Castell

STi
SERV TRAYVOU
INTERVERROUILLAGE

SAFE POWER MANAGEMENT IN DATA CENTRES:

TRAPPED KEY INTERLOCKING FOR DATA CENTRE APPLICATIONS

www.sentricsafetygroup.com



Real-World Data Centre Applications

As data centres grow in scale and power demand, the electrical infrastructure required to support them is expanding at a rapid rate. According to the European Data Centre Association's State of European Data Centres 2026 report, European IT power capacity reached almost 14.8 GW at the end of 2025 and is forecast to grow at approximately 17% annually through 2031. Similar trends are being seen globally. Research from Cushman & Wakefield indicates that APAC operational data centre capacity is expected to double by 2030, while Mordor Intelligence forecasts that installed data centre capacity in the United States will nearly double between 2025 and 2030. As a result, critical power infrastructure is becoming increasingly complex, often incorporating utility supplies, standby generators, transformers, UPS systems, and low, medium, and high-voltage switchgear that must operate together to maintain availability and resilience.

Managing switching and isolation activities within these environments is a critical operational challenge. Incorrect switching sequences can create risks for personnel, disrupt operations, and potentially impact the availability of mission-critical services. At the same time, operators are increasingly deploying highly resilient Tier III and Tier IV facilities, placing even greater emphasis on the safe management of power infrastructure and maintenance activities.

Castell™ and Serv Trayvou Interverrouillage™ (STi) trapped key interlocking solutions are used in critical infrastructure applications worldwide, helping operators manage complex power infrastructure with greater confidence while supporting safety, availability, and operational resilience.

Data Centre Application	Page
Safe Switching with Multiple Power Supplies	4
Safe UPS Maintenance Bypass Switching	6
Safe Static Transfer Switch Maintenance	8
Safe Transformer Switching & Isolation	10
Safe Interlocking & Access Across LV, MV & HV Systems	12



This document outlines the features of our solutions for information purposes only. As configurations may vary, the exact specifications will be agreed with you when the contract is finalised. For advice tailored to your specific situation, please contact our team. All trademarks are the property of their respective owners.

Sources: European Data Centre Association State of European Data Centres 2026; Cushman & Wakefield Data Centre Market Reports; Mordor Intelligence Data Centre Market Forecast Reports.

Why Trapped Key Interlocking for Data Centres?

Trapped Key Interlocking helps data centre designers improve operator safety and reduce the risk of equipment damage and unexpected downtime.

Enhancing Safety

Helps reduce the risk of exposure to live electrical and arc flash hazards by providing physical proof that isolation has been completed correctly before maintenance.

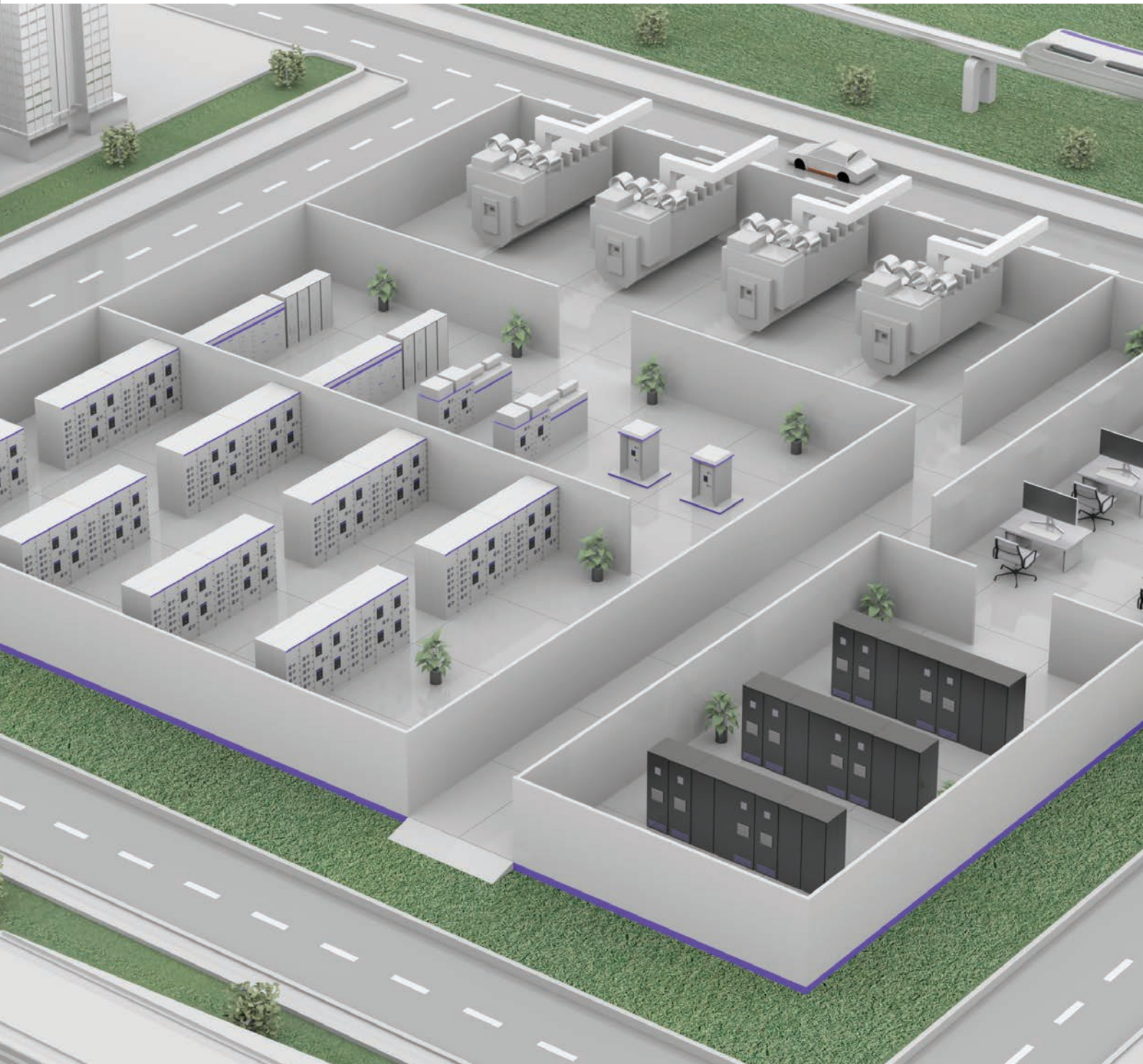
Improving Operational Reliability

Helps ensure consistent, repeatable switching procedures that help reduce human error, minimise equipment damage and downtime.

Adding Value Across the Facility

Trapped key interlocking is a well-established, simple and intuitive method for mechanically managing complex switching sequences. It integrates readily with switchgear and is commonly documented in manufacturers' procedures and technical materials.

The Result: Reduced risk to people and infrastructure, and greater operational resilience across critical data centre environments.



Safe Switching with Multiple Power Supplies

Overview

Continuous power availability is essential in modern data centres. To maintain uptime, facilities are commonly designed with redundant power architectures that allow critical loads to remain energised when supplies are taken offline for maintenance.

For example, a system may be set up with a main supply from the grid and an emergency supply from a generator; these would both be connected to a common distribution system.

These systems can include:

- Low Voltage (LV) and Medium Voltage (MV) switchgear
- Air Circuit Breakers (ACBs)
- Moulded Case Circuit Breakers (MCCBs)
- Distribution busbars

While redundant power systems improve reliability, they also introduce operational complexity.

Understanding the Risks

Operators regularly interact with equipment to transfer loads between power sources, isolate equipment for maintenance, and return systems safely to service while maintaining power to critical infrastructure. However, when done incorrectly, there can be serious consequences.

Common risks include:

Live Electrical Exposure
Equipment believed to be isolated may remain energised, exposing personnel to hazardous electrical energy during maintenance activities.

Backfeeding
Power may flow through unintended paths, energising equipment that operators believe to be isolated.

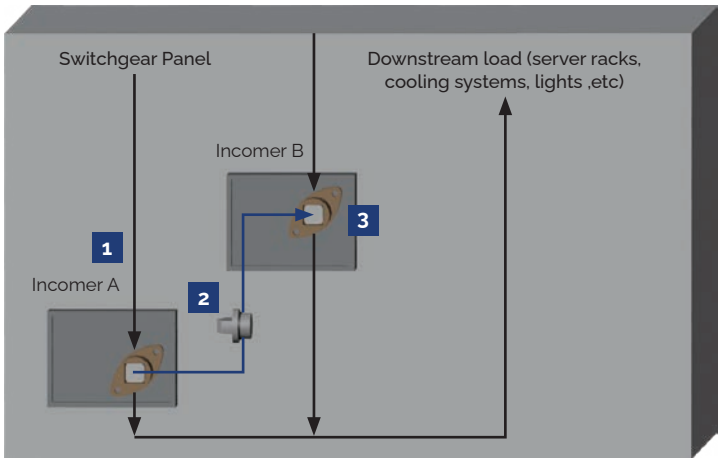
Arc Flash
Unexpected contact with energised equipment can result in arc flash incidents, causing serious injury and equipment damage.

Unintended Paralleling
If two incomers are closed simultaneously in a system not designed for parallel operation, equipment damage, protection issues, system instability, and downtime can occur.

For these reasons, switching and isolation activities must follow a clearly defined sequence to help prevent unsafe operating conditions and ensure maintenance can only proceed once equipment has been safely isolated.

Safe Switching & Isolation with Trapped Key Interlocking

As a general example, in a situation where an operator wants to perform maintenance on Incomer A, a trapped key interlocking sequence may operate as follows:



Safe Switching with multiple power supplies

1. Incomer A is supplying the load and retains a trapped key.
2. Opening Incomer A releases the key, providing physical confirmation that the breaker is open.
3. The released key enables operation of Incomer B or the next step in the switching sequence.

By enforcing the operating sequence, trapped key interlocking helps ensure that:

- Switching operations occur in the correct sequence
- Isolation is achieved before maintenance begins and cannot be unintentionally reenergized
- Multiple supplies cannot be closed at the same time

Key Takeaways

- Incorrect switching operations can result in electrical hazards, equipment damage, and downtime.
- Safe switching requires a controlled and repeatable operating sequence.
- Trapped key interlocking helps control the sequence of operations, supporting safer isolation and maintenance procedures.

Typical Interlocking Solution

Interlocks are installed directly onto the equipment.
The system can be integrated with switchgear from a wide range of manufacturers.

Cam Locks

Typically fitted to Air Circuit Breakers (ACBs) and integrated into the breaker operating mechanism.

 Castell FS Lock	 Castell Q Lock	 STi HBA	 STi ABA

Bolt Locks

Typically fitted to Moulded Case Circuit Breakers (MCCBs), where they physically interfere with breaker operation.

 Castell K Lock	 STi HVE	 STi AVE

Keys

 Castell FS Key	 Castell Q Key	 STi Star Key	 STi Flat Key (Ronis)

Safe UPS Maintenance Bypass Switching

Overview

Uninterruptible Power Supplies (UPS) are critical to maintaining continuous power in data centres. During a loss of utility power, UPS systems provide backup power to keep critical infrastructure online and maintain continuity until normal power is restored.

To ensure reliability, UPS systems require regular preventive maintenance and functional testing. During these activities, operators must safely transfer the load from the UPS onto a maintenance bypass supply, isolate the UPS, and maintain continuous power to critical loads throughout the process.

UPS systems can include:

- UPS modules
- Input and output breakers
- Maintenance bypass breakers
- Control systems for switching between normal and bypass modes

While UPS maintenance is essential to maintaining system reliability, it also introduces operational complexity.

Understanding the Risks

Operators regularly put the UPS into bypass mode for maintenance. When done incorrectly, there can be serious consequences.

Common risks include:

Equipment Damage
The UPS inverter and bypass source must be synchronised before any transfer occurs. Closing the bypass breaker before the UPS inverter and bypass source are synchronised can potentially damage the UPS and cause load disturbances.

Live Electrical Exposure
The UPS may accidentally remain energised during maintenance, exposing personnel to hazardous electrical energy and increasing the risk of injury.

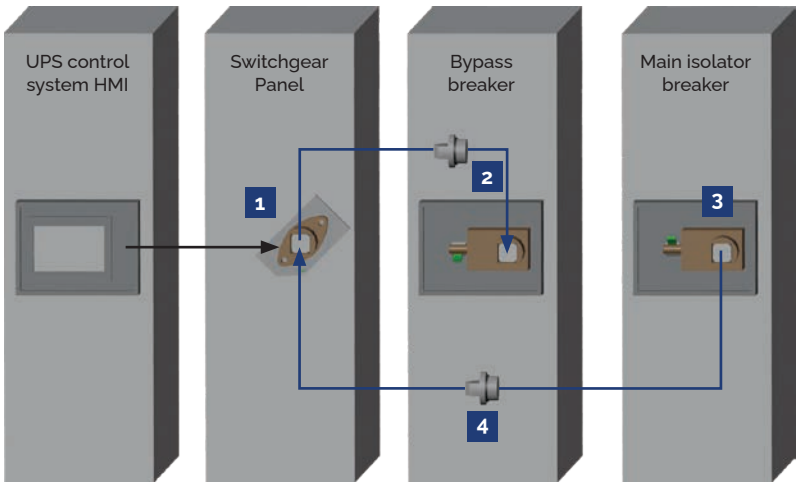
Arc Flash
Unexpected contact with energised equipment can result in arc flash incidents, causing serious injury and equipment damage.

Loss of Critical Load
Incorrect switching or isolation can unintentionally interrupt the power supply to critical systems, resulting in operational disruption and downtime.

For these reasons, UPS bypass and isolation activities must follow a clearly defined sequence to help prevent unsafe operating conditions and ensure maintenance can only proceed once the UPS has been safely isolated.

Safe Switching & Isolation with Trapped Key Interlocking

As an example, in a situation where an operator wants to perform maintenance on a UPS, a trapped key interlocking sequence may operate as follows:



Safe UPS Maintenance Bypass Switching

1. Once the UPS control system confirms the inverter and bypass source are synchronised and ready, a solenoid-controlled key is released.
2. This first key enables closure of the maintenance bypass breaker, ensuring the load remains supplied. The first key is now trapped.
3. The UPS breaker must now be opened and isolated. In doing so, this releases a second key.
4. A second key is returned and trapped in the solenoid-controlled unit to ensure the sequence cannot be reversed until it is safe to do so.

By enforcing the operating sequence, trapped key interlocking helps ensure that:

- The UPS is fully isolated before maintenance begins and cannot be unintentionally re-energised
- Power remains supplied to the critical load
- Operators have clear, physical proof of isolation

Key Takeaways

- Incorrect bypass and isolation operations can result in electrical hazards, equipment damage, and disruption to critical loads.
- By controlling the operating sequence, trapped key interlocking helps reduce the risk of transfer occurring before loads are synchronised and supports UPS isolation prior to maintenance.

Typical Interlocking Solution

Interlocks are installed directly onto the equipment.
These products are commonly installed within switchgear panels and preassembled UPS bypass cabinets.

Cam Locks

Typically fitted to Air Circuit Breakers (ACBs) and integrated into the breaker operating mechanism.


Castell FS Lock


Castell Q Lock


STi HBA


STi ABA

Bolt Locks

Typically fitted to Moulded Case Circuit Breakers (MCCBs), where they physically interfere with breaker operation.


Castell K Lock


STi HVE


STi AVE

Solenoid-Controlled Key Switches

Integrated with the UPS control system, these release a key only when the UPS is synchronised and ready to begin the maintenance sequence.


Castell KSUPS


STi HSE

Keys


Castell FS Key


Castell Q Key


STi Star Key


STi Flat Key (Ronis)

Safe Static Transfer Switch Maintenance

Overview

Static Transfer Switches (STS) are used in data centres to keep critical loads supplied by switching between two independent power sources. An STS transfers the load from the normal utility supply to a backup supply within milliseconds, with no interruption to the critical load if a source fails.

To ensure reliability, STS units require regular preventive maintenance and functional testing. To do this safely, operators must transfer the load onto a maintenance bypass supply and isolate the STS.

STS systems can include:

- Two independent input supplies (normal and backup)
- Input circuit breakers
- An output circuit breaker
- Maintenance bypass breakers

While the STS transfers automatically between sources during normal operation, isolating the unit for maintenance introduces operational complexity.

Understanding the Risks

Operators must transfer the load onto a bypass supply before isolating the STS for maintenance. When done incorrectly, there can be serious consequences.

Common risks include:

Equipment Damage
Paralleling of incoming sources or simultaneous closure of both bypass breakers can result in equipment damage and system instability.

Arc Flash
Unexpected contact with energised equipment can result in arc flash incidents, causing serious injury and equipment damage.

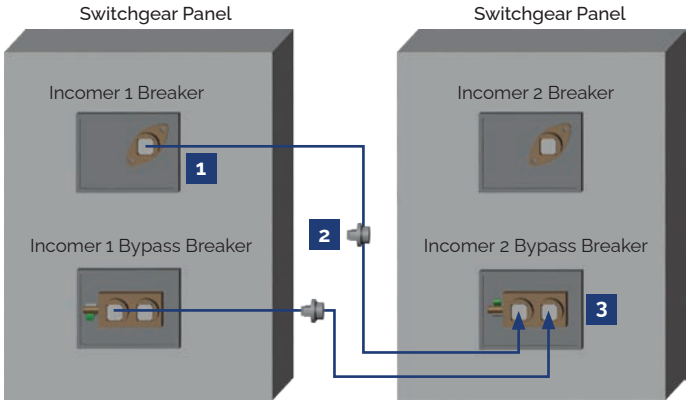
Live Electrical Exposure
The STS may accidentally remain energised during maintenance, exposing personnel to hazardous electrical energy and increasing the risk of injury

Loss of Critical Load
Incorrect switching or isolation can unintentionally interrupt the power supply to critical systems, resulting in operational disruption and downtime.

For these reasons, STS bypass and isolation activities must follow a clearly defined sequence to help prevent unsafe operating conditions and ensure maintenance can only proceed once the STS has been safely isolated.

Safe Switching & Isolation with Trapped Key Interlocking

As an example, in a situation where an operator wants to isolate an STS for maintenance, a trapped key interlocking sequence may operate as follows:



Safe Static Transfer Switch Maintenance

1. To begin maintenance, the input breaker on the opposite side to the chosen bypass path is opened and isolated. In doing so, this releases a key.
2. This released key, together with another key unique to the whole arrangement, must both be inserted into the interlock on the maintenance bypass breaker to close it.
3. With both keys trapped, the maintenance bypass breaker is closed, transferring and maintaining supply to the critical load.

By enforcing the operating sequence, trapped key interlocking helps ensure that:

- Only one bypass path can be established at any one time
- Input sources cannot be unintentionally paralleled
- The STS is isolated before maintenance begins and cannot be unintentionally re-energised
- Power remains supplied to the critical load
- Operators have clear, physical proof of isolation

Key Takeaways

- Incorrect bypass and isolation operations can result in electrical hazards, equipment damage, paralleling of sources, and disruption to critical loads.
- Trapped key interlocking provides a controlled operating sequence designed to help prevent multiple bypass paths from being established simultaneously and to support STS isolation.

Typical Interlocking Solution

Interlocks are installed directly onto the equipment.

Cam Locks

Typically fitted to Air Circuit Breakers (ACBs) and integrated into the breaker operating mechanism.

 Castell FS Lock	 Castell Q Lock	 STi HBA	 STi ABA

Bolt Locks

For STS applications, dual key bolt locks are typically used to interfere with breaker operation.

 Castell K Lock	 STi HVE	 STi AVE

Keys

 Castell FS Key	 Castell Q Key	 STi Star Key	 STi Flat Key (Ronis)

Safe Transformer Switching & Isolation

Overview

Transformers play a critical role by stepping down voltage to be used by equipment like server racks and cooling systems. To maintain uptime and improve resilience, transformers are commonly arranged in a loop feed configuration, allowing each transformer to be supplied by two or more independent power sources.

In normal operation, one source supplies the transformer while the second source remains available as a backup. This arrangement allows operators to transfer supplies during maintenance or in response to a fault without interrupting critical services.

These systems can include:

- Transformers (and associated load break switches, cabinet doors and rooms)
- Low Voltage (LV) and Medium Voltage (MV) switchgear
- Circuit breakers

Transformer systems can be organised radially or as a loop. While loop feed systems improve reliability, they also introduce operational complexity.

Understanding the Risks

Operators regularly interact with loop feed systems to transfer loads between sources and isolate transformers for maintenance. However, when done incorrectly, there can be serious consequences.

Common risks include:

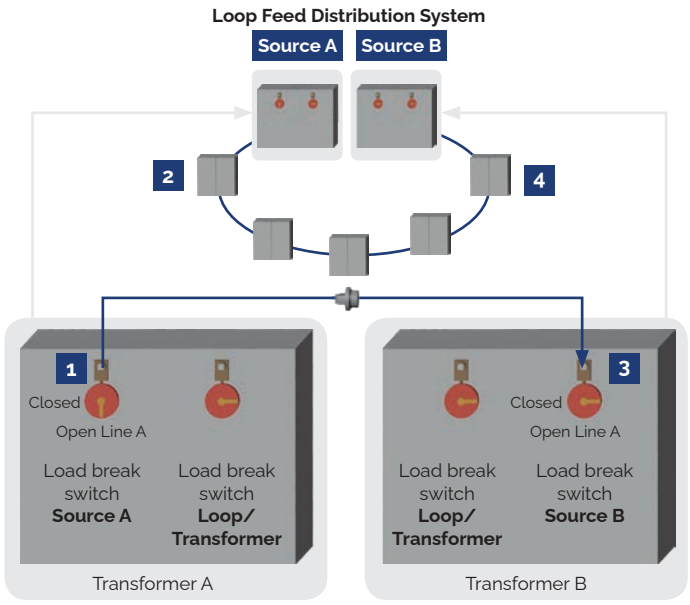
Live Electrical Exposure
Accessing a transformer cabinet before the equipment has been fully isolated may expose personnel to hazardous electrical energy, increasing the risk of arc flash and serious injury.

Equipment Damage
If multiple sources are connected to the transformer loop simultaneously, this paralleling can cause equipment damage, system instability and disruption to operations.

For these reasons, source transfer and isolation activities must follow a clearly defined sequence to help prevent unsafe operating conditions and ensure maintenance can only proceed once the transformer has been safely isolated.

Safe Switching & Isolation with Trapped Key Interlocking

In a situation where an operator wants to transfer the supply in a transformer loop feed system, a trapped key interlocking sequence may operate as follows:



Safe Transformer Loop Feed Switching and Isolation

1. Open the load break switch on Transformer A. This releases a key.
2. Confirm Source A is fully disconnected from the transformer loop feed system
3. Use the key to close the load break switch on Transformer B. The key is now trapped.
4. The loop feed system is now being fed by Source B

If maintenance is required, additional keys may be used to control access to the transformer cabinet or equipment room, and maintenance access is only possible once the transformer has been fully isolated.

By enforcing the operating sequence, trapped key interlocking helps ensure that:

- Multiple sources cannot be paralleled in the transformer loop
- Isolation is achieved before maintenance begins and cannot be unintentionally re-energised
- Operators have clear, physical proof of isolation

Key Takeaways

- Multiple sources must never be connected simultaneously unless the system has been specifically designed for parallel operation.
- Trapped key interlocking provides a physical means of helping to enforce the correct operating sequence, controlling access to transformer cabinets and associated equipment until safe isolation has been achieved.

Typical Interlocking Solution

Interlocks are installed directly onto the equipment.
The system can be integrated with transformers and associated equipment from a wide range of manufacturers.
Custom mounting arrangements can also be provided to suit different equipment configurations.

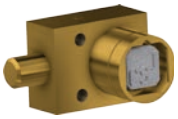
Cam Locks

May be fitted to associated circuit breakers and switchgear.

 Castell FS Lock	 Castell Q Lock	 STi HBA	 STi ABA

Bolt Locks

Typically fitted to transformer equipment, where they physically interfere with load break switches to secure them in position.

 Castell K Lock	 STi HVE	 STi AVE

Keys

 Castell FS Key	 Castell Q Key	 STi Star Key	 STi Flat Key (Ronis)

Safe Interlocking & Access Across LV, MV & HV Systems

Overview

Data centres rely on complex electrical infrastructure to deliver continuous power to critical loads. Power flows from the grid through high-voltage (HV) supply lines and transformers into medium-voltage (MV) switchgear, before being distributed at low voltage (LV) to server racks, cooling systems, and supporting infrastructure.

During scheduled maintenance, testing, or repairs, operators may need to access MV switchgear cabinets and HV transformer cable compartments.

These systems can include:

- Air Insulated Switchgear (AIS)
- Gas Insulated Switchgear (GIS)
- Ring Main Units (RMUs)
- LV and MV circuit breakers
- Transformers

Unlike many other maintenance activities, safe access to this equipment requires a multi-stage isolation and earthing sequence across different voltage levels.

Understanding the Risks

Operators regularly access MV switchgear cabinets and HV cable compartments for inspection, testing, and maintenance. However, when done incorrectly, there can be serious consequences.

Common risks include:

Live Electrical Exposure
Accessing switchgear cabinets or cable compartments before power has been fully isolated can expose personnel to hazardous electrical energy. At medium and high voltages, the energy involved is significantly greater and can result in severe injury.

Arc Flash
Unexpected contact with energised equipment can result in arc flash incidents, causing serious injury and extensive equipment damage.

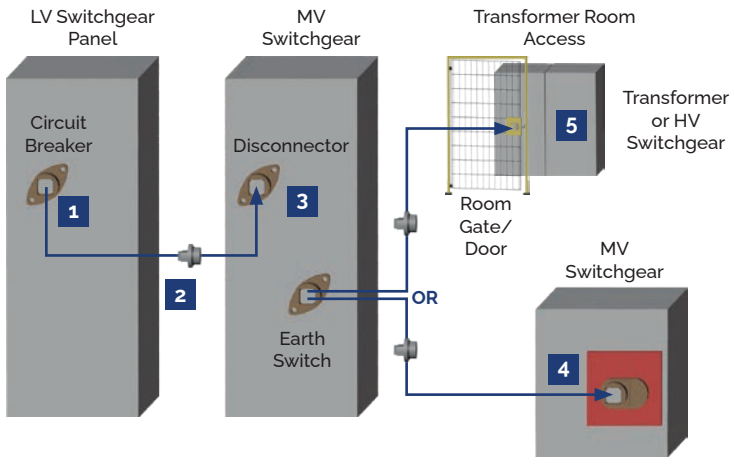
Residual Electrical Energy
If equipment has not been properly earthed, stored energy or induced voltages may still be present, creating hazards for personnel and equipment.

For these reasons, isolation and earthing activities must follow a clearly defined sequence to help prevent unsafe operating conditions and ensure access is only granted once equipment has been made safe.

Safe Switching & Isolation with Trapped Key Interlocking

Trapped key interlocking provides a mechanical method of enforcing safe isolation and earthing sequences. Rather than relying solely on procedures or operator judgement, the system physically controls the order in which equipment can be operated and when access can be obtained.

As a general example, in a situation where an operator requires access to an HV cable compartment, a trapped key interlocking sequence may operate as follows:



Interlocking across LV, MV and HV Systems

1. The LV circuit breaker retains a trapped key while energised.
2. Opening the LV breaker releases a key, providing physical confirmation that the supply has been isolated.
3. This key is used to isolate then earth the MV switchgear.
4. Another key is released to allow access to the MV switchgear cabinet.
5. The final key allows access to the transformer cables.

By enforcing the operating sequence, trapped key interlocking helps ensure that:

- Trapped key interlocking provides a controlled sequence for isolation and earthing procedures, helping operations to be performed in the intended order.
- Once the sequence has been completed, additional keys are released to provide physical proof of isolation and enable safe access to equipment.
- The system prevents the unintentional re-energisation of equipment, supporting safer maintenance activities.

Key Takeaways

- Access to MV switchgear and HV cable compartments requires a controlled isolation and earthing sequence.
- Incomplete isolation or failure to apply earthing can expose personnel to severe electrical hazards.
- Access should only be possible once all relevant voltage levels have been safely isolated and earthed.
- Operators are provided with clear proof of isolation, helping to improve safety and protect critical infrastructure.

Typical Interlocking Solution

Interlocks are installed directly onto the equipment.
The system can be integrated with switchgear and transformers from a wide range of manufacturers and adapted to suit different equipment configurations

Cam Locks

Typically fitted to LV and MV switchgear, circuit breakers, and earth switches, where they physically interfere with equipment operation and enforce the required isolation and earthing sequence.


Castell FS Lock

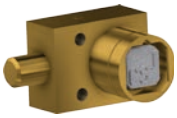

Castell Q Lock


STi HBA


STi ABA

Bolt Locks

Typically fitted to LV and MV switchgear, circuit breakers, and earth switches, where they physically interfere with equipment operation and enforce the required isolation and earthing sequence.


Castell K Lock


STi HVE


STi AVE

Access Locks

Installed on MV switchgear cabinet doors, HV cable compartments, and equipment room doors to prevent access until safe conditions have been established.


Castell D


Castell AI


STi HSP

Keys


Castell FS Key


Castell Q Key


STi Star Key


STi Flat Key (Ronis)

Conclusion

Modern data centres depend on resilient electrical infrastructure and carefully controlled operating procedures to maintain continuous power and protect critical assets. From redundant power systems and UPS maintenance to transformer loop feeds and medium-voltage switchgear, each application presents unique operational challenges and potential hazards.

Safe switching, isolation, and maintenance activities are essential to protecting both personnel and uptime. By physically enforcing critical operating sequences, trapped key interlocking helps reduce the risk of human error and provides clear proof that equipment has been placed in a safe state before work begins.

As electrical systems continue to grow in complexity, maintaining a balance between operational continuity and personnel safety remains fundamental to reliable data centre operation.



Every effort has been made to ensure that the information contained in this document is accurate and complete at the time of publication. The information is provided for general guidance and product description purposes only and does not form part of any contract or constitute guaranteed performance characteristics. Sentric Safety Group™ reserves the right to modify specifications and introduce improvements without prior notice.

Castell™ and Serv Trayvou Interverrouillage™ (STi) are registered trademarks of Sentric Safety Group™



Castell Safety International
The Castell Building, 217 Kingsbury Road
London, NW9 9PQ, UK
VAT registration number: GB649964668
Registered in England & Wales
with company number: 01514709

Tel: **+44 (0)20 8200 1200**
Email: **sales@castell.com**
www.sentricsafetygroup.com

Serv Trayvou Interverrouillage (STi)
1ter Rue du Marais – Bât. B
93106 Montreuil Cedex
France
Numéro SIRET 39143896700021
RCS Bobigny B 391 438 967

Tel: **+33 1 4818 1515**
Email: **sales@servtrayvou.com**
www.sentricsafetygroup.com

Sentric China
2nd Floor, Building 63
No. 421 Hongcao Road
Xuhui District, Shanghai, China
Post code: 200233

Tel: **+86 21 60407398**
Email: **mkt.china@sentricsafetygroup.com**
www.sentricsafetygroup.com

TOGETHER FOR A SAFER TOMORROW

© 2026 Sentric Safety Group. All rights reserved.

AG-EN-C-DC-0926