STEREO
IMPACT

IT Security Plan

ITSecurityPlan_B.doc
Version A – 2001-Dec-07

David Curtis, UCB IMPACT Project Manager

Janet Luhmann, IMPACT Principal Investigator

Document Revision Record

Rev.	Date	Description of Change	Approved By
A	2001-Nov-30	Preliminary Draft	-
B	2001-Dec-7	Minor rewording	

Distribution List

Dave Curtis, UCB
Mike Hashii, UCB
Peter Schroeder, UCB
Harry Culver, GSFC

Table of Contents

1. Overview

1.1. *Introduction*

IMPACT consists of a number of instruments connected to the STEREO spacecraft via the IMPACT IDPU. During operations, the IMPACT team communicates with the IMPACT instrument via the Mission Operations Center (MOC) at APL connected via the internet to the Payload Operations Center (POC) at U.C.Berkeley. This document describes the IT security system used to protect access to the IMPACT POC facilities.

1.2. *Document Conventions*

In this document, TBD (To Be Determined) means that no data currently exists. A value followed by TBR (To Be Resolved) means that this value is preliminary. In either case, the value is typically followed by a code such as UCB indicating who is responsible for providing the data, and a unique reference number.

1.3. *Reference Documents*

The following documents provide reference material (however, anything in these documents that is not in compliance with University policy is inapplicable to this Plan). Some of these and other IMPACT documents can be found on the Berkeley STEREO/IMPACT FTP site:

http://sprg.ssl.berkeley.edu/impact/dwc/

1. Operations/MOC-POC_ICD_update_209_10_01 MOC-POC ICD
2. SANS documents available at:
   www.sans.org
3. Center for Internet Security documents available at:
   www.cisecurity.org
4. NASA Incident Resource Center:
   http://www-nasirc.nasa.gov/access_policy.html

2. POC Description

The IMPACT POC consists of a Command & Telemetry GSE and Science Display GSEs.

2.1. *Command & Telemetry GSE*

This GSE is used at the IMPACT Suite level, and interfaces to either the APL-supplied Spacecraft Emulator (prior to IMPACT integration with the spacecraft), or the MOC (after integration with the spacecraft). It performs the command scripting and housekeeping display / limit checking functions. It will be used starting at IDPU bench testing, through Suite and Spacecraft I&T, and will form the heart of the POC during post-launch Operations. It is the only system that can command the IMPACT instrument.

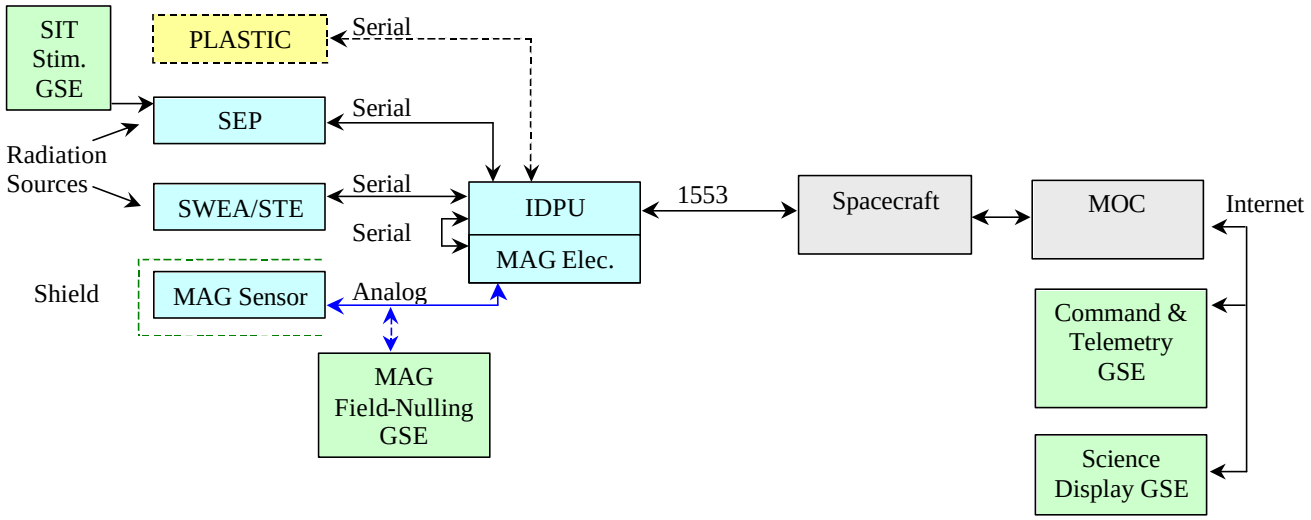

Figure 2.1-1 Spacecraft I&T GSE Setup

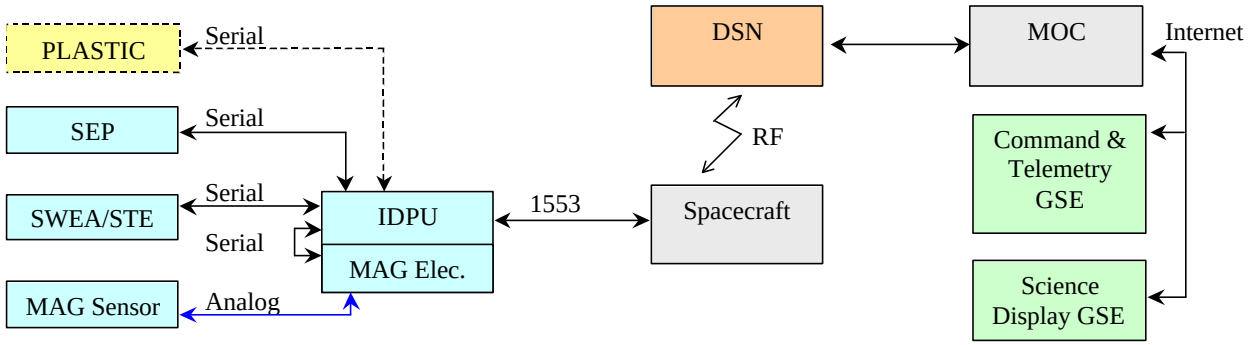

Figure 2.1-2 On-Orbit POC Setup

The C&T GSE is unable to send commands that will cause permanent damage the IMPACT instrument. The spacecraft controls IMPACT boom deployment. Hardware

interlocks prevent the IMPACT High Voltage from being turned on while the spacecraft is on the ground, which could otherwise cause damage to the instrument (this is not a problem once we are on-orbit).

2.2. *Science Display GSE*

Science Display GSE are used to display science telemetry, either via real-time connection, or via post-pass ftp of data files from the MOC. This GSE is not able to send commands or modify the data stored on the MOC.

3. IMPACT POC IT Security

The MOC is designed such that it will only accept IMPACT commands from the IMPACT C&T GSE. Commands from the IMPACT C&T GSE to other STEREO subsystems as well as commands from other machines to the IMPACT instruments are blocked by the MOC. The security of the MOC to POC interface is described elsewhere; this document only discusses how the POC is protected against unauthorized access.

The POC IT security plan is centered on the C&T GSE, since only it can send commands.

3.1. *Training*

The system administrator responsible for the C&T GSE shall be trained at the SANS/GSFC security training or similar prior to configuring the C&T GSE. System administrator selection and training shall be in accordance with University Policy, which prohibits discrimination in employment on the basis of citizenship.

3.2. *Configuration*

The C&T GSE shall be configured in compliance with best security practices benchmarks such as those published by the Center for Internet Security (reference 3), except those, if any, that are not in compliance with University policy.

Only software directly needed to support commanding and interfacing to the MOC shall be loaded on the computer. (e.g. No web servers, no chat software, no FTP daemons, etc.)

All interfaces to the computer should be via secure channels. i.e. SSH, or VPN or equivalent. TELNET access will not be allowed.

3.3. *Maintenance*

The C&T GSE shall have applicable operating system and application security patches and updates installed within seven days of their availability on the vendor's web site.

Automated records containing compliance scores and patch history information shall be maintained.