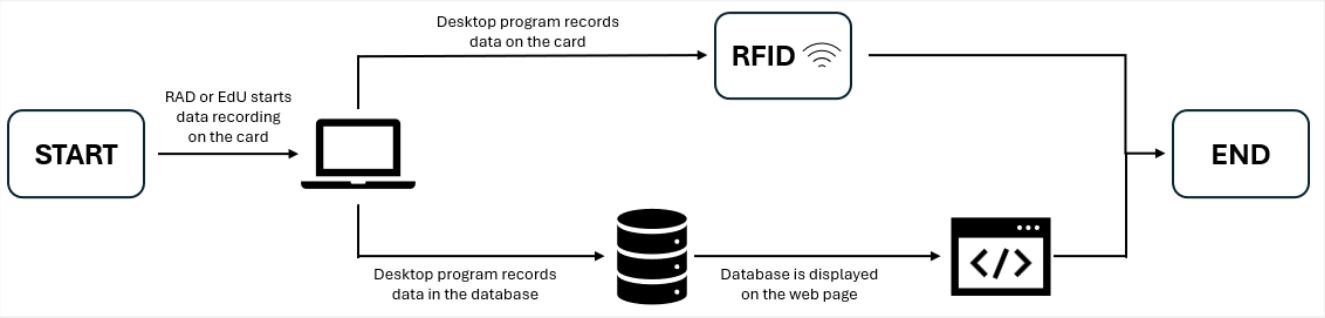
- Start date for search procedure authorization;
- End date for search procedure authorization;
- Beamline(s) the card is authorized for the search procedure;
- Card serial number.

Concurrently, the information recorded on the card is linked to the name of the user authorized to perform the search procedure. This association is stored in the database and displayed on the web page.

Figure 4 illustrates the data flow recorded on both the card and the database. After the data recording, the transponder is ready to be given to the user.

OPEN ACCESS

Figure 4: Data recording on the card and in the database



Source : Authoral image

2.9. Enabling the search procedure for users

The search procedure is enabled by the user, using a pre-recorded card. The user then brings the card close to the RFID reader. The information on the card will be read and decrypted by the PLC, and the search procedure will be authorized for the user if:

- The card usage date is after the start and at the end date of the search procedure authorization.
- The beamline where the search procedure is being attempted is one of the beamlines authorized on the card.
- The serial number read from the card matches the serial number recorded on the card itself. This comparison prevents cloned cards from being used in the traceability system, as each card's serial number is unique and cannot be altered.
- The card is not blocked for use (this topic will be covered in the "Card blocking" section).

If all these prerequisites are met, the user is notified with a green light that the search procedure is authorized. Then, the user has four seconds to initiate the procedure. In contrast, if any of these prerequisites are not met, the user is notified with a red light that their card is not authorized to perform the search procedure on that specific beamline.

OPEN ACCESS

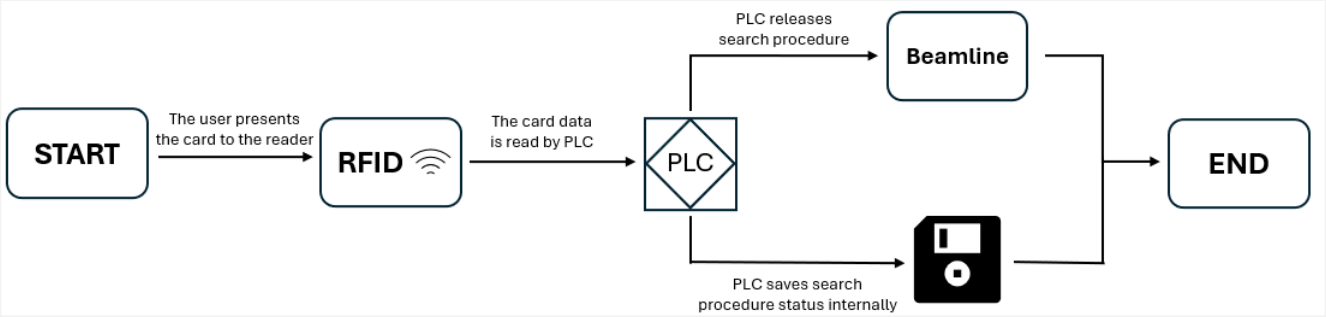
As soon as the search procedure begins, its status is stored in the PLC's internal data buffer. The procedure status can take on the following states:

- Search procedure in progress: This state occurs when the user is performing the search procedure by pressing the internal buttons to verify that no person is inside the hutch, closing the hutch door and pressing the external button to lock the door
- Search procedure finalized: This state indicates that no person is inside the hutch and, from both personnel safety and radiological perspectives, the beamline is enabled for operation
- Search procedure undone: This state occurs when the hutch is unlocked and enabled to enter inside it. To enable beamline operation again, a new search procedure must be performed

Along with these statuses, the timestamp for each event and the user who initiated and finalized the procedure are also stored. This data is temporarily held to be collected by Node-RED.

Figure 5 illustrates the data flow as it's read by the PLC, authorizing the search procedure for users, and saving information in the internal buffer.

Figure 5: Enabling the search procedure for users



Source: Authoral image

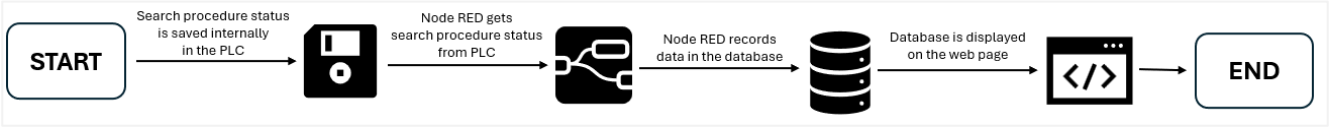
OPEN ACCESS
CC BY

2.10. Recording the search procedure status

The search procedure status is recorded in the MariaDB database. For this, Node-RED checks the PLC's buffer every 10 seconds for any unsaved data. If new data is found, Node-RED retrieves it from the PLC, processes it for proper formatting, saves it in the database, and then deletes it from the PLC's internal buffer. OPC UA is the communication protocol used between the PLC and Node-RED. The data saved in the database is then displayed on the web page.

Figure 6 illustrates the data flow from the PLC's internal buffer, read by Node-RED, and then saved in the database.

Figure 6: Data flow from PLC to the database



Source: Authoral image

It is important to note that saving data to the PLC's internal buffer and having Node-RED periodically check for new data is a more robust approach. This is because if the internet connection to the PLC drops, the search procedure will still be available, and its status updates will be saved in the internal buffer. Once the internet connection is restored, Node-RED can retrieve the full history of this data.

However, the internal data buffer is limited and only supports nine search procedure status records. If an internet connection drops and the search procedure status changes more than nine times, the oldest status records in the internal buffer will be lost.

2.11. Card blocking

Adopting the decentralized approach for RFID readers and cards offers the advantage of not depending on an internet connection to authorize the search procedure. However, there might be situations where the system needs to block a card from initiating the procedure, such as if it's lost, damaged, or stolen. Since authorization is based on data

OPEN ACCESS
CC BY

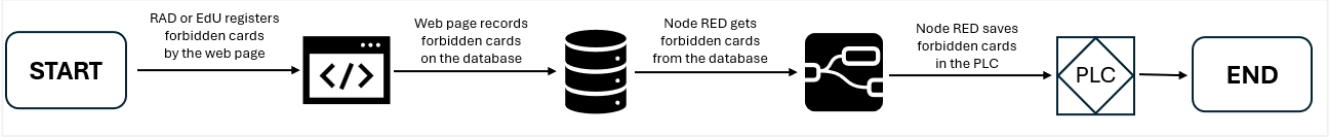
recorded directly on the card, a mechanism is required for the PLC to read a list of serial numbers belonging to blocked cards.

Without an internet connection, manually registering blocked card on every PLC used across the beamlines would be a cumbersome task.

To address this, a table from the database is responsible for recording blocked cards. Through the web page, it's possible to register these cards, and Node-RED periodically sends this data to the PLC.

Figure 7 illustrates the data flow of prohibited cards being sent to the PLC.

Figure 7: Data flow for saving blocking cards in the PLC



Source: Authoral image

This way, when the RFID reader on the PLC reads a card with a blocked serial number, the search procedure isn't authorized. Figure 8 illustrates this situation.

Figure 8: Data flow for PLC blocking forbidden cards



Source: Authoral image

3. RESULTS AND DISCUSSIONS

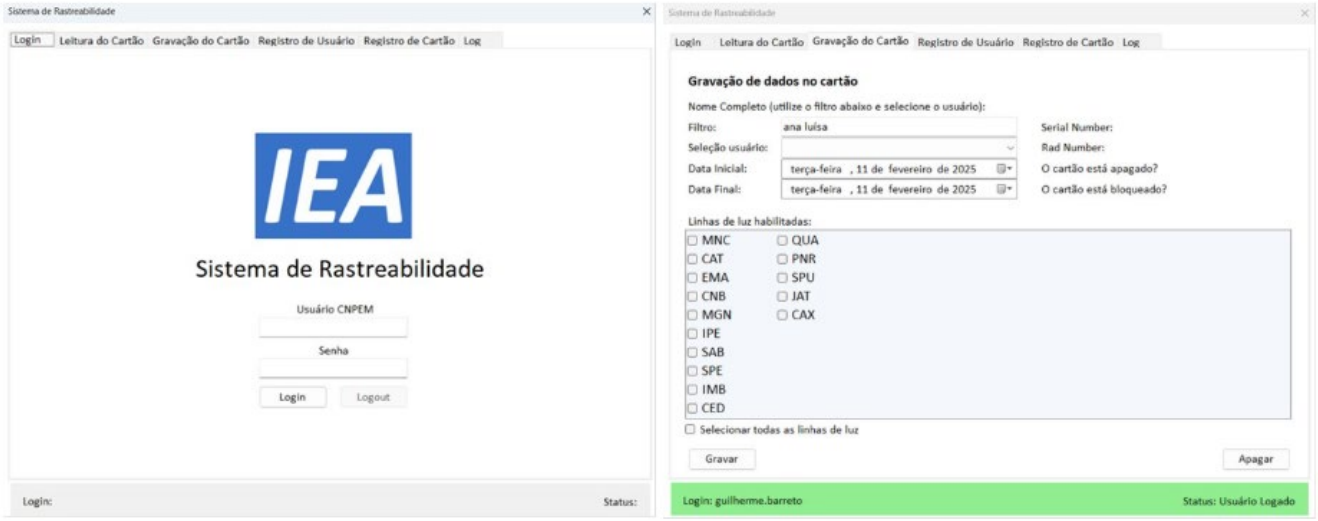
3.1. Deployment of the system on the beamlines

The traceability system has been operational at Sirius since June 2023. It ensures that only trained individuals can perform the search procedure, with all procedure data being recorded and monitored.

OPEN ACCESS
CC BY

Figure 9 shows the traceability system's desktop application, which is used to record data onto RFID cards. Access to this application is restricted and requires a registered user to log in.

Figure 9: Traceability system desktop application.



Source: Authoral image.

Figure 10 shows the reader installed on a beamline. Users must bring their card close to the reader to authorize the search procedure. The reader is indicated with a red arrow.

Figure 10: Reader installed on the beamline



Source: Authoral image.

OPEN ACCESS
CC BY

Figure 11 shows a screenshot of the traceability system's web page. Its purpose is to monitor card authorizations, users, and search procedures. The web page also allows for the blocking and unblocking of cards. Access to this page is restricted and requires a registered user to log in.

Figure 11: Traceability system web application



Source: Authoral image.

It is important to emphasize that, regarding the traceability system's reliance on internet connectivity, certain processes require a database connection. These include card recording, data transfer from the PLC to the database, and card blocking. However, it should be noted that both the database and the web page are hosted on a dedicated Sirius virtual machine, thereby significantly reducing the chances of losing connection between them. In terms of the system's robustness, the project's architecture placed a premium on facilitating the search procedure for the user, irrespective of an internet connection. This objective was achieved by the implementation of a direct data protection system on the card.

3.2. Data analysis

Data acquired by the traceability system provides information to understand the history of fades in an eventual radiological safety problem on the beamlines. Data also can be used to understand the user's behavior on the beamlines from the radiological safety point of view.

OPEN ACCESS
CC BY

3.3. Number of search procedures

Data acquired from June 15, 2023 to October 24, 2025 shows that it was registered 42714 search procedures in progress, 34099 search procedures finalized and 41302 search procedures undone. The number of search procedures in progress is bigger than the number of search procedures finalized because there are instances that the search procedure in progress is cancelled and return to search procedure undone. Most of that instances are errors in performing the search procedure and the search procedure withdrawal.

Some information needs to be clarified for better understanding of the number of finalized search procedures presented by beamlines:

- On the beamlines, hutches focused on initial filtering of beams may be installed. This type of hutch is called optical enclosure. Depending on the energy range, this hutch may be built by steel, insulated panel wall or even not required radiological shielding. Usually, users perform the search procedure only a few times on this type of hutch
- On the beamlines, hutches focused on beam treatment for experiments may be installed. This type of hutch is called experimental hutch. Depending on the energy range, this hutch may be built of steel, insulated panel wall of even no required radiological shielding. Usually, users perform the search procedure more times on this type of hutch, because inside these hutches samples are positioned for experiments
- Due to various factors, such as the energy range used in the experiments, the equipment on the Imbuia, Cedro, Tatu, and Sapê beamlines is not installed within radiological shielding that requires a search procedure. For this reason, there are no registered search procedure numbers on these beamlines;
- Carcará**:** This is a beamline used exclusively for electron beam diagnostics of the accelerator. Because of this, it is rarely necessary to perform a search procedure on it;

OPEN ACCESS

- Carnaúba, Cateretê, Ema, Manacá, Mogno, and Paineira: These beamlines consist of at least one optical hutch and one experimental hutch. All these hutches are made of steel; therefore, a search procedure is required to authorize experiments in these areas. This information explains the high number of search procedures performed on these beamlines;
- Ipê and Sabiá: These beamlines feature an optical hutch made of steel that requires a search procedure. However, the experimental sections of these lines do not require radiological shielding, and the equipment is not enclosed within a hutch. This characteristic eliminates the need for a search procedure in these experimental areas. This information explains the low number of search procedures performed on these beamlines;
- Quati and Sapucaia: Although these beamlines feature optical and experimental hutches with steel shielding that require search procedures, they are currently in the commissioning phase and are not yet open to external users. This explains the low number of search procedures compared to the other beamlines.

Table 1 shows the number of finalized search procedures for each beamline.

Table 1: Search procedures finalized for each beamline

Beamline	**Main Experimental Technique**	**Number of finalized search procedures**
Carcará	Diagnosis and monitoring of the Sirius accelerator electron beam	200
Carnaúba	X-Ray Nanoscopy	6427
Cateretê	Coherent and Time-resolsed X-ray Scattering	5759
Cedro	Circular Dichroism	0
Ema	X-ray Spectroscopy e Diffraction in Extreme Conditions	6143
Imbuia	Infrared Micro and Nanospectroscopy	0
Ipê	Resonant Inelastic X-ray scattering and Photoelectron spectroscopy	220
Manacá	Macromolecular Micro and Nanocrystallography	4956

OPEN ACCESS

Beamline	Main Experimental Technique	Number of finalized search procedures
Mogno	X-ray Micro- and Nanotomography	3538
Paineira	Powder X-ray Diffraction	4197
Quati	X-ray Spectroscopy with Temporal Resolution	1195
Sabiá	Soft X-Ray Absorption Spectroscopy and Imaging	238
Sapê	Angle-Resolved PhotoEmission Spectroscopy	0
Sapucaia	Small Angle X-ray Scattering	1226
Tatu	Terahertz Nanospectroscopy	0

Source: Authoral table

3.4. Number of registered and blocked cards

Currently, there are 300 cards registered in the traceability system. Of these, 256 are being used by internal and external users. The system's cards are reusable, meaning the same card can be used by different users on distinct dates.

Additionally, there are 10 cards that are currently blocked. The primary reason for blocking cards is loss by the user.

3.5. Number of users that perform the search procedure

Data obtained between June 15, 2023, and October 24, 2025, show that 1170 internal and external users performed search procedures on the beamlines, an average of 29 searches per user.

An interesting data point is that, of the 1170 users who performed a search procedure, 167 users (approximately 14%) performed only one procedure. Generally, this first search procedure is conducted while the user is being taught the procedure itself. This statistic reflects the policy of guiding all external users through radiological safety training. This training aims to provide information of radiological protection, as well as emergency

OPEN ACCESS
CC BY

procedures and signaling at the beamlines [13,19]. The training also includes instruction on the search procedure.

3.6. Required improvements to the traceability system

Over the two years of operation of the traceability system, several improvements to the system have been identified:

- The software used for data storage and visualization (MariaDB, Node-RED, and PHP) is currently installed directly on a virtual machine without the use of containerization technologies. Using modern containerization tools such as Docker or Podman, it is recommended that these software components be encapsulated in containers to facilitate migration to another virtual machine, if necessary
- Currently, during the card recording process, it is not clearly emphasized whether the user being associated with the card is an internal or external user. This is particularly problematic when an external user becomes an internal user (for instance, if they are hired by CNPEM). In such cases, these users remain registered as external users even after becoming internal ones. From a radiological safety perspective, this is not an issue; however, from a data storage standpoint, the primary concern is the collection of internal user data under the external user category. This discrepancy hinders the gathering of accurate statistics used to study the behavior of external users during search procedures.

OPEN ACCESS

4. CONCLUSIONS

Prior to the initiation of Sirius's operations, users of the beamlines underwent training to familiarize themselves with the search procedure as it is performed in other synchrotrons around the world. However, the absence of technological barriers made it difficult to maintain history and keep accurate record of the actions, as well as the sequence of those actions.

The Sirius traceability system has demonstrated to have a substantial impact on enhancing radiological safety. The system's primary function is to facilitate record-keeping; however, it also introduces a paradigm shift in the way safety protocols are monitored. The system meticulously tracks who performs critical operations. This detailed insight is important for proactive risk management. In situations where prompt and precise reconstruction of events is paramount, the system plays a pivotal role. It facilitates comprehensive investigations, identifies underlying causes, and enables the implementation of effective corrective measures.

A key strength of the program is its advanced data management. The system offers an intuitive interface for straightforward data export and visualization, thereby facilitating historical analysis. This enables the Radiological Protection Group to identify trends, evaluate training, and refine safety protocols. It is imperative to emphasize that this protocol ensures only personnel who have completed training are authorized to execute search procedures. This measure is instrumental in mitigating the potential for human error and strengthening Sirius's radiological safety culture, thus ensuring the integrity of its experimental processes.

CONTRIBUTORSHIP

Conceptualization: VALC, BGT, MFN, CHF

Investigation: VALC, BGT, MFN, CHF

Writing – review and editing: VALC, BGT, MFN, CHF

OPEN ACCESS

CONFLICT OF INTEREST

We have no conflicts of interest to disclose.

DATA AVAILABILITY STATEMENT

Interview transcripts and qualitative data are not publicly available due to confidentiality commitments made to research participants. Aggregated data supporting the findings are available from the corresponding author upon reasonable request and subject to participant privacy protections.

REFERENCES

[1] APACHE SOFTWARE FOUNDATION. **Apache HTTP Server Documentation**. [S. l.]: Apache, [2024?]. Disponível em: httpd.apache.org. Acesso em: 29 maio 2025.

[2] MICROSOFT. **C# language documentation**. [S. l.]: Microsoft, [2024?]. Disponível em: learn.microsoft.com. Acesso em: 29 maio 2025.

[3] W3C. **Cascading Style Sheets - home page**. [S. l.]: W3C, [2024?]. Disponível em: www.w3.org. Acesso em: 29 maio 2025.

[4] COMISSÃO NACIONAL DE ENERGIA NUCLEAR. **CNEN-NN-3.01**: Requisitos básicos de radioproteção e segurança radiológica de fontes de radiação. Rio de Janeiro: CNEN, 2025. Disponível em: https://www.gov.br/cnen/pt-br/acesso-rapido/normas/grupo-3/ansn-3-01-requisitos-basicos-de-radioprotecao-e-seguranca-radiologica-de-fontes-de-radiacao.pdf. Acesso em: 30 mar. 2026.

[5] COMISSÃO NACIONAL DE ENERGIA NUCLEAR. **CNEN-NN-6.02**: Licenciamento de instalações radiativas. Rio de Janeiro: CNEN, 2022. Disponível em: https://www.gov.br/cnen/pt-br/acesso-rapido/normas/grupo-6/NormaCNENNN6.02.pdf. Acesso em: 30 mar. 2026.

[6] SIEMENS. **Communication via the CM PtP RS232 of the SIMATIC S7-1500 using Freeport Protocol**. [S. l.]: Siemens Service & Support, [2024?]. Disponível em: cache.industry.siemens.com. Acesso em: 29 maio 2025.

OPEN ACCESS

[7] MORAES, I.; NETO, F.; MOURA, F. Análise para cálculo de blindagem de cabana óptica para linha de luz do Sirius. In: CONGRESSO BRASILEIRO DE METROLOGIA DAS RADIAÇÕES IONIZANTES, 15., 2020, Online. **Anais [...]**. Rio de Janeiro: CBMRI, 2020.

[8] DIAMOND. **Health Physics**: Radiation Safety Training. [S. l.]: IonActive, 2022. Disponível em: ionactive.co.uk. Acesso em: 27 maio 2025.

[9] BOOTSTRAP. **Get started with Bootstrap**. Versão 5.3. [S. l.]: Bootstrap, [2024?]. Disponível em: getbootstrap.com. Acesso em: 29 maio 2025.

[10] WHATWG. **HTML**: Living Standard. [S. l.]: WHATWG, [2024?]. Disponível em: html.spec.whatwg.org. Acesso em: 29 maio 2025.

[11] MOZILLA. **JavaScript**. [S. l.]: MDN Web Docs, [2024?]. Disponível em: developer.mozilla.org. Acesso em: 29 maio 2025.

[12] LIN, T. F.; WANG, J. P. The Safety Interlock System of Synchrotron Radiation Research Center. In: PARTICLE ACCELERATOR CONFERENCE, 1995. **Proceedings [...]**. [S. l.]: IEEE, 1995. p. 2108-2110.

[13] MARIADB FOUNDATION. **MariaDB Documentation**. [S. l.]: MariaDB, [2024?]. Disponível em: mariadb.org. Acesso em: 29 maio 2025.

[14] MAX IV. **Safety requirements for users**. Suécia: MAX IV Laboratory, 2023. Disponível em: www.maxiv.lu.se. Acesso em: 27 jul. 2025.

[15] NODE-RED. **Documentation**. [S. l.]: OpenJS Foundation, [2024?]. Disponível em: nodered.org. Acesso em: 29 maio 2025.

[16] PHP. **Documentation**. [S. l.]: PHP Group, [2024?]. Disponível em: www.php.net. Acesso em: 29 maio 2025.

[17] PROJETO SIRIUS. **A nova fonte de luz brasileira**. Campinas: LNLS, 2014. Disponível em: www.lnls.cnpem.br. Acesso em: 27 maio 2025.

[18] SIEMENS. **6GT2600-1AD00-0AX0**. [S. l.]: Siemens Industry Mall, [2024?]. Disponível em: mall.industry.siemens.com. Acesso em: 29 maio 2025.

[19] SIEMENS. **6GT2831-6CA60**. [S. l.]: Siemens Industry Mall, [2024?]. Disponível em: mall.industry.siemens.com. Acesso em: 29 maio 2025.

OPEN ACCESS

LICENSE

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material.
To view a copy of this license, visit http://creativecommons.org/ licenses/by/4.0/.