CSC-EPL-89/002

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF INFOTRON

INX4400/USM

6 JUNE 1989

FINAL EVALUATION REPORT

INFOTRON

INX4400/USM

NATIONAL
COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

6 June 1989

CSC-EPL-89/002
Library No. S232,551

This page intentionally left blank.

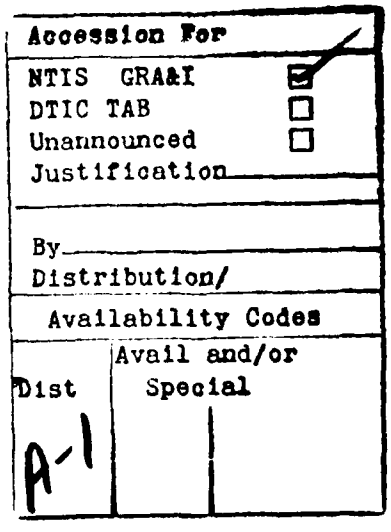
FOREWORD

This publication, the Final Evaluation Report Infotron, INX4400/USM, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center". The purpose of this report is to document the results of the evaluation of Infotron's INX4400/USM. The requirements stated in this report are taken from the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION* of the *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA* dated September 1988.

Approved:

Eliot Sohmer — 6 June 1989

Eliot Sohmer
Chief, Product Evaluations
and Technical Guidelines
National Computer Security Center



ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals:

Karen M. Bielat

Caralyn C. Crescenzi

David N. Robidoux

John W. Taylor

National Computer Security Center

Fort George G. Meade, Maryland 20755-6000

Table of Contents

EXECUTIVE SUMMARY

The Infotron Intelligent Network Exchange with the User Security Module option (INX4400/USM) is a high capacity digital data switching system (front-end connection switch) that handles asynchronous and synchronous data transmissions. It uses distributed logic and master-slave hierarchy to transfer data and control signals between devices that interface with the INX4400/USM. The INX4400/USM interfaces conform to EIA RS232C (CCITT V.24/V.28), and CCITT V.11 and V.35 standards. The INX4400/USM can include up to 4000 I/O interfaces and can consist of 64 nodes. Because the USM solely interacts with asyncronous devices, this evaluation only addresses asynchronous data transmissions.

The INX4400/USM system software is a menu driven program executing from a dual micro floppy drive. The program controls channel configuration, provides security features for access to the system console, provides access to the various menus, monitors selected events, and enables the USM. The USM is a security option of the INX4400. It allows an administrator to assign ID's, passwords, and Destinations Access Group (DAG) codes to users. This option, in conjunction with the system software, provides the Identification and Authentication (I&A).

The security protection provided by the INX4400/USM described in the INX4400 Operation Manual (part number 950067, dated February 1988) has been evaluated by the National Computer Security Center (NCSC). The security features of the INX4400/USM were evaluated against the requirements specified by the Computer Security Subsystem Interpretation of the DoD Trusted Computer System Evaluation Criteria (CSSI) dated 16 September 1988.

An I&A subsystem requires users to identify themselves to it before they perform any actions. A subsystem rated as an I&A/D2 system must provide a unique identity for each individual user and the authentication needed to provide accountability for controlled access to the protected system, export user identification to the protected system (host), and an auditing mechanism to log security relevant I&A events. The INX4400/USM does provide individual user I&A and an event log, but the INX4400/USM does not export any user identification to the host(s).

The INX4400/USM meets several I&A/D1 requirements, but a product must meet all the requirements of a given class to be given that class rating. Consequently, the INX4400/USM receives an I&A/D rating.

This page intentionally left blank.

INTRODUCTION

In September 1988, the National Computer Security Center (NCSC) began a product evaluation of the Infotron INX4400 with the User Security Module (USM). The objective of this evaluation was to rate the INX4400/USM against the Computer Security Subsystem Interpretation (CSSI), and to place it on the Evaluated Products List (EPL) with a final rating. This report documents the results of the evaluation of the INX4400/USM available from Infotron Systems Corporation.

Material for this report was gathered by the NCSC evaluation team through documentation, interaction with system developers, and hands-on experience using the INX4400/USM system.

Evaluation Process Background

The National Computer Security Center (NCSC) was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of Trust Technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program, the Center works with the manufacturers of hardware and software products to implement and make available to the public good computer security solutions. Under this program, the NCSC evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independant of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users and authoritative evaluation of a product's suitability for use in processing important information.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. Security Managers should note that subsystems are not capable of protecting information with such assurance that classified information may be maintained on a system protected only by subsystems. Neither may subsystems be used to

upgrade the protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

Subsystems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations, a subsystem's security-relevant performance is assessed against requirements in the Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report assigns a specific rating to the product and a summary of the evaluation report is placed on the Evaluated Products List.

Document Organization

This report consists of four major sections and three appendices. Section 1 is an introduction. Section 2 provides an overview of the system hardware and software architecture. Section 3 provides a mapping between the requirements specified in the CSSI and the INX4400/USM features that fulfill or do not fulfill those requirements. Section 4 presents the evaluation team's impressions of the system. The first two appendices identify specific hardware and software components to which the evaluation applies. The last appendix is a glossary of terms and acronyms contained in this report.

SYSTEM OVERVIEW

The following sections provide an overview of the INX4400/USM history, the subjects and objects in the system, and the hardware and software architecture that comprise the INX4400/USM.

INX4400/USM Background and History

The INX series of switching products evolved from the IS4000 Intelligence Switching System. The INX series and the ISN series share certain features inherent in the architecture of these product lines.

Many significant enhancements were added to the old IS4000 system with the release of the INX series of products. Optional software features in the IS4000 are Standard with the INX software. In addition, system functionality, versatility, and reliability were increased with both hardware and software changes and additions.

The IS4000 was introduced in January 1984 and had generated a number of hardware and software upgrades when the INX4400 evolved in 1985.

In 1988, the NX4600 series of products were introduced. Again, Infotron used the enhanced INX4400 hardware and software to produce the NX series.

An upward migration path has been in place thru the series changes that allows customers to upgrade from series to series without discarding their installed equipment.

SRP Protected Resources

The following section discusses the subjects and objects identified in the INX4400/USM subsystem.

Subjects

The subjects in this system are the users, the system administrators, and the security officers. A user only becomes a subject after both the USM security checks return with a positive result and a connection from the user to a channel has been made by the MCM. The two levels of system administrators are the master operator and regular operators. The master operator has the highest privileges, and he is responsible for assigning operator numbers and passwords, determining the access privileges given to the the other operators, and defining the amount of time an operator may stay logged in to the console without issuing a command. The subordinate operators may only use the menu functions for which they have access. The two types of security officers are master operator and subordinate operators. The master operator (number one) is able to change the password for any operator. However, the subordinate operators (numbers two through 16) can only change their own passwords.

Objects

The objects in the system are the channels, the connections between the user and his destination, and the system tables.

If a user is correctly identified and authenticated, the system assigns an appropriate channel to the user. Upon disconnection, the system deallocates the channel associated with the user.

The system tables are actually system objects. As a result of a menu-driven query, the system references the tables for security and system related data. Only security related data may be accessed by the security officers at the security console. All other types of data may be queried by the operators on the main console. The users of the system may not query any of this information directly.

INX4400/USM Hardware Architecture

The following section describes the INX4400/USM Master Control Unit, the Expansion Module, and the interactions between them.

Master Control Unit Hardware

The Master Control Unit hardware, the system administrators' interface to the INX4400/USM system, maintains the access control databases and provides the appropriate information to the Slave Controller Modules (SCM).

Master Controller Module with Expanded Memory

The Master Controller Module with Expanded Memory (MCME) provides the main control of the INX4400 system. It consists of a 6502 microprocessor, 36K of dynamic Random Access Memory (RAM), 54K of Read Only Memory (ROM), a Universal Asynchronous Receiver/Transmitter (UART) for communications between the MCME and MSME, address decoding circuitry, and a watch dog timer. The watch dog timer provides notification of system component failure and must be written to or read from every 250 milliseconds. Otherwise, the system resets.

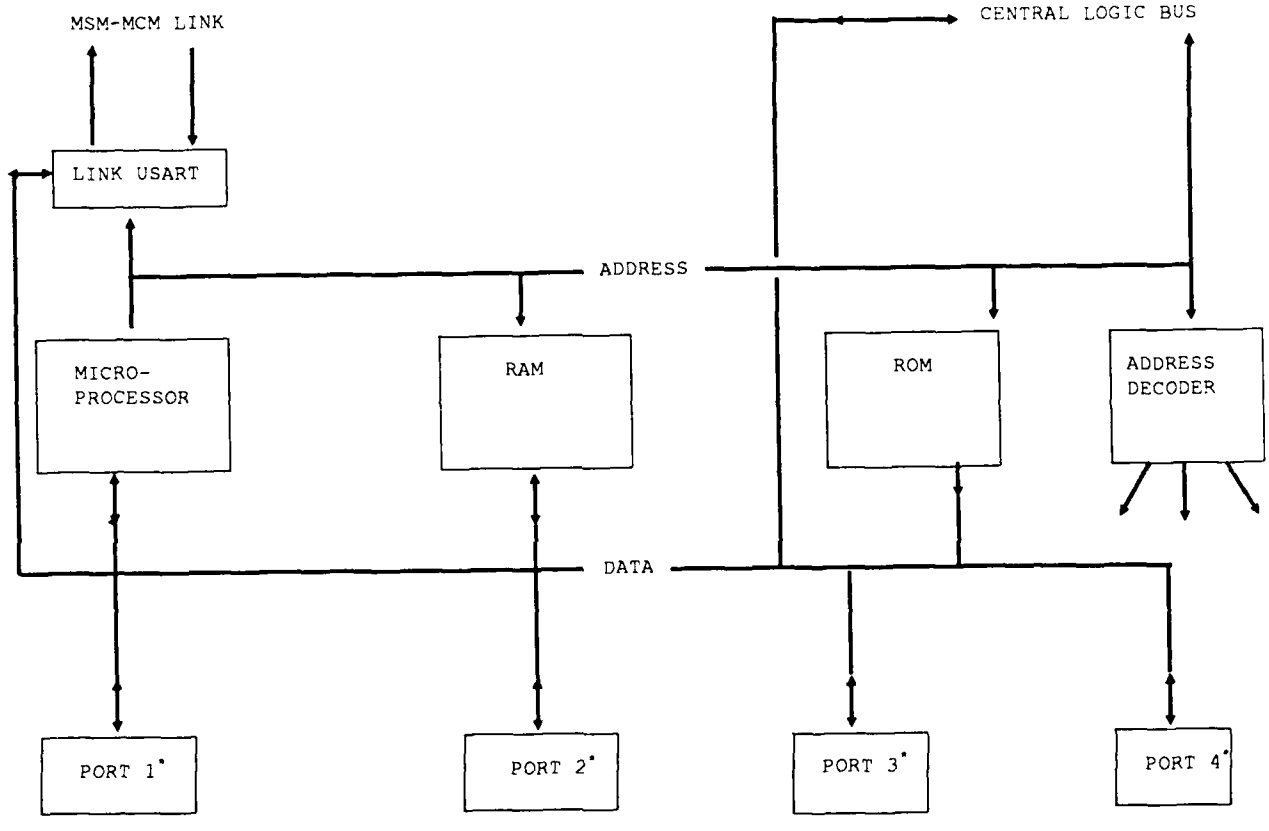
The MCME microprocessor stores information regarding transient channels in various queues (connect/disconnect requests, status, etc.), information reguarding time slot allocation, and various working tables in dynamic RAM.

Master Support Module with Expanded Memory

The Master Support Module with Expanded Memory (MSME) provides support for the system console terminals and printer. It consists of a 6502 microprocessor, 36K of dynamic RAM, 54K of ROM, a UART for communications between the MCME and MSME, address decoding circuitry, and a watch dog timer. In addition, four UARTs and a Parallel Interface Adapter (PIA) comprise ports A, B, C, and D which are used for the system console terminals and printers.

The MSME communicates with the Disk Controller Module (DCM) by way of a PIA located on the DCM module.

The following figure represents the MCME and MSME logic.



* MSME

LEGEND: RAM = Random Access Memory

ROM = Read only Memory

USART = Universal Synchronous/Asynchronous Receiver/Transmitter

Memory Expansion Module

The Memory Expansion Module (MEM) is part of the memory section of the MCME. The MEM contains two sections: the logical address section and the parameter storage section. The logical address section, a two-dimentional array, stores an eight-byte address, a one-byte "called" Restricted Access Group (RAG),[1] one byte of speed information, and one-byte of state information for each INX4400/USM channel (4096 maximum).

In addition, compare registers temporarily hold similar information for one calling channel except that a calling RAG is held rather than a called RAG. The compare logic "exclusive or"s (XOR) inputs from the compare registers and RAM data gates. When a comparison results in a match, the address of the found destination is made available to the MCME.

The parameter storage section is an array comprised of 4096 x 32 bytes of dynamic RAM which stores an auto-connect address, channel type, queueing information, a calling RAG, and feature flags for each channel. Address decoding allows the MCME microprocessor to access the MEM.

Switch Bus Interface Module with Remote Master Capability

The Switch Bus Interface Module with Remote Master Capability (SBIRM) is the interface between the Master Control Unit hardware and the Expansion Unit hardware. The SBIRM passes control and data signals to the Slave Control Modules, which in turn supervise the slaves.

The SBIRM consists of two sections: supervisory and data. The supervisory section consists of two online supervisory UARTs and two offline supervisory UARTs. The UARTs are part of the I/O section of the MCME microprocessor. The MCME accesses the UARTs via address decoding logic.

The data section of the SBIRM is comprised of 2048 RAM locations. Each location corresponds to a time slot and contains the 16-byte bit configuration (data and control lines) which will travel on the switch bus when read out of memory by the SBIRM Master Scan Address Counter (MSAC). The Slave Address Counter (SAC) of the last SCMU in the switch bus loop generates an address to be written into RAM. Setting the SCAN SIZE DIP switch on the SBIRM determines the upper limit of the counters.

---

1 The destination of a connection request is defined as "called", the originator of the request is defined as "calling".

Disk Controller Module

The Disk Controller Module (DCM) consists of two 3.5-inch microfloppy disk drives and associated control logic, 16K of RAM (8K reserved for future use) and 8K of ROM. A portion of the MSME resides on the DCM. The MSME portion consists of the PIA that interfaces the MSME to DCM address decoding logic for that PIA.

Expansion Module Hardware

Slave Controller Module with Expanded Memory

The Slave Controller Module with Expanded Memory (SCME) includes a 6502 microprocessor, programmable read only memory (PROM), and RAM. Both the microprocessor and the hardware scan counter address a portion of the RAM.

The SCME microprocessor sets up input/output address memory (IOAM) and time slot function memory (TSFM), sends parameters to channel adapter modules and service modules during setup, and monitors channel status. The actual transfer of information is the result of the scan address counter addressing (repetitively) IOAM and TSFM, hardware circuitry decoding, and acting upon the stored functions.

The time slot function switch is an arrangement of latches and buffers that allow communication paths to be created as defined by time slot function codes that are stored in the TSFM. These paths can be used for internal and external connections and for the SCME microprocessor to monitor and configure channels.

Quad Asynchronous Service Module Universal

The Quad Asynchronous Service Module Universal (4ASMU) includes a microprocessor, RAM, and ROM. The 4ASMU also includes address select circuitry, selection logic, and addressing logic for each of the four independent channels. The supervisory universal synchronous/asynchronous receiver/transmitter (USART) communicates with the SCME/SCMU. Communication with the SCME/SCMU and I/O channels occurs over the top plane connector in the expansion unit.

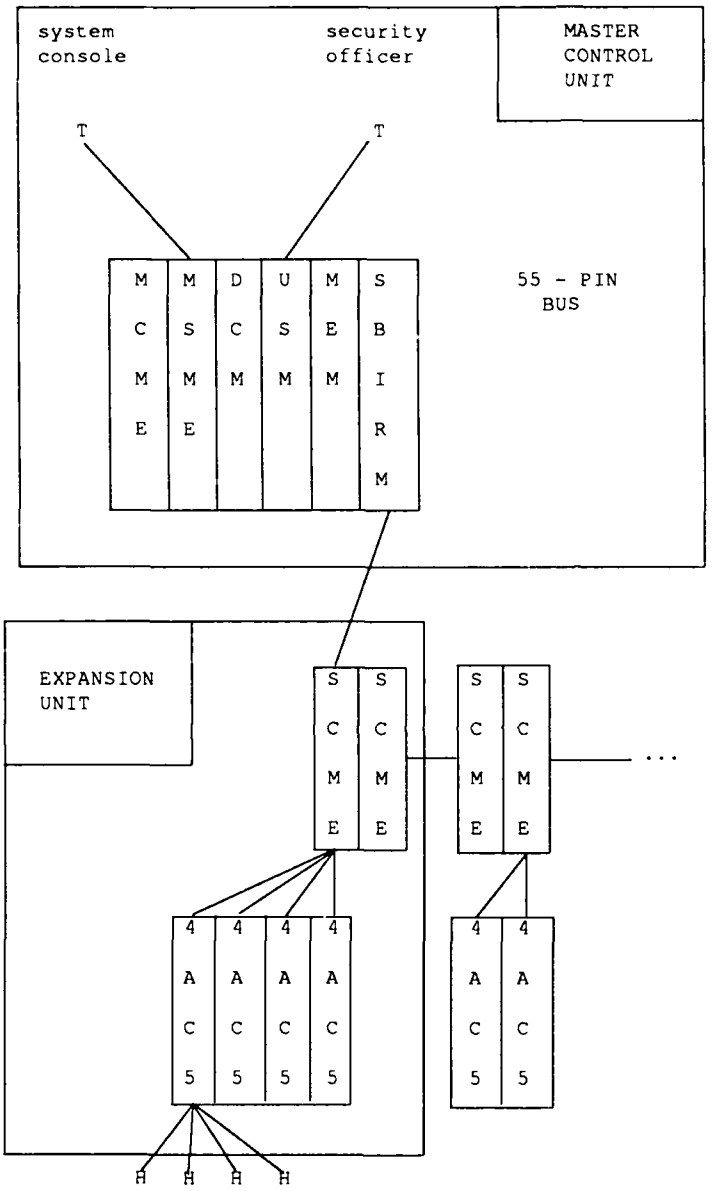
Quad Asynchronous Character-Oriented Channel Adapter

The Quad Asynchronous Character-Oriented Channel Adapter (4AC5) clocks data into a UART that is timed by an on-board oscillator and an associated baud rate generator. The UART strips start and stop bits before the contents of the UART (a character) is placed on the switch bus. A multiplexer controls writing to the switch bus by responding to addresses (via an address decoder) received from slave logic. Another multiplexer associated with each channel on the 4AC5 multiplexes I/O data and special function data (configuration parameters and status) to and from the switch bus by means

of the first multiplexer. I/O data received from the switch bus is read through a reverse process. Start and stop bits are reinstated.

Module Interfaces

To understand how each hardware module interfaces with the others, it is easiest to trace a character from the input port to the output port via hardware. Assume the following scenario: a user(A) on a terminal is hard-wired to a port of a 4AC5. The user has established a connection to host(B) which is connected to a separate 4AC5 in a separate expansion module. In other words, all necessary tables have been loaded with the appropriate addressing information. User(A) types a character on his terminal which the 4AC5 UART converts from serial input to parallel, stripping start and stop bits, and places the character on the data bus. The 4AC5 multiplexers decode the address and determine the character's destination on a separate 4AC5. The 4AC5 then places the character and routing information on the switch bus where the SCME receives the information. The SCME determines the character's destination on another SCME and routes that character to the appropriate SCME. The second SCME determines the appropriate 4AC5 to receive the character and sends the character to the new 4AC5 multiplexer. The multiplexer determines the appropriate port for the character and sends the charater to the correct UART. The UART converts the parallel data into serial, replacing the start and stop bits, and sends the data to host(B).



Key

T = Terminal

H = Host/Modem/Terminal

INX4400/USM Software Architecture

The following section discusses both the System and USM menu selection software.

System Software

The menu-driven system software appears on the system console, on a secondary console, or on an alternate console; all of which can be selected and configured according to the console operator's needs. By selecting the proper menu, the console (master) operator configures global parameters, port parameters, channel parameters, and patch panel functions. Patch panel functions (commands) allow the operator to enable and disable channels, monitor data and control signals, establish and destroy channel connections, and substitute resources.

The ID and password of the master operator are required to gain access to the main (master) menu. The master operator, who has the highest privilege, assigns IDs and passwords to subordinate system console users (up to 15), and controls their access to all the menu options on the main menu.

System Console Menu Selections

There are 14 main menu options, each a submenu of commands (for details, see the INX4400 Operator Manual, part number 950067). Each will be discussed in detail throughout the following sections.

System Commands

System commands allow the operator to view slave status, load slave parameters, exchange the configuration of one group of channels with another on both system and disk (full resource sparing), view software revision levels of master logic modules, set and display time and date, view events, reset or initialize the system,[1] clear the system, and activate the alternate console.

The audited operational events consist of boot up messages - all connected terminals and loaded channels upon initialization; valid user logons with user ID's, and user logon failures; all user actions including the calling channel address and the destination address. Audited critical events consist of excess login failures, a power failure anywhere in the system, errors in the supervisory links, a cleared slave (initialization due to a watch dog timer reset), and a module initialization switch depressed or power loss and restoration of that module. The critical events buffer stores a maximum of 20 critical events. The events log is not accessible by users, only by the system console operator(s).

---

1 Audited events are lost when the system is reset or initialized.

Channel Commands

The channel commands permit the operator to check channel status, make or break connections, transfer connections, monitor data and control signals, enable and disable test tone generation and detection on voice channels, placing channels in loopback, and priming or resetting an alarm on a channel. Both physical and logical addresses identify channels.

One of the channel commands, forced connect, allows the system operator to force two channel connections. This action overrides the USM's DAG table configuration by the security officer, (see USM - DAG Table section). For example, if the security officer has denied a particular user access to a resource, and if the "forced connect" involves the channels of the user and the resource, there will be a security violation unknown to the security officer. No critical event message is created.

Disk Commands

The system administrator uses the disk commands to create a default disk, format a disk, duplicate a disk, write a disk header, read a disk status, reset the disk drive controller, toggle from one system disk to the other, and verify disks.

System Parameters

The system parameters allow the operator to set all global parameters for the system such as terminal prompts, interactive timeout interval, local node number and name, etc. Ports A (main system console), B, C, and D of the MSME and the main system console security parameters are also established in this menu. Port parameters consist of 8 port types (main, alternate, CPU, English events, secondary, compressed events, printer, and inactive), baud speed, echo, flow control, data bit length, parity, number of stop bits, hardcopy only, network debugging, and event filter strings. The console security parameter menu allows the master operator to activate the password prompt on ports A, B, C, and/or D. This is also the menu where the master operator creates the ID and password for him/herself, (which is the password to initially access the system console), and where the master operator defines the subordinate system console operator(s) IDs, passwords, and assigns menu access privileges to these operators.

System Tables

The system tables, also called address maps, allow routing a call to a substitute destination. A destination is represented by a logical address and can be a single channel or group of channels. Address mapping configuration consists of making entries in the system table. A maximum of 64 address maps can be entered into the system table. A logical address could appear as: CPUA01. A physical address would appear as: 0301.

Channel Parameters

This menu enables the operator to access submenus that configure individual channel parameters, channel parameters by group, channel parameters by slave, channel parameters by link, group parameters, and link parameters. The INX4400 can be configured so that a larger number of calling channels contend for access to a smaller number of called channels. Contention promotes efficient use of data processing and data communications resources. Users that require a particular resource will be placed in a queue until the resource has been freed. A maximum of 128 users may be in a queue at any one time per called channel.

For individual channels, the operator defines, per physical address of a channel: the logical address, the restricted access group (RAG) assignment for the given "calling" channel(s) , the RAG for the "called" channel(s), what group the channel is in, and an address modifier if applicable.

Group Parameters

The System Administrator uses the Group Parameters screen to configure link source and destination channels. Group parameters provide the facility to allocate data processing and data communication resources based upon actual use and upon the type of tasks performed by the user or the types of tasks performed at a given terminal or group of terminals. A given terminal (it's address) can be configured two different ways: Auto-Connection and Keyboard Select Routing (KSR). The system software does not provide a destination prompt for an auto-connected terminal, rather the terminal is fixed to the channels and resources it may connect to. A KSR terminal provides a destination prompt and allows the user to select the channel or resource to which it may connect.

The Channel Parameters by Slave menu allows the operator to view the individual channel parameters of each channel by slave. The System Administrator can edit channel parameters and store them individually or in ranges.

The System Administrator uses the Link Parameters table to define the characteristics of up to 99 high-speed links. The parameters are displayed in 7 consecutive screens. This table must be completed before any trunk or link channels can be configured.

Monitor Events

This option lets the operator view the output messages at an MSME port defined as type "English Events". A two-character code, event description, date and a time tag comprise each event message.

Statistics Summary

Using this menu, the operator may view system statistics and link statistics. System Statistics provide information concerning the number of channel connections and connection attempts that have been initiated by the system, by operator command, or by commands received at an MSME port that is defined as type CPU. These statistics also show the number of instances when a source channel could not gain access to an interswitch link and the number of links at a node that have reported

errors. The statistics are compiled over the last 10-minute, 1-hour, and 24-hour periods. In addition, system statistics present the number of active connections at the time the report is requested, the average number of connections during the 24-hour period, and the peak number of simultaneous connections that have occurred over the 24-hour period. Statistics relating to connection attempts are presented in six categories: Busy, Restricted, Unavailable, Queued, No ASM, and Link reported errors.

The Link Statistics provide a 10-minute error summary for each T1/M2CM, VS1/VS2LM, and VS1/VS2LME as configured in the Link Parameters menu in the Channel Parameters commands. The information provided for each link is as follows: Link number, number of seconds and the number of times within a 10-minute period that an out-of-frame error, a very-severe-error-burst, and an excessive-bipolar-violation event occurred.

System Diagnostics

Only MSME port A can perform diagnostics. The diagnostics assist in isolating a malfunction to an SBIRM, an SCME or LCM, or a damaged switch bus cable. There are 3 diagnostic commands: online up-link test, online down-link test, and up/down-link test. Results of these tests include: TEST PASSED or TEST FAILED, the physical address of the SCME or LCM, whether it is an Up-link or a Down-link, and an Online designator.

Log-Off Console Command

When the password feature is enabled for port A, the operator must logoff (LO) to exit the main menu. The system console will show a prompt, requesting the master operator ID and password.

Print Commands

The Print Commands menu allows the operator to print channel parameters according to slave, to print group parameters, and to print the system table (address mappings). An MSME port, defined as type PRINTER, receives the ouput from disks. The printer must be able to print in a 132-column format.

Use Online Console

The System Administrator enters a Control-A to use the online console.

Use Offline Console

The System Administrator enters a Control-B to use the offline console.

Request Help

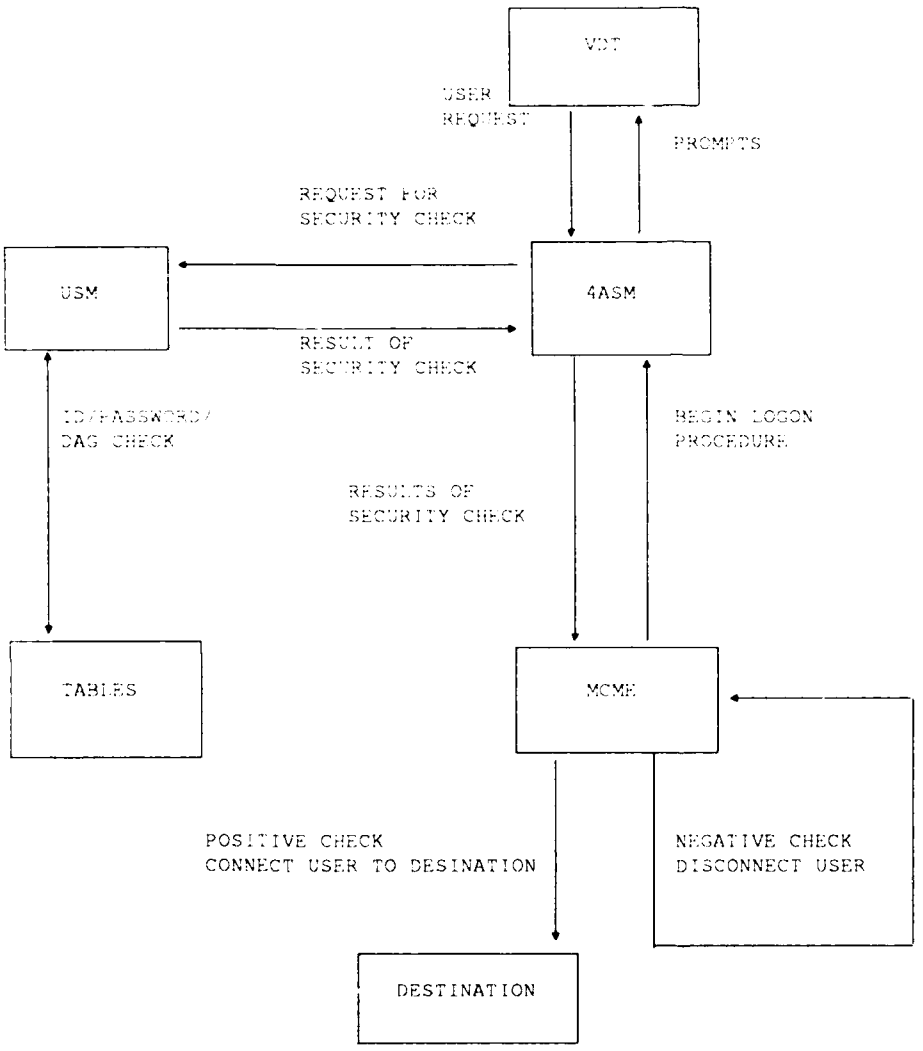
To receive help concerning a menu that is displayed on the console, the system administrator enters a question mark followed by a carriage return, or to receive help concerning a specific command in a menu, enters the letter associated with the command, a (?) question mark, and a <CR> .

User Security Module

The User Security Module (USM) performs the identification and authentication checks for each user attempting to logon by referencing its database. The USM can be activated for calling or called channels with different degrees of security: user ID only; user ID and password; user ID, password, and DAG (Destination Access Group); and user ID and DAG. The USM tables maintain the user ID, password and DAG codes for each user. A user id must be alphanumeric and unique among the system. The password also must be alphanumeric and no greater than eight characters. The DAG codes represent all the destinations a user is allowed to access. A DAG consists of one or more DAG codes; a DAG code is a numeric representation of a destination. There is a maximum of 128 destinations for one DAG, and up to 128 DAG codes can be defined. The Channel Parameters Menu on the main console maintains the DAG code for each channel.

When I&A is initiated, the user connects to the 4ASMU. The 4ASMU sends the information that the user enters at the login prompts to the USM. Then USM compares this information against the appropriate security table entries. The particular instance of when the USM is referenced depends on whether the USM is enabled at the calling channel, the called channel, or both channels. If the USM is activated at the calling channel, then the USM software checks its security tables each time a user attempts to initiate a call. If the security options of the USM are activated at the called channel, then the USM software checks the security tables only when the users attempts a connection to that channel. If the USM is activated at both the calling and called channels, the USM references its tables only once at the calling channel. In addition, the USM performs security checks only once, even if the user is put into a queue to wait for a free channel or puts a channel on hold and continues with it later. The USM returns with the results of the check to the 4ASMU which then returns those results to the MCME. If the check was successful, then the user is connected; otherwise the user is disconnected from the 4ASMU. (See the following figure.)

I&A Process


VDT
USER REQUEST
PROMPTS
REQUEST FOR SECURITY CHECK
USM
4ASM
RESULT OF SECURITY CHECK
ID/PASSWORD/ DAG CHECK
BEGIN LOGON PROCEDURE
RESULTS OF SECURITY CHECK
TABLES
MCME
POSITIVE CHECK CONNECT USER TO DESINATION
NEGATIVE CHECK DISCONNECT USER
DESTINATION

USM Console

Since the USM console is password protected, an operator must enter a valid operator number and password to access the USM. If the login procedure is successful, the Master Menu appears. The Master Menu selections are:

- System Commands
- Disk Commands
- System Parameters
- Id Commands
- DAG Table
- Log-off Console

System Commands

The System Commands selection allows an operator to change passwords for operators on the USM, to view the status of the USM, and to reset the USM. Only operator one may change any password; the other operators (two through sixteen) may only change their own password. Additionally, the system verifies password changes and does not echo them to the screen.

The System Status menu selection displays the PROM revision number, the number of the operator who is currently logged in, and the number of users in the system.

By choosing the Reset option, the operator has the ability to reset the USM. Resetting the USM causes the DAG table on the disk to be loaded into RAM.

Disk Commands

The Disk Commands selection allows an operator to backup a disk, write to a disk header, format a disk, initialize a disk, and read a disk header.

The Backup selection allows the operator to copy the contents of the disk in drive one to the disk in drive two.

Selecting the Write Header to Disk option creates a 32-character disk header that can serve as a label to describe the contents of the disk.

A disk must be formatted by the Format Disk selection before it can be used by the USM. A disk can be formatted in either drive one or two. While the disk is being formatted, the USM displays a

"W" as each sector is written and a "V" as each sector is verified. When the operation has been completed, the USM displays "done".

In order to initialize a disk, it must be in drive one when the Init Disk command is run. Initialization causes the default parameters to be written out to the disk. Former user IDs, passwords, and DAGs are overwritten.

Selecting the Read Header of Disk command causes the USM to display the header of the disk in drive one.

System Parameters

There are five choices in the System Parameters menu: CR Only, Flow Control, Default User Password, Default User Group, and User Password Change Enabled. The CR Only selection allows the operator to set up the console port to transmit a CR or a CR and a linefeed when displaying menus and messages. The Flow Control parameter disables or enables the flow control at the console security port.

The Default User Password and Default User Group selections allow the operator to define a default user password and DAG respectively. The system uses these defaults when a new user is added. Unless changed by the operators, the default user is USER and the default DAG is zero.

The User Password Change Enable parameter disables or enables the ability of the user to change his/her own password.

ID Commands

The five commands of the ID Commands menu are: add a user's ID, change a user's ID information, delete a user's ID, list a user's ID(s), and print a user's ID(s). The Add a User's ID selection allows the operator to add a user, his/her password, and associated DAG. If the operator enters a CR only when prompted for the user's password and DAG, the system will assign the defaults. The Change a User's ID Information parameter allows an operator to change the selected user's password and DAG and store the new information to the disk.

The Delete a User's ID command will erase the user ID, password, and DAG information from the system. The system will respond with "DONE" when it has completed the request.

"List a User's ID" and "Print a User's ID" both display a single user and his DAG, all the users and their associated DAG, or all the users the begin with a specific letter and asterisk combination entered by the operator. The only difference between the two commands is that the first displays the information to the screen and the second sends the information to a printer.

DAG Table

The DAG codes, which are kept in the DAG tables, define a user's allowable destinations. For each user, one DAG consists of one or more DAG codes. When the DAG Table option is chosen, the operator is given the ability to add, delete, or save DAGs. Selecting Exit returns the operator to the main menu of the USM.

Log-off Console

This command logs the operator off of the USM. The USM then displays a prompt for the next logon.

Affects of USM on System Console

Installation of the USM can affect the main console format in these areas: global and channel parameters, channel commands, statistics summary report, and event message generation.

Global Parameters

The USM adds the enable feature to the GLOBAL FEATURE parameter and adds the following parameters: System Password PCI Address, System Password Channel Type, and System Password Reprompt Count. The first added feature provides the ability to enter physical address of the Password Controller Interface (PCI) channel. The second choice allows an operator to enter the type of channel that is used as the PCI channel. The last command allows the operator to define the number of times a user can fail the security checks before the system disconnects him, disables the channel, or "strings the user along."

Channel Parameters

The USM adds the enable option to the FEATURES parameter and adds the password type and password-failure action parameters. The first command allows the operator to determine which of the security checks must be completed for a successful logon (user ID, password, and DAG). The second command allows the operator to choose how to handle the defined numbered of logon failures (user disconnected, channel disabled, or user "strung along").

Channel Commands

When the USM has been activated, the CHANNEL STATUS command can execute. Thus when the command has been issued for a PCI channel, the system will respond with a message saying that the channel is busy and indicate the connection. If the USM has not been activated, then the command will return with a "invalid message" response.

Statistics Summary

Additional statistics are collected when the USM is activated. They are:

ID FAILED	- Invalid ID
PASSWORD FAILED	- Invalid password
DAC FAILED	- Incompatible DAC
PSW RESOURCE FAILED	- A bad disk or no disk has been mounted on the USM or read/write error
PSW CHANGE FAILED	- Unsuccessful change of password
ASM INPUT ERRORS	- User ID contains too many characters or an invalid character

Event Messages

The activation of the USM causes several possible event messages to be added. They are:

- A PCI channel is busy due to a configuration error.
- A user ID or password format is invalid.
- A user was not connected due to invalid DAC.
- A user was not connected due to invalid ID.
- A user was not connected due to invalid password.
- A user was not connected due to a password resource failure.
- A user changed his/her password.
- A user was unable to update his/her password.
- A user successfully logged in and all security checks were performed.

This page intentionally left blank.

EVALUATION AS AN I&A/D1 SUBSYSTEM

This section of the report maps the INX4400/USM features and assurances to the applicable CSSI requirements and interpretations for an I&A/D1 subsystem.

In summary, the INX4400 with the User Security Module option, meets and exceeds class I&A/D1 feature requirements. The INX4400/USM meets system architecture and system integrity assurance requirements, however it fails the security testing assurance requirement because test documentation was not provided. The evaluation team did produce test scenarios to assure that there were no obvious ways to circumvent the I&A mechanism(s), as claimed by the Operator's Manual.

Identification and Authentication

Requirement

> **The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.**

Interpretation

> The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.
>
> The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

Applicable Features

The User Security Module (USM) performs the security checks for the system by retrieving the user ID, password, and DAG information from its database and comparing this information with the information submitted by the user during the logon process. If the security checks return positive, the MCME then connects the user to his destination. Otherwise, logon fails and the user receives a new logon prompt. Unauthorized users may not retrieve the security information from USM database.

Conclusion

The Infotron INX4400/USM meets the D1 Identification and Authentication requirement.

System Architecture

Requirement

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the systems I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

Applicable Features

The INX4400/USM provides a domain for its own execution by providing a separate hardware and software platform than that of the protected host(s). In the evaluated configuration, this platform must be physically protected from unauthorized access. A well defined, menu driven interface protects the INX4400/USM's code and data structures from unauthorized modification. The subset of resources protected by the INX4400/USM are only users connected to a protected system through

the INX4400/USM. Those users directly connected to a protected system are outside the protection domain of the INX4400/USM.

Conclusion

The INX4400/USM meets the D1 System Architecture requirement.

System Integrity

Requirement

> **Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.**

Interpretation

> In the TCSEC quote, "TCB" is interpreted to mean "subsystem".
>
> This requirements applies to all subsystems evaluated at any class, regardless of the functions they perform.

Applicable Features

There are two types of system diagnostic test that can be run at the system administrator's convenience. The first set of diagnostics checks the supervisory link errors, thus determining if there are any problems with an SBIRM, an SCMU/LCM or a switch cable bus. The second, the switch bus data path test, detects switch bus data and control lead errors. In addition, there are real-time supervisory link checks, which run during normal system operations, that will produce a critical error report identifying the link with the error. For more information on how to run and understand the tests exists in the INX4400 Operation Manual under the maintenance section.

Conclusion

The Infotron INX4400/USM meets the D1 System Integrity requirement.

Security Testing

Requirement

> **The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an**

unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB.

Interpretation

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

Applicable Features

Although the evaluation team performed limited security testing, Infotron did not provide tests or test results to the team. The team's tests attempted to verify that the subsystem's SRP worked as claimed in the subsystem's documentation.

Conclusion

Since Infotron did not provide the evaluation team with security tests, the Infotron INX4400/USM does not meet the D1 Security Testing requirement.

Security Features User's Guide

Requirement

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Interpretation

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

Applicable Features

The INX4400 Operation Manual (Part No. 950067) dated February 1988 contains an appendix B entitled "User Security". Although this appendix is intended to address the security officer at the security console and the system administrator/operator at the system console, it provides minimal guidance to the user on the security features provided by the INX4400/USM. It does not provide guidelines for the use of these security features.

Conclusion

The Infotron INX4400/USM does not meet the D1 Security Features User's Guide requirement.

Trusted Facility Manual

Requirement

> **A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.**

Interpretation

> This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

Applicable Features

The INX4400 Operation Manual (Part No. 950067) dated February 1988 contains an appendix B entitled "User Security". Although this appendix is intended to address the security officer at the security console and the system administrator/operator at the system console, it does not provide guidance on running in a secure facility, nor does it provide direction for effectively integrating the INX4400/USM into an overall system.

Conclusion

The Infotron INX4400/USM does not meet the D1 Trusted Facility Manual requirement.

Test Documentation

Requirement

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Interpretation

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

Applicable Features

Infotron did not provide any test documentation to the evaluation team.

Conclusion

The Infotron INX4400/USM does not meet the D1 Test Documentation requirement.

Design Documentation

Requirement

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact

with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

Applicable Features

Infotron does not have a document that describes Infotron's philosophy of protection and, consequently, does not have a document that shows how this philosophy is implemented in the INX4400/USM.

Conclusion

The Infotron INX4400/USM does not meet the D1 Design Documentation requirement.

This page intentionally left blank.

EVALUATOR'S COMMENTS

The evaluation team perceives the INX4400/USM to be a very good product. Although the given rating is a class I&A/D, the subsystem does possess some features that meet and exceed the I&A/D1 requirements.

Both the Security Console and the System Console require passwords to access the main menus. The USM (security console) allows individual ID and password combinations to be assigned to users. The System Console allows 1 master operator ID and password for the system console and 15 subordinate system console operator IDs and passwords. The master operator can control which system console menus the other subordinate system operators may access. The IDs and passwords for users are accessible via the USM software, whereas system operator IDs and passwords are accessible via the System Console; one does not know about the other. An important note: the USM can be logically turned off and/or restrictions overridden by someone who has access to the System Console. For this reason, assigning one person as the Security Officer (USM controller) and the System Operator (master operator) should be taken under consideration.

The deficiency of required documentation (Security Features User's Guide, Trusted Facility Manual, Test Documentation, and Design Documentation) kept this product from exceeding a class I&A/D rating. The evaluation team depended on the Operator's Manual for guidance, which in many areas was lacking the in-depth detail the team required.

This page intentionally left blank.

EVALUATED HARDWARE COMPONENTS

Scope of Hardware Evaluation

The hardware covered by this evaluation is the Infotron INX4400 product line, including hardware present in the field at existing customer sites.

The primary requirement for hardware evaluation is that the hardware function properly. This was verified by the system integrity tests (see page 9, "System Integrity") and was not given a detailed reevaluation by the team. The integrity assurances provided by the Infotron-supplied diagnostic tests are satisfactory.

List of Evaluated Components

This section lists the Infotron marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluated release.

To operate in correspondence with the I&A/D rating, the hardware configuration must contain only components listed in this section.

INX4400 Master Control Unit (Stand-Alone Model)

1 ISS/MCME Master Controller Module with Expanded Memory (MCME)

1 ISS/MSME Master Support Module with Expanded Memory (MSME)

1 ISS/MEM Memory Expansion Module

1 ISS/DCM Disk Controller Module

1 ISS/SBIRM Switch Bus Interface Module with Remote Master Capability (SBIRM)

1 ISS/USM User Security Module (USM)

INX4400 Expansion Unit (Stand-Alone Model)

2 Slave Controller Module with Expanded Memory (SCME)

1 Quad Asynchronous Service Module Universal (4ASMU)

4 Quad Asynchronous Character-Oriented Channel Adapter (4AC5)

This page intentionally left blank

EVALUATED SOFTWARE COMPONENTS

Scope of Software Evaluation

This section lists the programs that make up the various major divisions of the INX4400/USM software.

SRP Software

System Software - revision level 12A.2

USM (User Security Module) Software - revision level 12A.2

This page intentionally left blank.

GLOSSARY

The following section defines terms commonly used in this report.

4AC5 - Quad Asynchronous Character-Oriented Channel Adapter

4ASMU - Quad Asynchronous Service Module Universal

ADP - Automated Data Processing

ASM - Asynchronous Service Module

CSSI - Computer Security Subsystem Interpretation

DAC - Destination Access Criteria

DAG - Discretionary Access Group

DCM - Disk Controller Module

EPL - Evaluated Products List

INX - Intelligent Network Exchange

IOAM - Input Output Address Memory

KSR - Keyboard Select Routing

LCM - Link Control Module

MCME - Master Controller Module with Expanded memory

MEM - Memory Module

MSAC - Master Scan Address Counter

MSME - Master Support Module with Expanded memory

MUX - Multiplexer

NCSC - National Computer Security Center

NSDD - National Security Decision Directive

PCI - Password Controller Interface

PIA - Parallel Interface Adapter

PROM - Programmable Read-Only Memory

RAG - Restricted Access Group

RAM - Random Access Memory

ROM - Read-Only Memory

SAC - Slave Address Counter

SBIRM - Switch Bus Interface Controller Module

SCME - Slave Controller Module with Expanded Memory

SCMU - Slave Controller Module Universal

SRP - Security Relevant Portion

TCSEC - Trusted Computer System Evaluation Criteria

TSFM - Time Slot Function Memory

T1/M2CM - High Speed Data Links

UART - Universal Asynchronous Receiver/Transmitter

USART - Universal Synchronous/Asynchronous Receiver/Transmitter

USM - User Security Module

VS1/VS2LM - High Speed Data Links

VS1/VS2LME - High Speed Data Links

XOR - Exclusive OR

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT **UNLIMITED DISTRIBUTION**
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL--SUM-89/002	5 MONITORING ORGANIZATION REPORT NUMBER(S) S232,551
6a NAME OF PERFORMING ORGANIZATION **National Computer Security Center** 6b OFFICE SYMBOL (If applicable) **C12**	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State and ZIP Code) **9800 Savage Road** **Ft. George G. Meade, MD 20755-6000**	7b ADDRESS (City, State and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State and ZIP Code)	10 SOURCE OF FUNDING NOS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO
11 TITLE (Include Security Classification) **Final Evaluation Report INFORTRON INX4400/USM**	
12 PERSONAL AUTHOR(S) **Karen M. Bielat; Caralyn C. Crescenzi; David N. Robidoux; John W. Taylor**	
13a TYPE OF REPORT **Final**	13b TIME COVERED FROM ____ TO ____
14 DATE OF REPORT (Yr, Mo., Day) **890608**	15 PAGE COUNT **45**
16 SUPPLEMENTARY NOTATION	

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB GR	**NCSC, I&A, Infotron, INX4400/USM, CSSI**

19 ABSTRACT (Continue on reverse side if necessary and identify by block number)

The INFOTRON INX4400/USM has been evaluated by the National Computer Security Center (NCSC). The security features of the INX4400/USM were examined against the requirements specified by the *COMPUTER SECURITY SUBSYSTEM INTERPRETATION OF THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (CSSI) dated 16 September 1988.* The NCSC evaluation team has determined that the INX4400/USM has some I&A/D1 and I&A/D2 class features, however, all requirements of a given class must be met for a subsystem to receive that rating. It has been determined that the highest class at which the INX4400/USM satisfies all the specified requirements of the CSSI is class I&A/D.

This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL **DENNIS E. SIRBAUGH**	22b TELEPHONE NUMBER (Include Area Code) **(301)859-4458** 8b OFFICE SYMBOL **C12**

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE