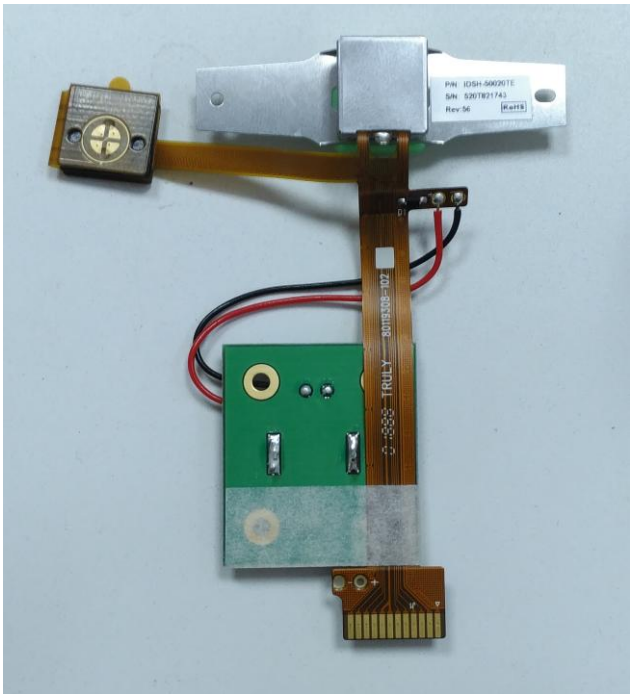
Value through Innovation

Design Guide P/N 80119502-001

SREDHead Card Reader Design Guide



Rev 80119502-001--B
Date: 4/5/2016

International Technologies & Systems Corporation
10721 Walker Street, Cypress, CA 90630-4720; Tel: (714) 761-6368; Fax: (714) 761-8880
www.idtechproducts.com

Revision History

Revision	Date	Description of Changes	By
A	6/08/2015	Released	J.H.
B	4/5/2016	Updated reference file	J.H.

Table of Contents

1.)Scope

The SREDHead is designed to meet the PCI 4.x SRED requirement, however since it is a component it cannot be certified alone by PCI which means the final enclosure which incorporates the SREDHead needs to obtain PCI certification. Following is a set of design guidelines on how the MSR solution needs to be designed in order to obtain the PCI SRED certification.

2.)Design Requirements:

The SREDHead itself has tamper switches built into the head so when the head can is opened, the encryption key will be destroyed immediately.

For PCI compliance, other types of attacks are also considered in scope outside of directly at the MSR head, including an attacker being able to install a "fake" head next to the SREDHead or to replace it. To overcome that requirement, the SREDHead was designed to provide an external tamper switch signal to the head. When this tamper switch signal is triggered, the encryption key in the head will be destroyed.

To facilitate production of the units, the SREDHead FPC is designed such that there are two tamper switch bypass bridges in parallel with the tamper switch. Those bridges will bypass the tamper switch input until the SREDHead is installed in the unit. In the design of the unit, it is necessary to design in a mechanism such as plastic tabs so when the tamper switch is installed and the unit is closed, it will be able to break off those bridges. Once those bridges are broken, the tamper switch will be active. When the surrounding case is opened, the tamper switch will be open and triggers the tamper detection signal that goes to the head and erase the keys.

a. Mechanical Drawing:

The following diagrams showing the location of the tamper switch and the bridges

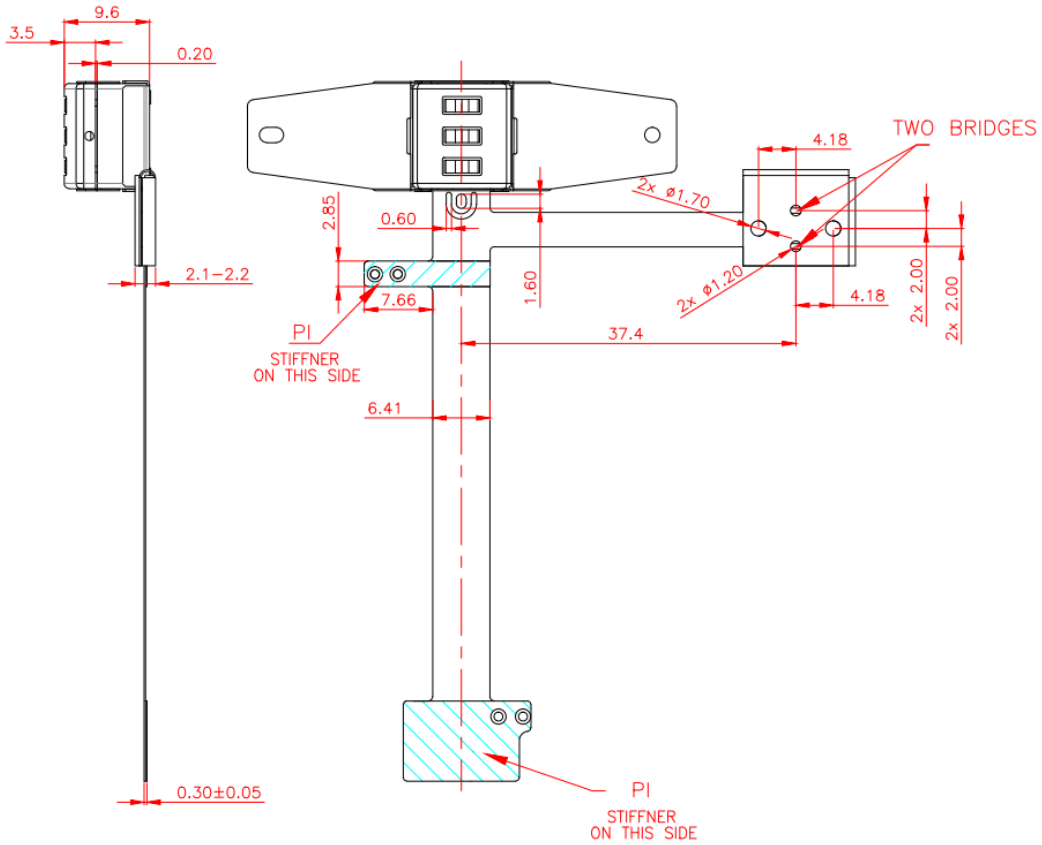
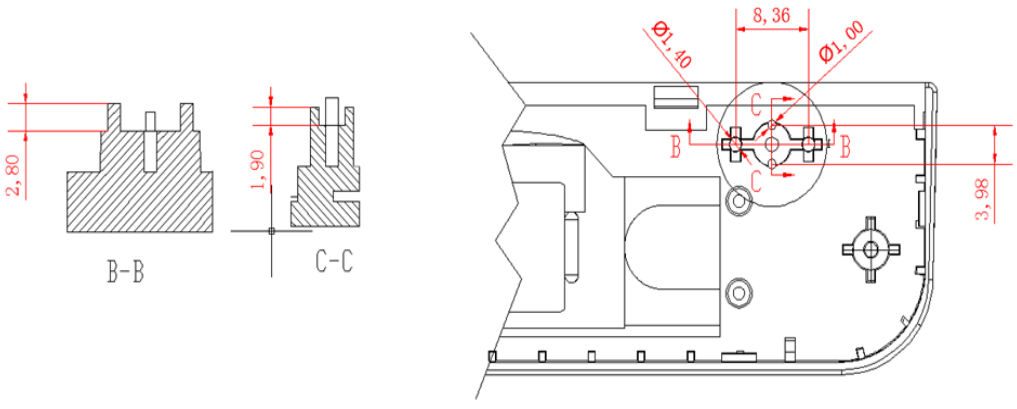


Figure 1 Front side of the SREDHead



Bridge Breaking Mechanism

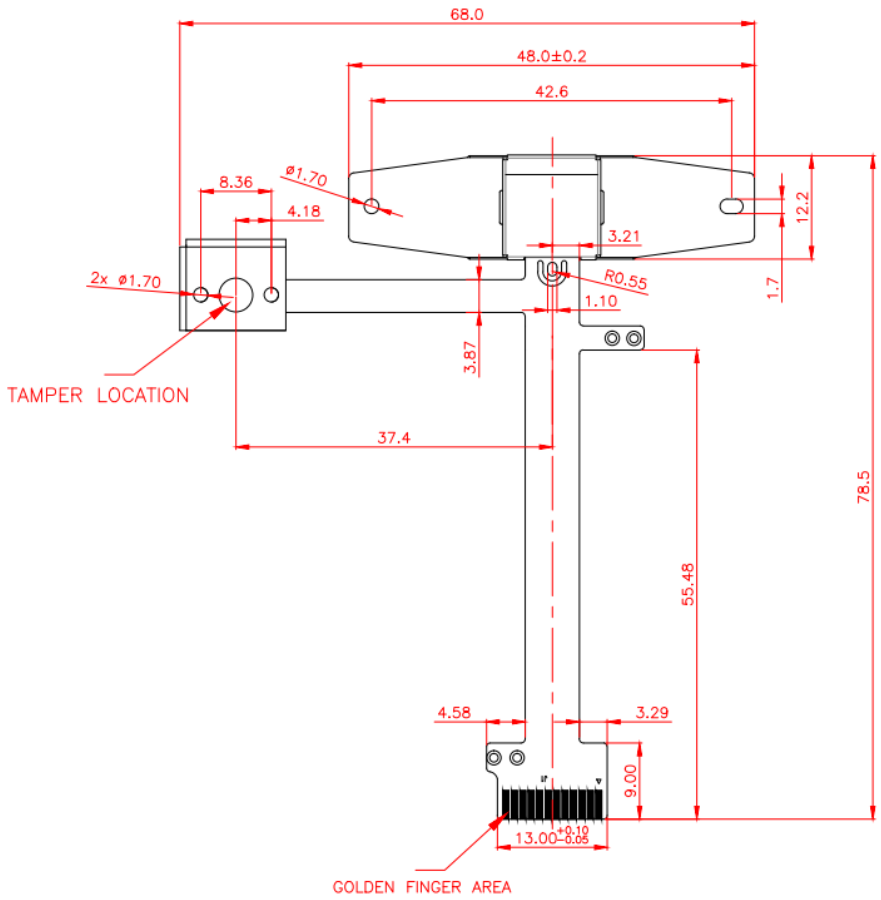
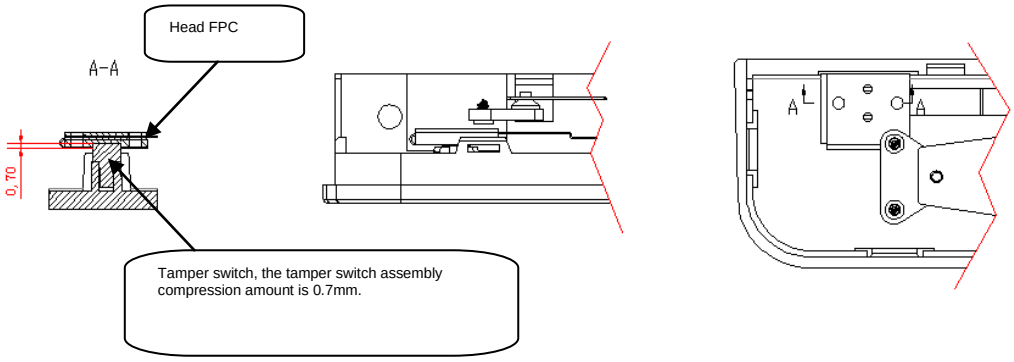
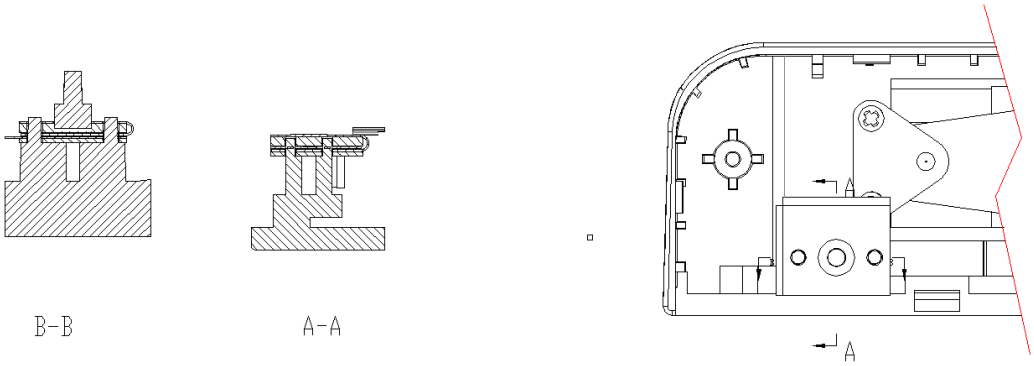


Figure 2 Back side of the SREDHead



Tamper Button

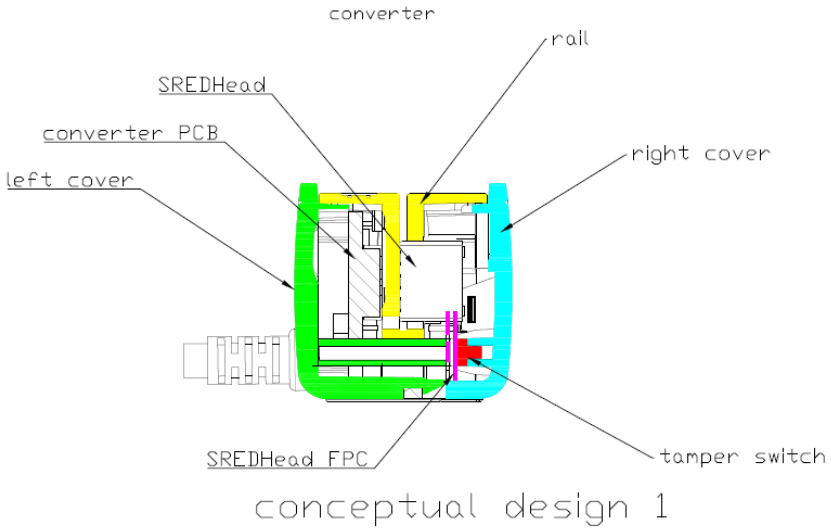


FPC with bridges broken and tamper switch engaged.

b. Reference Design

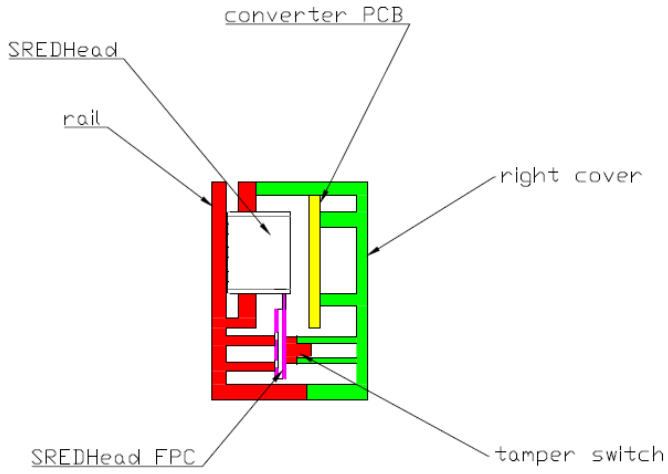
ID Tech reviewed with a PCI lab two versions of the SREDHead integration design that would pass PCI SRED certification. Following are diagrams illustrating the design.

Design 1:



The tamper switch is between the left cover and right cover , connect to the MSR mesh circuit (Reader FPC), the FPC fix on the rail bottom, that prevent the left cover, right cover and head separate from the rail.

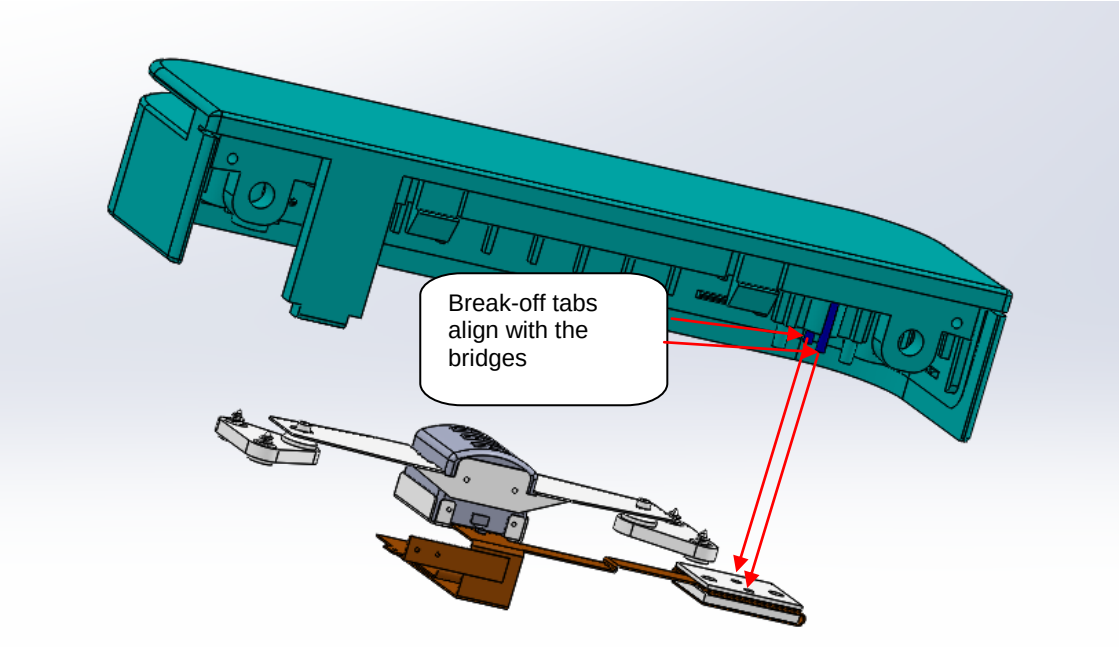
Design 2:



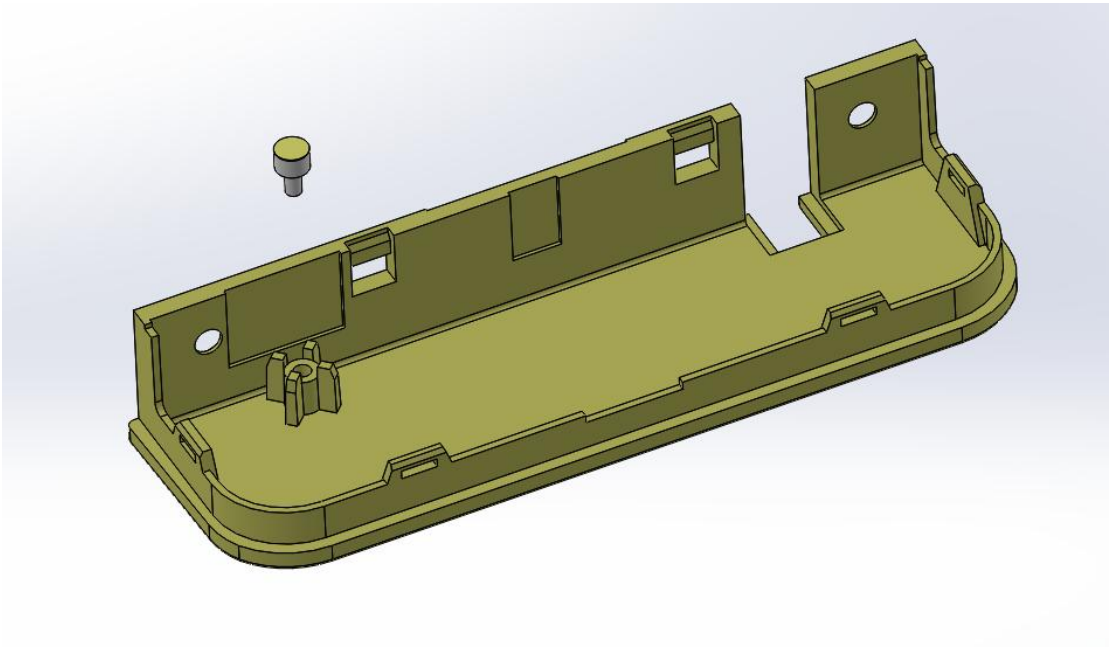
conceptual design 2

The tamper switch is between the left cover and rail , connect to the MSR mesh circuit (Reader FPC), the FPC fix on the rail bottom, that prevent the right cover and head separate from the rail.

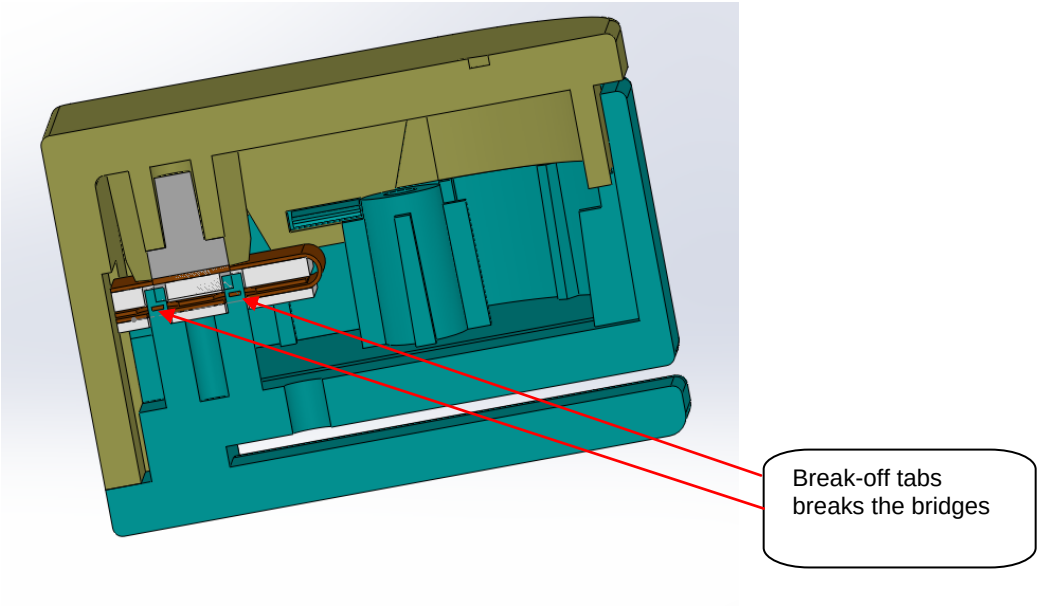
Below are 3D views of Design 1.



When the SREDHead is installed in the housing, the break-off tabs are aligned with the bridges.



Within the ID Tech reference design, the tamper button is compressed .7mm when installed. This will provide enough force to break the bridges as well as maintain constant contact between the tamper button and the tamper switch.



When the unit is closed, the break-off tabs break the tamper switch bridges. The tamper switches closed the tamper detecting circuit.

c. Battery Consideration

The SREDHead comes with a small battery. The battery is used to retain the encryption keys. The design can either continue using the supplied battery or the design can supply its own power to the SREDHead and remove the battery that comes with it. The SREDHead must have power supplied at all times for the active tamper monitoring.

3.) Reference Files:

ID Tech has a reference file available for design consideration. Please coordinate with your sales rep to execute ID Tech's Mutual NDA for file sharing.

SREDHead 3D drawing with internal design disable.zip

4.) Key Injection:

Being a SRED device, the SREDHead must have a data key injected into the unit in order for the unit to function properly; this needs to be done either at ID Tech or a certified key injection facility. The SREDHead allows for two methods of key injection: direct injection or remote key injection.

When designing the SREDHead into the enclosure or tablet for direct key injection, ensure that the enclosure or tablet allows pass through communication capability to the SREDHead or that the host is able to deliver the key injection commands to the head directly. The preferred key injection method is over a RS232 signal, but if USB is preferred, it needs to comply with ID Tech USB.