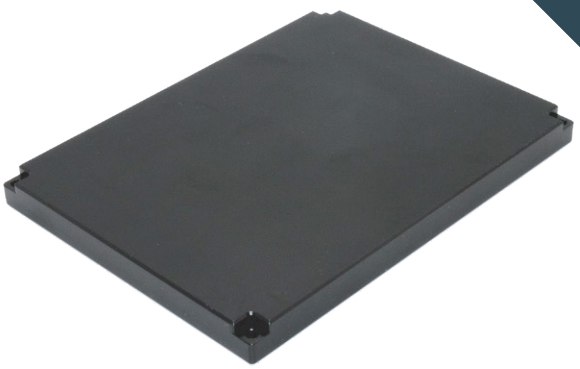
TE CONNECTIVITY TAMPER DETECTION SENSOR

Application Note for Handling and Assembly Procedures





EVERY CONNECTION COUNTS

TABLE OF CONTENTS

INTRODUCTION.....3

GENERAL.....4

Objective.....4

Sensor Electrical Connections.....4

Sensor Physical Attachment.....6

SHIPPING AND TRANSPORTATION.....6

Factory Packaging.....6

INCOMING RECEIVING.....6

Proper Handling.....6

Visual Inspection.....6

Electrical Operation.....6

INVENTORY GOOD PRACTICE.....7

Environmental Conditions and Contro.....7

Inventory Management.....7

Shelf Life.....7

ASSEMBLY TO A PC BOARD.....7

PC Board Mounting Guidelines.....7

Permanent Bond Attachment.....7

Conductive Film Attachment.....8

Cleaning and Preparation of Mating Surfaces 8

Thermal Management Features.....8

Operator Procedures and Protections.....9

Cleanliness Control.....9

Mechanical Handling.....9

Electrostatic Discharge (ESD).....9

Electrical Connections.....9

FPC Tail Connection.....9

FPC Tail with Solder Pads.....9

Compression Pad Connections.....10

Compression Connectors for Interior Connection.....10

Physical Attachment and Mounting Hardware 10

RECOMMENDED TEST AND ASSEMBLY FIXTURES.....11

Strategy and Caution.....11

Test Fixtures.....11

Incoming Receiving Test.....11

Assembly Station Test.....11

Post Assembly Test.....11

Assembly Fixtures.....11

Adhesive Frame Alignment Fixture.....11

PC Board Alignment Fixture.....11

Adhesive Cure Fixtures.....11

POST ASSEMBLY TESTING AND TROUBLESHOOTING.....12

Testing After Installation.....12

Removal From an Assembly and Reattachment.....12

Troubleshooting.....12

DISPOSITION OF DEFECTIVE, NON-CONFORMING, AND OBSOLETE DEVICES.....12

INTRODUCTION

The TE Connectivity (TE) tamper detection sensor provides a compact, high-security solution for detecting physical tampering in small, secure enclosures. The sensor creates a continuous physical barrier around sensitive assets and is designed to register any penetration of that barrier. In addition, the sensor incorporates features that detect attempts to bypass, disable, or remove the sensor itself.

When installed, the tamper sensor establishes a secure perimeter around the protected asset. The device provides a high-speed, binary electrical output (N.O. or N.C.) that signals a tamper event within milliseconds. In addition to its primary switching function, the sensor's electrical parameters, including element resistance and capacitance, may be monitored to detect secondary indicators of tampering or attempts to compromise the device.

The TE tamper detection sensor is widely deployed in high-security systems that require compliance with government, industrial, or commercial security standards. Typical applications include systems subject to FIPS (Federal Information Processing Standards) 140 and PCI-HSM (Payment Card Industry – Hardware Security Module) requirements. TE Connectivity also follows established internal protocols that align with ITAR standards for the development and manufacture of security-related components.

This document outlines recommended methods and practices for handling and assembly of the tamper detection sensor during manufacturing to enable reliable performance and long-term durability.

GENERAL

Objective

For optimal performance, the tamper detection sensor must be fully integrated into the end-product design. The device functions as a physical barrier surrounding a protected asset and is engineered to detect any breach, penetration, or attempt to remove or circumvent the barrier. The sensor is designed to attach to a PC board and cover critical components, chips, and circuits. The sensor engages the board along its perimeter and is attached with adhesives and/or fasteners. A second cover can be attached to the underside of the PC board to create a fully protective envelope around the critical assets. See figures 1 and 2.



Figure 1 – Tamper Sensor Cover

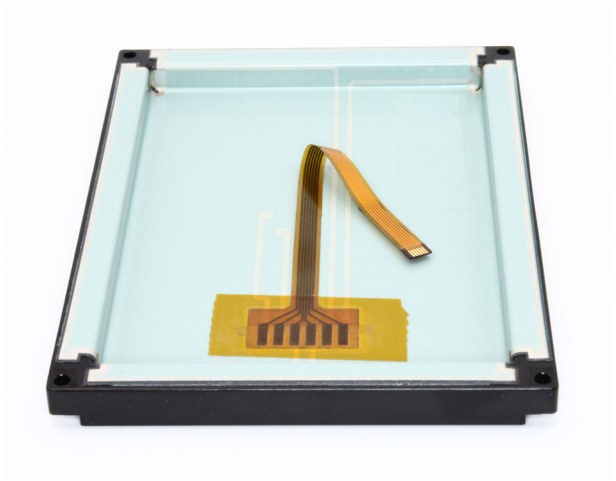


Figure 2 – Tamper Sensor Underside

Sensor Electrical Connections

Three configurations are available to make electrical connections to the tamper sensor:

- An FPC tail is permanently bonded to the interior surface of the tamper sensor housing. The opposite termination of the tail is designed for insertion into an FPC connector mounted on the printed circuit board (PCB) and positioned within the secure perimeter. Refer to Figures 3 and 4 for illustration of this configuration.

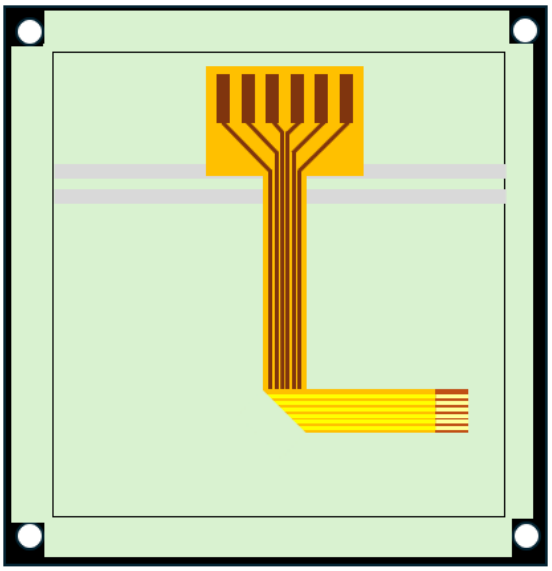


Figure 3 - Underside Showing FPC

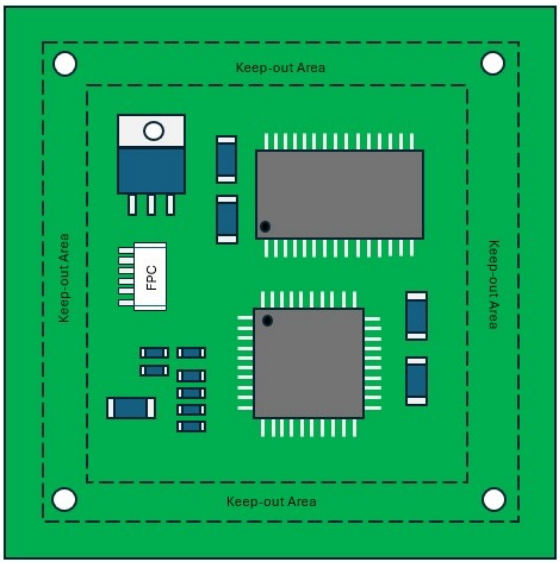


Figure 4 - PCB Layout for FPC Connection

- Electrical compression contacts may be incorporated along the perimeter mounting surface of the tamper sensor. These contacts align with corresponding conductive pads on the printed circuit board (PCB), as shown in Figures 5 and 6. During assembly, fasteners secure the sensor to the PCB, confirming that all contacts establish electrical connection. A Z-axis conductive film is positioned between the sensor contacts and the PCB pads to enhance connection reliability.

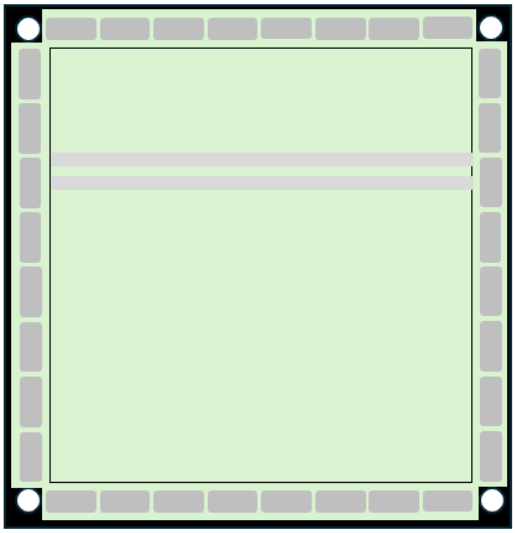


Figure 5 - Underside Showing Compression Contacts

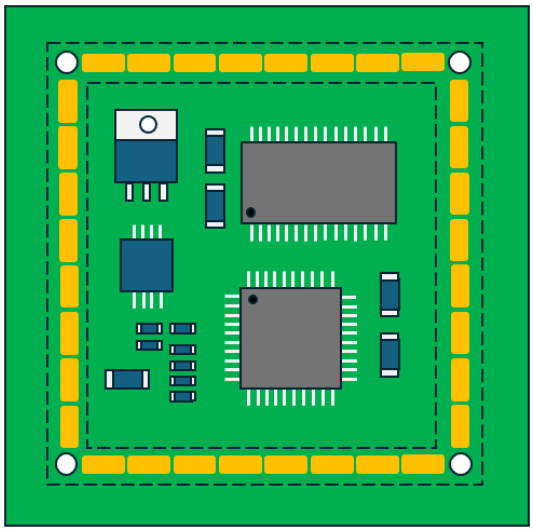


Figure 6 - PCB Layout for Compression Contacts

- Another connection approach is to use the same contact pad scheme as shown in Figures 5 and figure 6 but utilize Zebra strip connectors along the connection pad areas. Zebra strip is a compression type connector that has vertically oriented alternating layers of conductive and non-conductive silicone. Zebra strip provides a very reliable connection between conductive pads when sandwiched between the tamper sensor and PC board. Proper orientation of the Zebra strip is shown in figure 7 and figure 8.

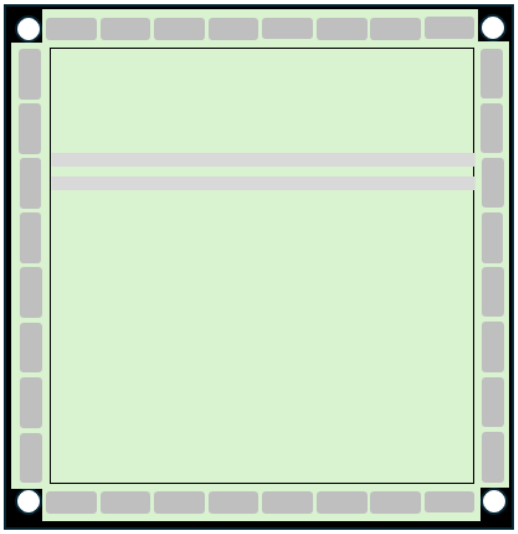


Figure 7 - Underside Showing Compression Contacts

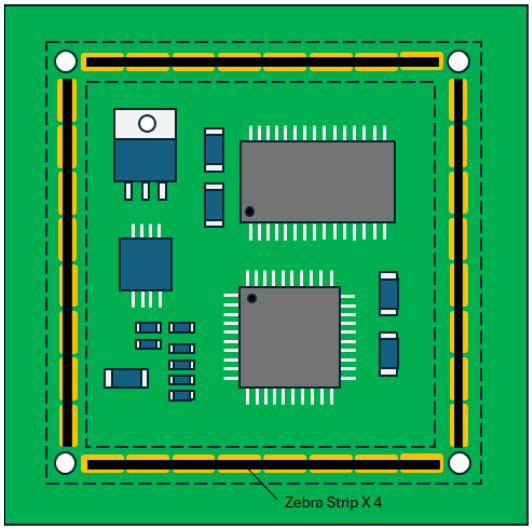


Figure 8 - Layout for Zebra strip Contacts

Sensor Physical Attachment

Two primary attachment configurations are available for securing the tamper detection sensor to the printed circuit (PC) board: adhesive bonding and electrical bonding.

In the adhesive bonding design, the tamper detection sensor is bonded to the PC board using a thermoset adhesive applied between the sensor perimeter flange and the board surface. Mechanical fasteners are used to maintain sensor alignment and stability during the adhesive curing process.

In the electrical bonding design, the tamper detection sensor is secured to the PC board exclusively with fasteners. A Z-axis conductive film is inserted between the sensor mounting flange and the board during assembly. When the fasteners are tightened, this film helps provice reliable electrical continuity between the sensor and the PC board.

Both attachment methods are engineered to trigger detection if the tamper detection sensor is removed or compromised. This enables rapid response to intrusion attempts and helps maintain system security integrity.

SHIPPING AND TRANSPORTATION

Factory Packaging

Tamper detection sensors are manufactured in a controlled cleanroom environment to protect product integrity. Following fabrication, each sensor may be individually packaged in protective bags and/or loaded into custom thermoformed trays. These trays are subsequently placed into cardboard overpacks for shipment. Customer-supplied tray designs may be utilized if required, with consignment to TE permitted upon agreement.

INCOMING RECEIVING

Proper Handling

If the customer has an incoming or receiving inspection and test requirement, it's important to unpack the tamper detection sensors in a clean area free of dust, dirt, debris, and contamination sources. Certain designs of the tamper detection sensor electrical connections rely on an intimate compression fit to a PC board and any contamination on the connecting pads can interfere with reliable operation.

Visual Inspection

Tamper detection sensors should undergo visual inspection to verify the absence of surface contamination, physical damage to the sensor body or electrical contact features, and signs of delamination from the underlying cover or housing. Upon completion of inspection, the sensor should be returned to its original packaging and resealed to preserve cleanliness and protect against handling-related contamination.

Electrical Operation

Tamper sensors incorporate electrical features designed to provide output signals when a tamper event or perimeter breach is detected. Verification of sensor integrity should be performed using a dedicated electrical test fixture. The fixture interfaces with the sensor and enables measurement of key parameters, including electrical continuity, open-circuit conditions, resistance, and capacitance.

Because tamper detection sensor designs vary, most applications will require a custom test fixture to support accurate performance validation. For assistance with fixture design and test methodology, contact the TE Connectivity engineering team.

For tamper detection sensors utilizing compression pad connections, test fixtures should employ spring-loaded contact pins (pogo pins). **Contact pins with sharp or pointed ends must not be used, as they can cause permanent damage to the sensor.** Pins with a rounded tip (R-type) or flat tip (F-type) are recommended to promote reliable contact while maintaining sensor integrity.

INVENTORY GOOD PRACTICE

Environmental Conditions and Control

The sensors should be transported and stored in conditions that do not exceed these limits:

- Temperature: -40 to +60^{0}C
- Humidity: 0 to 60% RH typical. If exposed or stored in a high humidity environment, it's recommended to dry the sensors prior to installation. 48 hours in a humidity of <20 RH will be sufficient.
- Shock and Vibration: ±20g in any axis

Inventory Management

Tamper sensors are serialized, marked with a date code and lot number for traceability. These identifiers support customer inventory management practices, including first-in/first-out (FIFO) and last-in/first-out (LIFO) strategies, as well as safety stock rotation and control of overstock storage. Proper use of these markings supports efficient material handling and reduces the risk of deploying aged or expired components.

Shelf Life

Due to the stability of materials used in the sensor, shelf life can be 8 years or longer if environmental conditions listed above are not exceeded.

ASSEMBLY TO A PC BOARD

PC Board Mounting Guidelines

Most tamper detection sensors are mounted directly to a printed circuit (PC) board to provide coverage over critical or security-sensitive components. The sensor incorporates a perimeter mounting flange along its bottom edge, which interfaces with a designated mating area on the PC board. This flange-to-board interface forms part of the secure perimeter and must be sealed to maintain system integrity. An adhesive layer or conductive/insulating film is typically applied at this interface to help provide reliable attachment and tamper resistance.

Once mounted, any attempt to lift the sensor from the board surface or to intrude laterally into the flange interface is detected as a tamper event. To help maintain assembly integrity, the tamper detection sensor must be installed only after all other PC board components have been placed and soldered. **The sensor is not compatible with wave soldering, infrared (IR) reflow, or aqueous cleaning processes, and should not be subjected to these operations.**

Depending on the design of the tamper detection sensor and the connection means, one of two assembly processes is recommended:

Permanent Bond Attachment

Tamper detection sensors that use an FPC tail for electrical connection should use a structural adhesive film between the sensor flange and PC board. TE can suggest recommendations if desired. These films result in a high bond strength over a broad temperature range as well as high fracture resistance and peel strength.

Bonding film may be applied as four individual strips, one along each perimeter edge of the tamper sensor, or as a single die-cut frame applied in one operation. Films supplied with a release liner on one side offer improved handling stability. In this case, apply the adhesive with the liner to the sensor flange, remove the liner, and then position the assembly onto the PC board. During attachment, ensure precise alignment of sensor mounting holes with the corresponding PC board holes.

Structural adhesive films typically require elevated temperature and pressure to achieve full bond strength. Refer to the adhesive manufacturer's (e.g., 3M) technical data sheet for detailed bonding and curing procedures.

Once bonded, the sensor cannot be lifted or repositioned without triggering a tamper event. Any attempt to remove the sensor will cause permanent damage, rendering the device nonfunctional and requiring replacement.

Conductive Film Attachment

For tamper detection sensors that employ conductive pads along the mounting flange for electrical interface, the use of specialized Z-axis conductive films is recommended. These materials conduct only in the thickness (Z) direction and, when compressed between the sensor flange and a PC board with aligned conductive pads, establish a reliable electrical path. No lateral conductivity occurs between adjacent pads, thereby preventing shorting or cross-talk.

Conductive films and adhesives are typically supplied with a release liner on one side to improve handling during placement. The recommended procedure is to first apply the film with liner to the sensor flange, remove the liner, and then position the assembly onto the PC board. Careful alignment is required to help ensure that sensor mounting holes and conductive pads register precisely with their corresponding features on the PC board.

When attached using adhesive film, the sensor becomes permanently bonded to the board. Any attempt to lift or reposition the sensor will generate a tamper event and cause irreversible damage, requiring sensor replacement.

In contrast, some conductive films contain no adhesive properties. When these films are used, the sensor may be lifted, removed, and repositioned without damage to sensor features.

Cleaning and Preparation of Mating Surfaces

The performance and integrity of the tamper detection sensor are dependent on the cleanliness of all mating surfaces. Contamination in the form of dust, dirt, or debris may compromise sensor function, reduce detection effectiveness, and increase susceptibility to perimeter penetration. For sensor designs utilizing perimeter connection pads, clean pad surfaces are essential to enable reliable electrical contact.

Contaminants observed on the sensor surface should be removed using low-pressure clean air or by gently wiping with a lint-free cloth. **Solvents, detergents, and abrasive cleaning compounds should not be used, as these materials may damage the sensor or degrade surface quality.**

Similarly, the PCB mounting surface must be maintained in a clean condition, free of dust, debris, and other contaminants. Cleaning of PCB mounting areas may be accomplished with dry air, a soft lint-free cloth, or isopropyl alcohol to effectively remove contaminants and finger oils.

Thermal Management Features

In certain applications, components located beneath the tamper detection sensor generate heat that must be transferred to the exterior cover for dissipation. To facilitate this thermal conduction, additional features, hardware, or materials may be incorporated during sensor-to-PC board assembly. Common solutions include non-conductive thermal transfer pads, metallic heat spreaders, thermal interface compounds, gels, and thermoelectric cooling elements.

Specific assembly procedures should be developed to document the installation and placement of these thermal management components. Refer to Figure 7 for illustration.

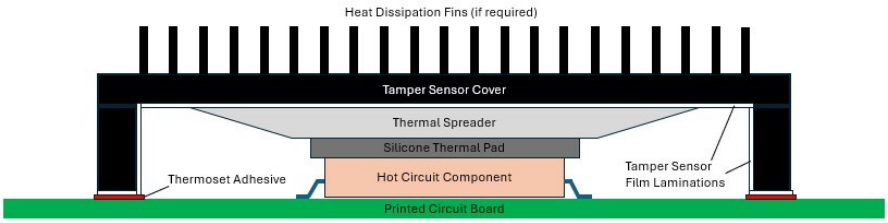


Figure 9 - Location of Heat Dissipation Components

Operator Procedures and Protections

Assembly personnel and all production floor staff responsible for handling tamper detection sensors should be made aware of the following considerations:

Cleanliness Control

The tamper detection sensor, particularly the mounting surfaces, must remain free of contamination to ensure proper system performance. During handling and assembly, operators should use protective measures to prevent transfer of finger oils, perspiration, lotions, or other contaminants. Finger cots or latex gloves are recommended.

Mechanical Handling

The sensor must be protected from dropping or rough handling, which can result in blemishes, dents, scratches, or deformations that compromise functionality. Following any incident of mechanical impact, the sensor should undergo visual inspection and an electrical re-test. Devices exhibiting deformation or damage along the mounting surface must be scrapped.

Electrostatic Discharge (ESD)

The tamper sensor does not exhibit high sensitivity to ESD. Standard workstation precautions—such as wrist straps, grounded bench mats and floor mats, and static neutralizers—are sufficient for protection.

Electrical Connections

The tamper detection sensor incorporates electrical circuits that form an integral part of the tamper detection system and require reliable electrical connections. Two connector schemes are employed for interfacing the sensor with the system:

FPC Tail Connection

The tamper detection sensor may include a Flexible Printed Circuit (FPC) tail extending from the inner surface or edge of the sensor. The tail is designed to interface with a standard FPC female connector mounted on the PC board within the protected area. Prior to mounting the tamper detection sensor, the FPC tail should be fully inserted into the connector, ensuring complete engagement (bottomed) in the connector cavity. For connectors equipped with a latch, verify that the latch is closed and locked after insertion. During sensor installation, the FPC tail should be carefully folded in an accordion configuration to fit beneath the sensor without contacting other assembly components. Once the sensor is secured to the PC board, the FPC connection cannot be accessed or re-inserted. Any attempt to remove the sensor will cause irreversible damage, and the sensor must be discarded. Refer to Figure 8 for illustration.

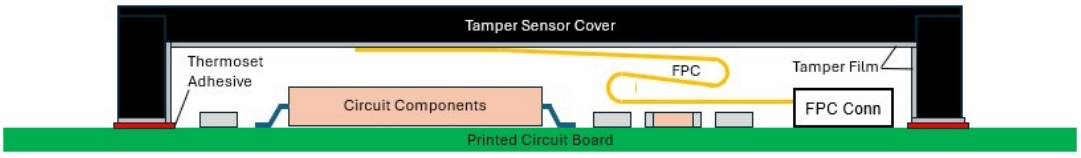


Figure 10 - FPC Folding Location

FPC Tail with Solder Pads

An alternative FPC tail design terminates in multiple solder pads for direct attachment to the PC board. Each pad includes a central via to facilitate solder flow and enhance mechanical and electrical connection. Soldering shall be performed using a temperature-controlled soldering iron, with dwell times selected to confirm proper solder joint formation without damaging the FPC or PC board. Careful orientation of the first pad is critical to confirm proper registration of all remaining pads with their corresponding PC board pads. Use of a clamping or alignment fixture is recommended to improve process efficiency and maintain consistent pad alignment.

Compression Pad Connections

Certain tamper detection sensor designs incorporate connection pads along the bottom surface of the mounting flange. These pads align with corresponding conductive pads on the PC board, and electrical contact is established via the previously described conductive films. Proper orientation and placement of the sensor are critical to help ensure reliable connections. Mounting holes in both the sensor flange and PC board provide registration, and the use of guide pins is recommended to facilitate accurate alignment. Depending on the type of conductive film employed, the sensor may be removable and repositionable if necessary. For other film types, the attachment is permanent; removal will result in sensor damage, and the device must be discarded.

Compression Connectors for Interior Connection

As with compression pad connections, alignment of the tamper detection sensor to the connectors on the PC board is critical. Ensure the sensor is aligned with any outline markings printed on the PC board.

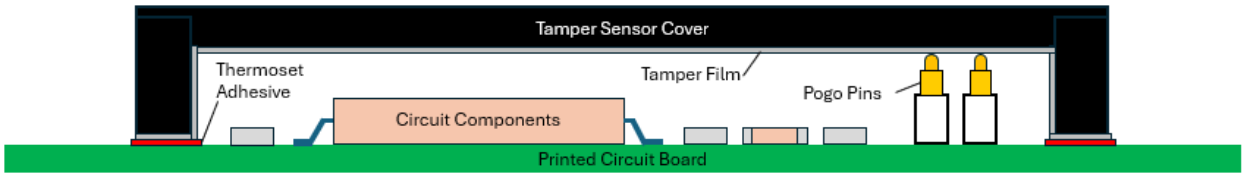


Figure 11 – Interior compression connectors (pogo-pins)

Physical Attachment and Mounting Hardware

Most tamper sensors include mounting holes located in the corners and/or along the perimeter flange. These holes are designed to align with corresponding holes in the PC board and should be secured with fasteners to maintain proper sensor-to-board attachment.

For sensors with conductive connection pads integrated into the mounting flange, the use of bolts, nuts, and washers is mandatory. Z-axis conductive films installed between the flange and the PC board require controlled compression to help ensure reliable electrical contact. Fasteners should be torqued to a predetermined value appropriate for the selected hardware size and type. Lock washers or thread-locking compounds are recommended in high-vibration environments to prevent loosening.

For sensors employing an FPC connection tail, flange compression is less critical. In these cases, alternative attachment methods such as rivets, blind rivets, eyelets, push-tight fasteners, or equivalent clamping solutions may be used effectively.

Self-tapping screws are not recommended. The debris generated during installation can contaminate the flange interface and compromise the integrity of the sensor attachment.

RECOMMENDED TEST AND ASSEMBLY FIXTURES

Strategy and Caution

Once the tamper detection sensor is secured to the PC board, removal is extremely difficult without generating a tamper event. In most designs, removal also results in permanent, non-repairable damage to the sensor, requiring replacement. For this reason, pre-assembly testing is strongly recommended to verify proper operation of all elements of the tamper detection system prior to final attachment. The use of dedicated test and assembly fixtures is advised to oonfirm functionality and reliability of the completed assembly.

Test Fixtures

These test fixtures are recommended:

Incoming Receiving Test

A dedicated test system should be used to evaluate all electrical parameters of the tamper detection sensor. Measurements include verification of continuity for designated circuits, isolation between independent circuits, and evaluation of circuit resistances and capacitances. For sensors with an FPC tail connection, insertion into the test system is sufficient to perform all electrical tests. For sensors with flush conductive pads along the mounting flange, a bed-of-nails or pogo-pin fixture is recommended. Care must be taken to confirm that the fixture does not compromise the integrity of the connection pads, which are designed to be mechanically fragile.

Assembly Station Test

A similar test fixture at the assembly station can be used to confirm proper sensor operation just prior to attachment to the PC board.

Post Assembly Test

Testing can be done only by powering up the system and checking to see that all features are operating properly.

Assembly Fixtures

These assembly fixtures are recommended:

Adhesive Frame Alignment Fixture

A fixture onto which a sensor can be placed upside down with pins protruding through the mounting holes in the flange. Pre-cut adhesive frames can be placed onto the mounting surface of the sensor and located properly using the pins through mating holes in the adhesive frame. This confirms proper alignment of the sensor flange and adhesive.

PC Board Alignment Fixture

A similar fixture with alignment pins will help to locate the sensor/adhesive film onto the PC board. Place the PC board onto the pins first and then drop the sensor/adhesive assembly into place.

Adhesive Cure Fixtures

For sensors using thermoset adhesives, the PC board with sensor properly located must be baked at elevated temperature to create a secure adhesive bond between the sensor and board. The sensor must also be clamped with pressure as recommended by the adhesive manufacturer. Placing clamped assemblies in a temperature-controlled oven is the most common method for this step. Clamps can be removed after the assembly has cooled to room temperature.

POST ASSEMBLY TESTING AND TROUBLESHOOTING

Testing After Installation

The tamper detection sensor is designed with security as a primary operational requirement. To prevent external probing or reverse engineering, no test pads or test points are exposed on the exterior surfaces of the device. This design approach eliminates potential access paths that could otherwise be exploited to evaluate internal circuitry or compromise the security features of the sensor.

Removal From an Assembly and Reattachment

In all applications, removal of the tamper detection sensor from the PC board will generate a tamper signal to the system. When the interface film incorporates adhesive, sensor removal will result in permanent damage, rendering the device non-repairable and requiring scrapping. In configurations where the interface film is non-adhesive, the sensor may be removed and reinstalled. In these cases, the mating surfaces must be inspected to confirm they are free of dust, debris, or other contamination prior to reassembly. During reattachment, the specified hardware torque values must be followed to help ensure proper sealing and reliable system performance.

Troubleshooting

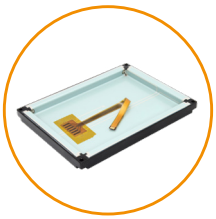
A non-functional “dummy” tamper detection sensor can be implemented to emulate the electrical connections and operational characteristics of a production sensor. When installed on the PC board, the dummy device presents itself to the system as a fully functional tamper sensor. This approach allows differentiation between failures originating in the sensor and those occurring within the associated electronic circuitry. The dummy unit may incorporate diagnostic electronics and visual indicators to aid in fault isolation and system troubleshooting. For development of such diagnostic hardware, contact TE engineering support.

DISPOSITION OF DEFECTIVE, NON-CONFORMING, AND OBSOLETE DEVICES

The TE Tamper Detection Sensor is a critical component of perimeter security systems, providing detection and notification of attempts to breach secured enclosures. Due to the sensitive nature of its design and operation, strict precautions must be taken to prevent unauthorized access to technical details.

Defective, damaged, non-conforming, or obsolete tamper detection sensors represent a potential security risk. If recovered and analyzed, these devices could enable reverse engineering efforts that reveal methods to circumvent detection mechanisms. Such information could compromise the integrity of a security system.

To mitigate this risk, tamper detection sensors that are not incorporated into secure products must be disposed of in a manner that prevents disassembly, reverse engineering, or analysis. Physical destruction is the recommended method of disposal. Devices should be rendered permanently inoperative by shredding, incineration, or other means that make the sensor unrecognizable and unusable.



Tamper Detection Sensors

Secure what matters:

Intelligent tamper detection for maximum physical protection

Connect With Us

For help and assistance regarding the tamper sensor and how best to work with it in a manufacturing environment, please fill out the contact form provided here: Tamper Detection Sensors

TE Connectivity
Sensors

te.com

TE, TE Connectivity, TE connectivity (logo), and EVERY CONNECTION COUNTS are trademarks owned or licensed by the TE Connectivity plc family of companies. Other product names, logos, and company names mentioned herein may be trademarks of their respective owners.

The information given herein, including drawings, illustrations and schematics which are intended for illustration purposes only, is believed to be reliable. However, TE Connectivity makes no warranties as to its accuracy or completeness and disclaims any liability in connection with its use. TE Connectivity's obligations shall only be as set forth in TE Connectivity's Standard Terms and Conditions of Sale for this product and in no case will TE Connectivity be liable for any incidental, indirect or consequential damages arising out of the sale, resale, use or misuse of the product. Users of TE Connectivity products should make their own evaluation to determine the suitability of each such product for the specific application.

© 2025 TE Connectivity. All Rights Reserved.

06-26