15370 Barranca Parkway
Irvine, CA 92618
USA

Physical Reader Security, Tamper and Supervisor Features

APPLICATION NOTE

AN0112, Rev B.0

1 Introduction

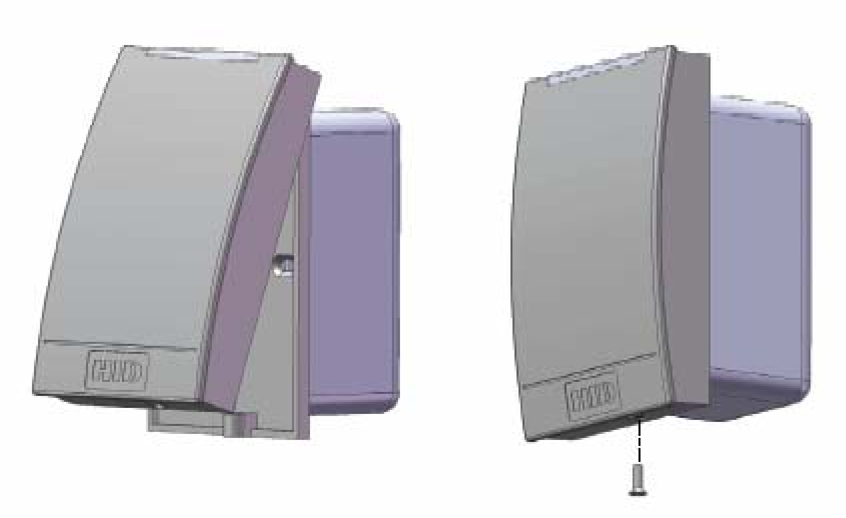
HID Global offers a variety of reader products, many of which include physical anti-tampering and supervisory functions. These security functions disable reader functionality and notify access systems of physical tampering states or power loss through a variety of methods.

When the reader cover and core are removed (from the reader mounting plate or spacer), or the reader loses power, access systems receive tamper signals and heartbeat (I'm Alive) messages receive unexpected reader states. Upon alarm notification, facility managers may take appropriate action, sending guards to readers or reviewing video to determine if facility or system breeches have occurred. This application note summarizes HID Global Physical Access Reader tamper and supervision capabilities and the associated field implementation details.

2 The Basics

2.1 Reader Mounting

HID Prox and iCLASS readers typically encompass two or three components that include the mounting plate, reader electronics and reader cover. Recommended is securing the assembly using a tamper resistant screw because it adds the requirement of non-standard tools to uninstall readers. The following pictures show the installation of a two-piece iCLASS Reader utilizing the security screw that is included with the reader (HID Global Part Number 400-2D71-06).



2.2 Reader Supervision

Implement a variety of methods to monitor the presence of a reader. If powering the readers off, a change in the reader state signals to an access control system that the reader is no longer online (for example, disconnected power or cut wires). Methods to supervise the reader include the following.

- Hard Supervision – physical tamper wire(s) supervised by a panel using a technique that involves an additional pair of wires connected together through a resistor at the reader. The panel using this technique monitors this loop, and detects cuts, shorts, or if other electrical characteristics of the wires are changed.
- Soft Supervision – readers configured to output an I'm Alive, over a cyclical period, notify the panel that the reader is online and working. If there is a disruption in the I'm Alive cycle (an example is from once every minute to non-existent), the panel detects a change in the reader state.

2.3 Reader Tampering

Implement a variety of methods monitor the physical tampering of a reader. More specifically, the removal of the reader cover that is required as a first step to removing the reader from the wall.

- Hard Tampering – connect physical tamper wire(s) in between the reader and panel to provide physical supervision on reader installation. If separating the reader core from the backplate, a tamper switch activates a state change in the wire(s). An advantage of the hard implementation is that hooking up the output to an external relay triggers a sounder or other notification device. HID Global readers provide either physical or optical tamper switches.
- Soft Tampering – configure readers to output an I'm Alive over a cyclical period notifying the panel that the reader is online and operational. If separating the reader core from the backplate, the I'm Alive is modified, thus notifying the panel of the change in reader state.

3 Tamper and Supervisor Implications

3.1 Hard Implementation (Physical Wiring)

All implementations of tampering and supervision involve the additional physical reader hookup of one to two additional conductors. If these conductors do not exist, pull wire in order to hookup the feature. Additionally, tamper and supervision input(s) must be available on the access control (or intrusion) system's reader interface units. Furthermore, ensure a complementing feature is available in the physical access control system to accept and process the tamper signal. To reduce costs of additional deployment, HID recommends limiting implementation of tamper to only perimeter and high security doors, or providing a soft implementation of tamper if possible.

3.2 Soft Implementation (Augmenting Physical Wiring)

Many HID Global readers offer soft implementation of tamper or supervision. During soft implementation, the readers must provide the feature and the panel and associated access control system must have compatibility with the feature. It may be less expensive to replace a reader capable of software tamper implementation than pulling wire to an existing reader to provide the hard implementation.

Note: Some legacy access control panels are not upgradeable and may not provide compatibility with the I'm Alive feature. Additionally, panel's setup to receive 8-bit burst keypad messages may be confused by the I'm Alive feature. The access control panel's confusion depends on the I'm Alive normal / off-normal value in relation to individual key outputs and the unique implementation of the panel. Consult your system provider determining if tamper or supervisor implementation limitations exist.

4 Reader Tamper and Supervision Implementation

4.1 iCLASS

There are up to three iCLASS reader tamper and supervisor options (depending on the model and version of the product installed). The options are mutually exclusive and therefore only one hard or one soft tamper/supervision behavior exists at one time. The tamper and supervision options include the following.

- Open Collector (hard, single physical wire)
- I'm Alive (soft, utilizes pre-existing Wiegand wires)
- OSDP (soft, utilizes pre-existing reader OSDP communication interface)

When tamper detection is enabled[1], the tamper response is one of the following.

- **Open Collector**. The reader open collector line is sinked from a high state (5VDC) to a low state (Ground). The open collector line always behaves in this manor and cannot be inverted. See the product installation guide (www.hidglobal.com > Support > Document Library) for open collector line specifics.
- **I'm Alive**. During a tamper state, the I'm Alive[2] message is inverted.
- **OSDP**. Upon reception of a Reader Status Report Request (0x67), the reader responds with a Reader Tamper Status Report (0x4B). For more information, contact HID Technical Support for the **HID Advanced Device Protocol (HADP)** (P/N 3123-902).

The tamper detect remains active while the reader is attached to the back plate. Depending on wiring installation (for example, using additional set of wires and resistance), the tamper is also active if the reader is powered off.

The following circuit diagram shows the iCLASS Optical Tamper.

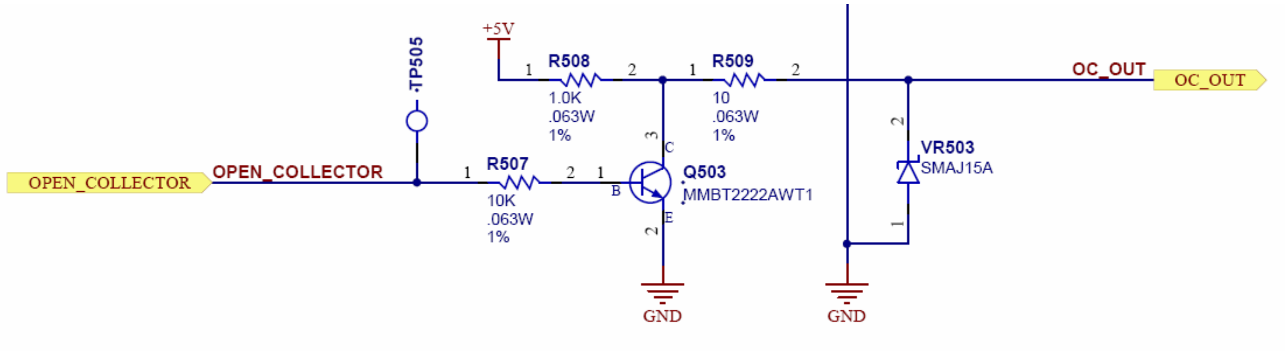


Figure 1 – iCLASS Optical Tamper Circuit

[1] All readers utilizing a physical tamper switch have tamper enabled automatically. By default, readers utilizing an optical switch do not come with tamper enabled. Order tamper enabled part numbers from the factory (see How To Order Guide) or field configure readers with tamper enable configuration cards See Appendix A – iCLASS Tamper for more information on enabling this feature.

[2] I'm Alive is byte sized message consistently sent over Wiegand or Clock-and-Data output lines. This repeating message informs the host the reader is online and functioning. The I'm Alive (normal) message is configurable to any single byte value. The I'm Alive (tamper) always reports the inverse of I'm Alive (normal).

Use the following wiring guides for open collector tamper for both unsupervised and supervised inputs.

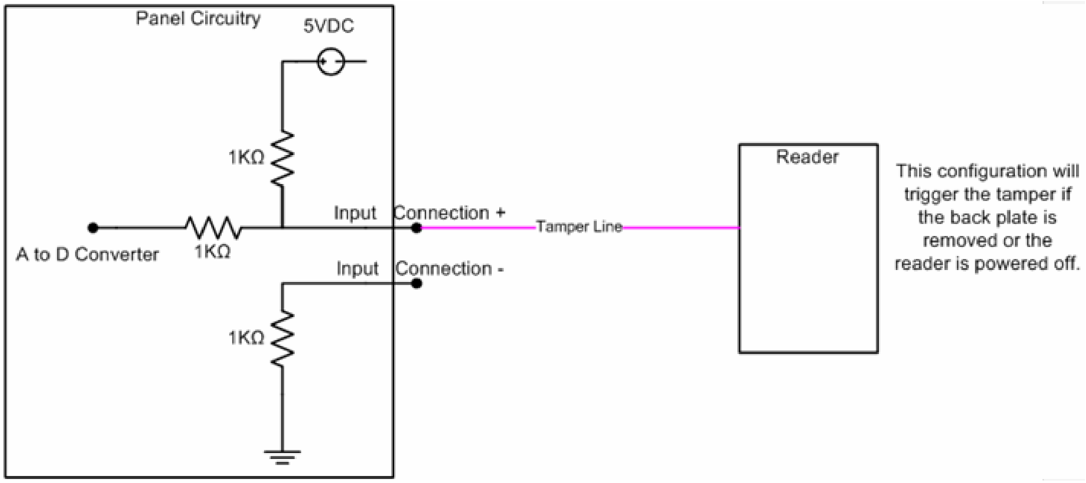

Panel Circuitry
5VDC
1KΩ
Input
Connection +
Tamper Line
A to D Converter
1KΩ
Input
Connection -
1KΩ
Reader
This configuration will trigger the tamper if the back plate is removed or the reader is powered off.

Figure 2 – Unsupervised Open Collector Tamper

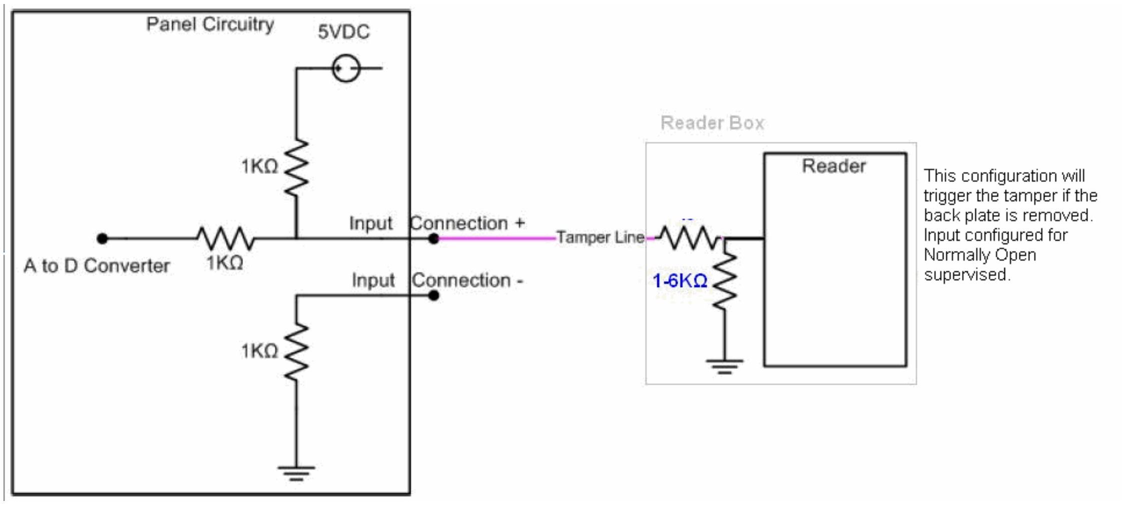

Panel Circuitry
5VDC
1KΩ
Input
Connection +
Tamper Line
A to D Converter
1KΩ
Input
Connection -
1KΩ
Reader Box
Reader
1-6KΩ
This configuration will trigger the tamper if the back plate is removed. Input configured for Normally Open supervised.

Figure 3 – Supervised Open Collector Tamper

For VertX / EDGE set input to Normally Open within the Configuration software. If using the **Supplemental Configuration** page, set the A to D configuration to 255 197 196 0 (Decimal for unsupervised implementation). Consult your system provider when working with other types of panels.

Use the correct electrical polarity for generating a tamper signal when the wires are cut. Furthermore, Installers can include an additional pair of wires connected together through a resistor at the reader. The panel using a technique called Supervision monitors this loop. Supervision detects when wires are cut, shorted, or when other electrical characteristics of the wires change.

4.2 HID Prox

HID Global's MaxiProx, ProxPro and ProxPro keypad products offer a hard implementation of tamper and supervision through a two conductor NC (Normally Closed) / NO (Normally Open) tamper implementation. When separating the reader core from the backplate, the physical tamper switch is activated causing the state of the circuit to change.

Find details of the tamper installation in the following installation guides.

- MaxiProx - www.hidglobal.com > documents > MaxiProx DFM Reader - 5375
- ProxPro - www.hidglobal.com > documents > ProxPro Wiegand / Clock-and-Data

Additionally, all HID Prox readers offer the I'm Alive feature for supervision. By default, HID Prox readers do not ship with tamper enabled. To enable tamper in the field, order HID Prox configuration card part number ANK21 from HID Global technical support.

Note: The inverted I'm Alive for tamper signaling is not available on HID Prox readers.

When working with any other HID Prox products, HID Global recommends replacement with a multiCLASS® reader for perimeter and high security access points. multiCLASS readers provide more tamper functions combined with Genuine HID compatibility for existing HID Prox credentials. The readers are available in mullion, wall switch and wall switch keypad form factors. Find more information at the following websites.

- multiCLASS RP15 Mullion: www.hidglobal.com/prod_detail.php?prod_id=137
- multiCLASS RP40 Wall Switch: www.hidglobal.com/prod_detail.php?prod_id=136
- multiCLASS RPK40 Wall Switch: www.hidglobal.com/prod_detail.php?prod_id=135

5 Appendix A – iCLASS Tamper

Approved is a variety of tamper implementations on iCLASS readers.

The earliest version of iCLASS readers require the installation of an external reed switch (not included) that works with a magnet located inside the reader potting. For questions, contact Technical Support.

The following table lists the reader model and base part numbers.

Model	Base Part Number
R30	6110A
R40	6120A
RK40	6130A
RW100	6101A
RW300	6111A
RW400	6121A
RWK400	6131A

The next version of iCLASS readers includes an integrated tamper switch. The reader model and base part numbers are noted in the following table.

Note: The implementation of tamper changed to an optical sensor midway through reader production (signaled by Change to Optical = Yes).

Model	Base Part Number	Change to Optical
R10	6100B	Yes
R30	6110B	Yes
R40	6120B	Yes
RK40	6130B	Yes
RW100	6101B	Yes
RW300	6111B	Yes
RW400	6121B	Yes
RWK400	6131B	Yes
RP40	6125B	Yes
RP40	6125A	No
R90	6150A	No

The following table details the manufacturing date code information for cut-in of the optical tamper. The physical tamper switch utilized prior to the WWYY Start Manufactured Date Code column values is shown. The optical tamper switch was cut-in during WWYY Start Manufactured Date Code and after.

Products	Part Number	Start Manufactured Date Code	Start Serial Number	Mounting Plate Revision
R10 / RW100	610xBKT	1607	000001	6303-104-01 Rev 3
	610xBGN	2207	000001	6303-104-01 Rev 3
	610xBGT	3307	000001	6303-104-01 Rev 3
	610xBKN	0707	000001	6303-104-01 Rev 3
R30 / RW300	611xBGN	2907	000001	6304-103-01 Rev 3
	611xBKT	1607	000001	6304-103-01 Rev 3
	611xBKN	0707	000001	6304-103-01 Rev 3
R40 / RW400	612xBGT	3007	000001	6305-103-01 Rev 4
	612xBKN	0707	000001	6305-103-01 Rev 4
	612xBGN	2207	000001	6305-103-01 Rev 4
	612xBKT	0807	000001	6305-103-01 Rev 4
RK40 / RWK400	613xBGT	3307	000001	6094-101-01 Rev 9
	613xBKN	3107	000001	6094-101-01 Rev 9
RP40	6125BKX	0707	000001	6305-103-01 Rev 4

All reader models listed below are manufactured using optical tamper.

Model	Base Part Number
R10	6100C
R15	6140A
R15	6140C
R30	6110C
R40	6120C
RK40	6130C
RW100	6101C
RW300	6111C
RW400	6121C
RWK400	6131C
RP15	6145A
RP15	6145C
RP40	6125C
RPK40	6136A
RPK40	6136C

By default, tamper outputs are disabled in iCLASS readers with optical sensors. Order the Tamper option through the iCLASS How To Order Guide to activate. Additionally, a configuration card enables the Tamper feature in field-installed readers.

Note: Activating the optical tamper increases the current draw of the product by roughly 20mA nominal and peak. Order configuration cards through HID Technical Support using the following configuration card part numbers.

Enable/Disable	Tamper Type	Configuration Card Part Number
Tamper Enable	Open Collector	2000-08-00-000009
Tamper Enable	OSDP	2000-15-00-00P000 R15, R30, R40 OSDP Address = 0 Baud = 9600 Data Frame Size = 8 bit Parity = None 2000-15-00-00P000 RK50, RKL55 OSDP Address = 0 Baud = 9600 Data Frame Size = 8 bit Parity = None Keypad = 00
Tamper Enable	I'm Alive Message	2000-13-00-000577 I'm Alive heartbeat = 0xAA Tamper (heartbeat inverted) = 0x55 Pulse Interval = 1 Minute
Tamper Disable	Disable All	2000-08-00-000038

Contacts

North America

15370 Barranca Parkway
Irvine, CA 92618
USA

Phone:	800 237 7769
Fax:	949 732 2120
Support:	support.hidglobal.com

Europe, Middle East and Africa

Phoenix Road
Haverhill, Suffolk CB9 7AE
England

Phone:	+44 1440 714 850
Fax:	+44 1440 714 840
Support:	support.hidglobal.com

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong

Phone:	852 3160 9800
Fax:	852 3160 4809
Support:	support.hidglobal.com