The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SPACECRAFT ONBOARD INTERFACE SERVICES—DEVICE ACCESS SERVICE

RECOMMENDED PRACTICE

CCSDS 871.0-M-1

MAGENTA BOOK

March 2013

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Practices

SPACECRAFT ONBOARD INTERFACE SERVICES—DEVICE ACCESS SERVICE

RECOMMENDED PRACTICE

CCSDS 871.0-M-1

MAGENTA BOOK

March 2013

AUTHORITY

Issue:	Recommended Practice, Issue 1
Date:	March 2013
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 871.0-M-1	Spacecraft Onboard Interface Services—Device Access Service, Recommended Practice, Issue 1	March 2013	Current issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE AND SCOPE OF THIS DOCUMENT

This document is one of a family of documents specifying the Spacecraft Onboard Interface Services (SOIS)-compliant service to be provided in support of applications.

The purpose of this document is to define services and service interfaces provided by the SOIS Device Access Service (DAS). Its scope is to specify the service only and not to specify methods of providing the service, although use of the SOIS subnetwork services is assumed.

This document conforms to the principles set out in the SOIS Green Book (reference [D3]) and is intended to be applied together with it.

1.2 APPLICABILITY

This document applies to any mission or equipment claiming to provide a SOIS-compatible DAS.

1.3 RATIONALE

SOIS provide service interface specifications in order to promote commonality of functionality amongst systems implementing well-defined services. These interfaces do not dictate implementation of interfaces or protocols supporting the services.

1.4 DOCUMENT STRUCTURE

This document has four major sections:

- this section, containing administrative information, definitions, and references;
- section 2, containing general concepts and assumptions;
- section 3, containing the Device Access Service, in terms of the services provided, services expected from underlying layers, and the service interface;
- section 4, containing the Management Information Base (MIB) for this service.

In addition, one normative and three informative annexes are provided:

- annex A, comprising a Service Conformance Statement Proforma;
- annex B, discussing security considerations relating to the specifications of this document;
- annex C, containing a list of acronyms;
- annex D, containing a list of informative references.

1.5 CONVENTIONS AND DEFINITIONS

1.5.1 DEFINITIONS

1.5.1.1 General

For the purpose of this document the following definitions apply.

1.5.1.2 Definitions from the Open Systems Interconnection (OSI) Basic Reference Model

This document is defined using the style established by the Open Systems Interconnection (OSI) Basic Reference Model (reference [D2]). This model provides a common framework for the development of standards in the field of systems interconnection.

The following terms used in this Recommended Practice are adapted from definitions given in reference [D2]:

(N)-layer: A subdivision of the architecture, constituted by subsystems of the same rank (N).

(N)-protocol: A set of rules and formats (semantic and syntactic) which determines the communication behaviour of (N)-entities in the performance of (N)-functions.

(N)-protocol-data-unit: A unit of data specified in an (N)-protocol and consisting of (N)-protocol-controlinformation and possibly (N)-user-data.

(N)-service: Capability of a layer, and the layers beneath it (service providers), provided to the service users at the boundary between the service providers and the service users.

(N)-service-access-point, (N)-SAP: The point at which (N)-services are provided by an (N)-entity to an (N+l)-entity. Within the spacecraft, a SOIS User SAP. As a minimum it locates a data system and an application within that data system.

1.5.2 TERMS DEFINED IN THIS RECOMMENDED PRACTICE

For the purposes of this Recommended Practice, the following definitions also apply.

application: Any component of the onboard software that makes use of the DAS.

NOTE – Such components include flight software applications and higher-layer services.

device: Real hardware component of the spacecraft or a single register within such a component.

NOTE – Examples of such component are sensors and actuators.

physical device identifier: Abstract identification of a device.

NOTE – The format of a device identifier is implementation-specific.

remotely connected device: Device that for access requires the use of a device-specific access protocol that connects two different instances of the DAS in such a way that the first relays the user requests to the second, which in turn directly accesses the remote device.

timestamp: Time associated with a value.

NOTES

1 The format of a timestamp is implementation-specific.

2 The timestamp may indicate the time the value was generated by the device, emitted by the device, or acquired by the service. This is implementation-specific.

value: Formatted atomic unit of data that is acquired from or used as a command to a device.

value identifier: Abstract identification of a value.

NOTE – The format of a value identifier is implementation-specific.

1.6 NOMENCLATURE

1.6.1 NORMATIVE TEXT

The following conventions apply for the normative specifications in this Recommended Practice:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.6.2 INFORMATIVE TEXT

In the normative sections of this document, informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

- Overview;
- Background;
- Rationale;
- Discussion.

1.7 REFERENCES

This document contains no normative references. Informative references are contained in annex D.

2 OVERVIEW

2.1 FUNCTION

The DAS provides a standard interface between onboard software applications and flight hardware such as sensors and actuators.

2.2 CONTEXT

The DAS is defined within the context of the overall SOIS architecture (reference [D3]) as one of the Command and Data Acquisition services of the Application Support Layer, as illustrated in figure 2-1.

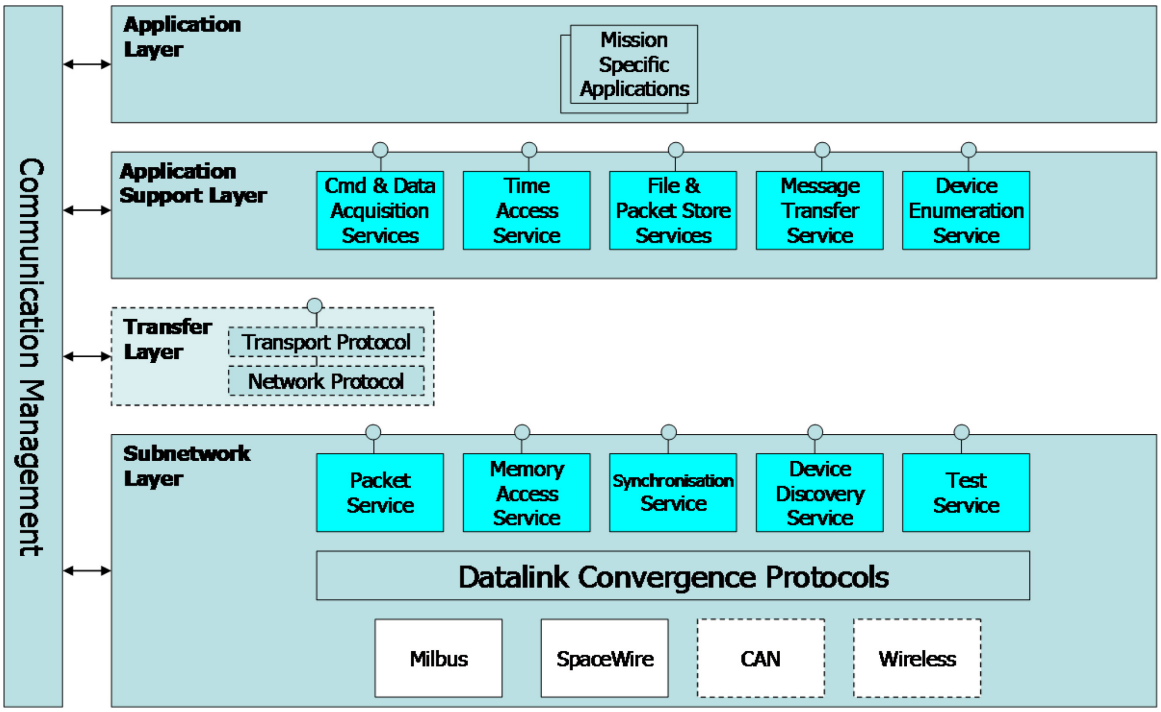

Figure 2-1: Command and Data Acquisition Services Context

The relationship of the DAS to the other Command and Data Acquisition services is illustrated in figure 2-2.

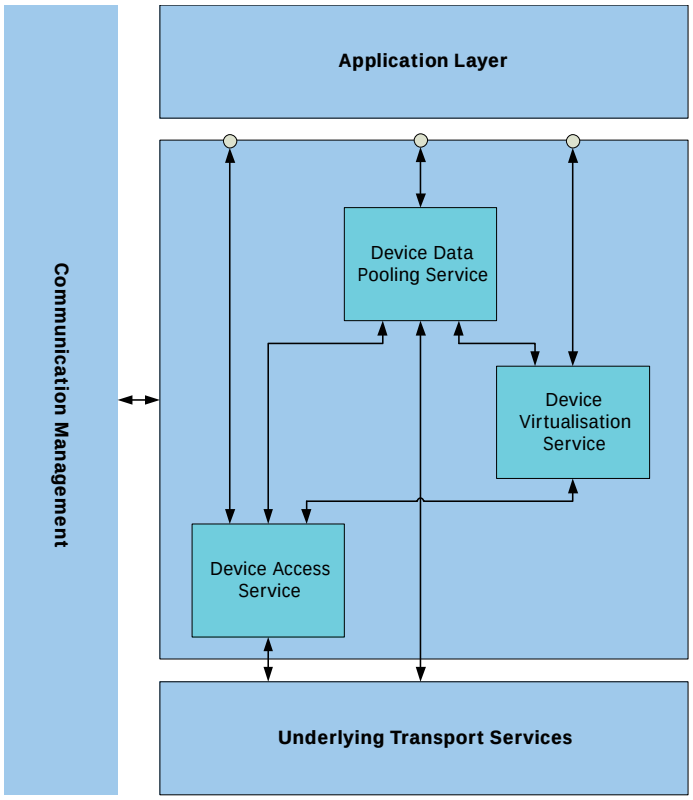

Figure 2-2: Relationship between Command and Data Acquisition Services

The DAS provides a standard interface between onboard software applications and flight hardware such as sensors and actuators. The basic concept underlying the service is that the software application is able to access hardware devices independently of the precise physical location of the device, and without requiring detailed knowledge of the electrical interface to the device. A standard interface makes it easier to develop the onboard software, enables configuration changes in the spacecraft design to be easily tolerated, and increases the re-use potential of the software.

To acquire a value (i.e., data) from a device, an application provides a physical device identifier and a value identifier. The service resolves the physical device identifier in order to determine the Device-specific Access Protocol (DAP) and an Underlying Transport (UT) service. The service maps information associated with the request onto the parameters of the protocol or the underlying service's service-access-point, e.g., destination address and QoS parameters. The service then uses the DAP to transfer the value from the device and returns the acquired value. The logical relationship between the service, the DAPs and the UT service-access-points is illustrated in figure 2-3.

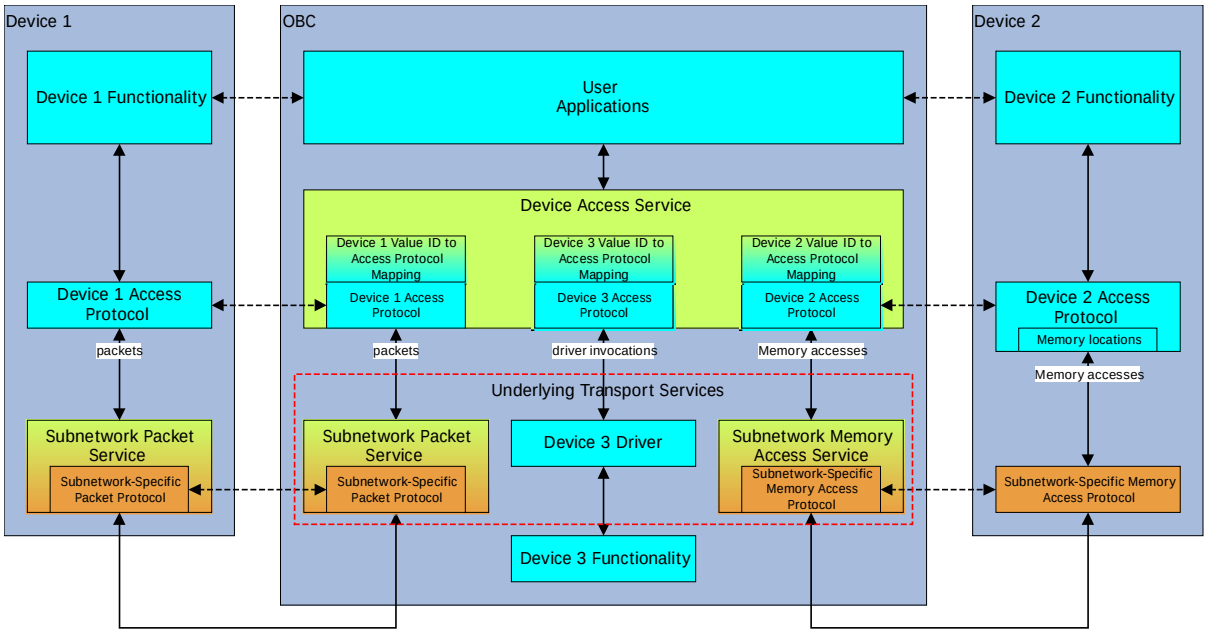

Figure 2-3: Relationship between DAS, DAPs, and Underlying SAPs

Certain devices asynchronously emit values that are stored by the service.[1] To acquire such a value, an application provides a device logical identifier and a value identifier, which the service resolves in order to determine the stored value. The service then returns the most recently stored value. Optionally, the service may emit an indication to an application when an asynchronously emitted value from a device is acquired by the service.

Optionally, the service may indicate a timestamp associated with an acquired value. This timestamp indicates the time the value was generated by the device, emitted by the device, or acquired by the service (which is implementation-specific).

To command (i.e., send a value to) a device, an application provides a physical device identifier and a value identifier, together with the command value to be sent. The service resolves the physical device identifier in order to determine the DAP and a UT service, and if a response is generated by the device (as some devices do not generate a response to a command). The service maps information associated with the request onto the parameters of the protocol or the underlying service's service-access-point, e.g., destination address and QoS parameters. The service then uses the DAP to command the device.

Figure 2-3 also illustrates how the DAS accesses devices using an underlying packet service or directly accesses them using a local driver. The benefit of the service is that the user is no longer concerned with the details of the location of the sensor, its physical interface, or how it is accessed (i.e., communication protocols). As a result, configuration changes involving a change in the physical location of a device, or changes to its electrical interface, do not require changes to the application software using that device.

[1] The manner in which the emitted value is obtained by the service is part of the DAP.

Although isolated from the details of device location and interface type, the user still needs to know the format of command values sent to and data values acquired from the device, and the user remains responsible for correctly composing and interpreting those formats.

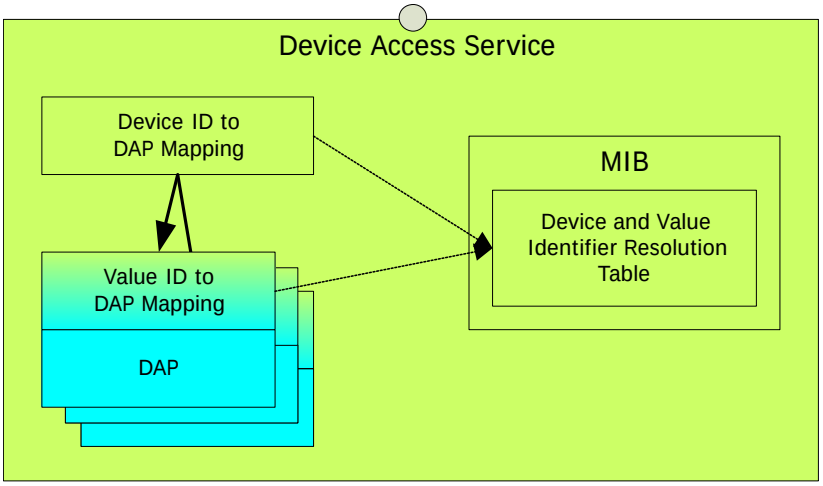

Figure 2-4: Relationship between DAS, DAPs and MIB

A MIB is also provided for the configuring, managing, and collecting status information from the DAS (see figure 2-4).

2.3 PURPOSE AND OPERATION OF THE DEVICE ACCESS SERVICE

Applications use the DAS to acquire data from and send commands to devices rather than to read or write directly to the hardware itself.

The DAS provides a consistent, standard interface to onboard software; the interfaces are described by sets of primitives and related parameters.

From the application software perspective, use of the DAS will result in applications that are more portable, that are easier to develop, and that can tolerate changes in the spacecraft hardware configuration.

From the spacecraft platform implementers' perspective, use of the DAS will make it easier to control the access to shared hardware resources.

3 DEVICE ACCESS SERVICE

3.1 PROVIDED SERVICE

3.1.1 GENERAL

3.1.1.1 The DAS shall provide on-demand access to (i.e., commanding of and acquiring data from) devices using a logical identifier to identify the device and a value identifier.

3.1.1.2 The DAS shall map information associated with the request onto the parameters of the DAP and the UT service-access-point.

NOTE – E.g., destination address and QoS parameters.

3.1.2 DATA ACQUISITION

3.1.2.1 For data acquisition, the service must take the appropriate action to acquire the value from the specified device and return it to the application.

3.1.2.2 The format of the value acquired from the device shall be preserved regardless of any encapsulation.

NOTE – In order to transfer this value from a remotely located device, the value can be encapsulated within another data structure, e.g., to be transferred across an underlying bus.

3.1.3 COMMANDING (OPTIONAL)

3.1.3.1 For commanding, the value to be sent to the specified device is provided as a parameter by the application, and the service shall preserve the format of this data so that it is received by the device exactly as it is provided.

NOTE – Again, preservation of format can require encapsulation within another data structure in order to deliver the value to the device.

3.1.3.2 In the cases where a command operation on a device elicits a response from the device, the response value shall be returned to the application.

3.2 EXPECTED SERVICES FROM UNDERLYING LAYERS

3.2.1.1 For locally connected devices, the expected service shall provide direct access to the underlying hardware registers.

3.2.1.2 For remotely connected devices, the expected service provides the capability to relay device access requests to, and responses from, the remotely connected device.

NOTES

1 Definition of remotely connected device can be found in 1.5.2.

2 As shown in 3.2.1.1 and 3.2.1.2, the minimum expected service from the underlying layers depends on the physical location of the device to be accepted.

3.3 SERVICE PARAMETERS

3.3.1 GENERAL

The DAS shall use the parameters specified in 3.3.2 to 3.3.6.

3.3.2 TRANSACTION IDENTIFIER

3.3.2.1 The Transaction Identifier parameter shall be a value, assigned by the invoking user entity, which is subsequently used to associate indication primitives with the causal request primitives.

NOTE – The user entity is thus able to correlate all indications and confirmations with the originating service request.

3.3.2.2 Transaction Identifier shall be unique within the user application entity.

3.3.3 RESULT METADATA

The Result Metadata parameter shall be used to provide information generated by the DAS provider to the service invoking entity to provide information related to the successful or failed result of a device access operation.

NOTE – The parameter can also include other information indicating failure conditions, e.g., that the specified request could not be serviced within the managed timeout period or the DAS is not functioning correctly.

3.3.4 PHYSICAL DEVICE IDENTIFIER

The Physical Device Identifier parameter shall be used to identify the device from which a value is to be acquired.

3.3.5 VALUE IDENTIFIER

The Value Identifier parameter shall be used to identify the data value to be acquired from the device or the command value to be sent to the device.

3.3.6 VALUE

The Value parameter shall be used to state the value acquired from or previously asynchronously emitted by the device, or the command value that is to be sent to the device.

3.3.7 TIMESTAMP

3.3.7.1 The Timestamp parameter shall be used to indicate a time associated with a value.

3.3.7.2 The Timestamp may indicate the time the value was generated by the device, emitted by the device, or acquired by the service. This is implementation-specific.

3.4 DEVICE ACCESS SERVICE PRIMITIVES

3.4.1 GENERAL

3.4.1.1 The DAS interface shall implement the following primitives:

a) ACQUIRE_FROM_DEVICE.request, as specified in 3.4.2;

b) ACQUIRE_FROM_DEVICE.indication, as specified in 3.4.3.

3.4.1.2 The DAS interface may implement the following primitives:

a) COMMAND_DEVICE.request, as specified in 3.4.4;

b) COMMAND_DEVICE.indication, as specified in 3.4.5.

3.4.2 ACQUIRE_FROM_DEVICE.REQUEST

3.4.2.1 Function

The **ACQUIRE_FROM_DEVICE.request** primitive shall be passed to the DAS provider to request that a data value be acquired from a device.

3.4.2.2 Semantics

The **ACQUIRE_FROM_DEVICE.request** primitive shall use the following semantics, with the meaning of the parameters specified in 3.3.

ACQUIRE_FROM_DEVICE.request (Transaction Identifier,
Physical Device Identifier, Value Identifier)

3.4.2.3 When Generated

The **ACQUIRE_FROM_DEVICE.request** primitive shall be passed to the DAS provider to request that a data value be acquired from a device.

3.4.2.4 Effect on Receipt

3.4.2.4.1 Receipt of the **ACQUIRE_FROM_DEVICE.request** primitive shall cause the DAS provider to acquire data value from a device.

3.4.2.4.2 Depending upon the nature of the device, the data value acquired shall be either a value directly acquired from the device or the value most recently asynchronously emitted by the device.

3.4.3 ACQUIRE_FROM_DEVICE.INDICATION

3.4.3.1 Function

The **ACQUIRE_FROM_DEVICE.indication** primitive shall be used to pass the acquired data to the user entity.

3.4.3.2 Semantics

The **ACQUIRE_FROM_DEVICE.indication** primitive shall use the following semantics, with the meaning of the parameters specified in 3.3.

ACQUIRE_FROM_DEVICE.indication (Transaction Identifier, Value,
Result Metadata, Timestamp (optional))

3.4.3.3 When Generated

3.4.3.3.1 The **ACQUIRE_FROM_DEVICE.indication** primitive shall be issued by the service provider to the receiving user entity in response to an ACQUIRE_FROM_DEVICE.request.

NOTE – This primitive:

- contains the value directly acquired from or, where an asynchronously emitted value is requested, the value previously emitted by the device, and
- provides metadata concerning whether the request was executed successfully or not.

3.4.3.3.2 Optionally, the **ACQUIRE_FROM_DEVICE.indication** primitive may be issued by the service provider to the receiving user entity in response to an asynchronously emitted value received by the DAS.

3.4.3.4 Effect on Receipt

The response of the user entity to an **ACQUIRE_FROM_DEVICE.indication** primitive is unspecified.

3.4.4 COMMAND_DEVICE.REQUEST

3.4.4.1 Function

The **COMMAND_DEVICE.request** primitive shall be used to request the service to command a device.

3.4.4.2 Semantics

The **COMMAND_DEVICE.request** primitive shall use the following semantics, with the meaning of the parameters specified in 3.3.

COMMAND_DEVICE.request (Transaction Identifier, Physical Device Identifier, Value Identifier, Value)

3.4.4.3 When Generated

The **COMMAND_DEVICE.request** primitive shall be passed to the DAS provider to request that a command value be sent to a device.

3.4.4.4 Effect on Receipt

Receipt of the **COMMAND_DEVICE.request** primitive shall cause the DAS provider to send a command value to the device.

3.4.5 COMMAND_DEVICE.INDICATION

3.4.5.1 Function

The **COMMAND_DEVICE.indication** primitive shall be used to pass the response to a command to a device to the user entity.

3.4.5.2 Semantics

The **COMMAND_DEVICE.indication** primitive shall use the following semantics, with the meaning of the parameters specified in 3.3.

COMMAND_DEVICE.indication (Transaction Identifier, Result Metadata)

3.4.5.3 When Generated

The **COMMAND_DEVICE.indication** primitive shall be issued by the service provider to the receiving user entity in response to a COMMAND_DEVICE.request.

3.4.5.4 Effect on Receipt

The response of the user entity to a **COMMAND_DEVICE.indication** primitive is unspecified.

3.4.5.5 Discussion

The Result Metadata parameter can also contain other information indicating failure conditions such as Device or Value Identifier resolution failure or an inability to write to the device. It can also contain ancillary information that is returned by the device in response to the command.

Not all devices will produce a response when a command value is sent to them. As specified in section 4, the Device and Value Identifier Resolution Table indicate to the service whether a specific device will generate a response or not. Where a device does not generate a response, a COMMAND_DEVICE.indication can indicate only that the command was successfully sent or that there was an error at the sending side; there can be no indication of whether the command was received by the device or successfully acted upon.

4 MANAGEMENT INFORMATION BASE

4.1 OVERVIEW

There is currently no MIB associated with this service. All management items are associated with the implementation providing the service. However, guidance is provided as to MIB contents in 4.3.

4.2 SPECIFICATIONS

Any protocol claiming to provide this service in a SOIS-compliant manner shall publish its MIB as part of the protocol specification.

4.3 MIB GUIDANCE

The MIB of the protocol providing the DAS should consider the following aspects:

Device and Value Identifier Resolution Table, as specified in 4.4.

NOTE – These aspects are not in any way an indication of the complete contents of a MIB for a protocol providing the DAS but are offered as guidance as to those aspects of the MIB which may relate to DAS interface.

4.4 DEVICE AND VALUE IDENTIFIER RESOLUTION TABLE

4.4.1 The **Device and Value Identifier Resolution Table** shall contain a set of managed parameters that map device and value identifiers onto individual DAPs, underlying services, and their associated available addressing mechanisms.

4.4.2 The table specified in 4.4.1 should indicate to the service whether or not a specific device will generate a response.

4.4.3 Any entity managing the service should be able to:

a) access the table specified in 4.4.1; and

b) update it to reflect changes in the flight hardware configuration and relocation of devices.

NOTE – Whether the Device and Value Identifier Resolution Table can be updated dynamically during service operation is not specified here. This question is an implementation issue to be decided according to the needs of the particular mission for which the service implementation is being developed.

ANNEX A

DEVICE ACCESS SERVICE PRTOOCOL IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(NORMATIVE)

A1 INTRODUCTION

This annex provides the Protocol Implementation Conformance Statement (PICS) Requirements List (PRL) for implementation of the DAS, CCSDS 871.0-M-1, March 2013. The PICS for an implementation is generated by completing the PRL in accordance with the instructions below. An implementation shall satisfy the mandatory conformance requirements of the base standards referenced in the PRL.

The PRL in this annex is blank. An implementation's complete PRL is called a PICS. The PICS states which capabilities and options of the services have been implemented. The following can use the PICS:

- The service implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;
- The supplier and acquirer or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- The user or potential user of the implementation, as a basis for initially checking the possibility of interoperability with another implementation;
- A service tester, as a basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A2 NOTATION

The following are used in the PRL to indicate the status of features:

Status Symbols

M	mandatory
O	optional

Support Column Symbols

The support of every item as claimed by the implementer is stated by entering the appropriate answer (Y, N or N/A) in the Support column:

Y	Yes, supported by the implementation
N	No, not supported by the implementation
N/A	Not applicable

A3 REFERENCED BASE STANDARDS

The base standards references in the PRL are:

– Device Access Service – this document.

A4 GENERATION INFORMATION

A4.1 IDENTIFICATION OF PICS

Ref	Question	Response
1	Date of Statement (DD/MM/YYYY)	
2	PICS serial number	
3	System Conformance statement cross-reference	

A4.2 IDENTIFICATION OF IMPLEMENTATION UNDER TEST (IUT)

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Special configuration	
4	Other information	

A4.3 IDENTIFICATION

Ref	Question	Response
1	Supplier	
2	Contact Point for Queries	
3	Implementation name(s) and Versions	
4	Other information necessary for full identification, e.g., name(s) and version(s) for machines and/or operating systems: System Name(s)	

A4.4 SERVICE SUMMARY

Ref	Question	Response
1	Service Version	
2	Addenda implemented	
3	Amendments implemented	
4	Have any exceptions been required? NOTE – A YES answer means that the implementation does not conform to the service. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming.	Yes _____ No _____

A5 INSTRUCTIONS FOR COMPLETING THE PRL

An implementer shows the extent of compliance to the protocol by completing the PRL; that is, compliance to all mandatory requirements and the options that are not supported are shown. The resulting completed PRL is called a PICS. In the Support column, each response shall be selected either from the indicated set of responses or it shall comprise one or more parameter values as requested. If a conditional requirement is inappropriate, N/A shall be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference X*i*, where *i* is a unique identifier, to an accompanying rationale for the non-compliance.

A6 GENERAL/MAJOR CAPABILITIES

Service Feature	Reference	Status	Support
ACQUIRE_FROM_DEVICE.request	3.4.2	M	
ACQUIRE_FROM_DEVICE.indication	3.4.3	M	
COMMAND_DEVICE.request	3.4.4	O	
COMMAND_DEVICE.indication	3.4.5	O	
Timestamp parameter	3.3.7	O	

ANNEX B

SECURITY CONSIDERATIONS

(INFORMATIVE)

B1 SECURITY BACKGROUND

The SOIS services are intended for use with protocols that operate solely within the confines of an onboard subnet. It is therefore assumed that SOIS services operate in an isolated environment which is protected from external threats. Any external communication is assumed to be protected by services associated with the relevant space-link protocols. The specification of such security services is out of scope of this document.

B2 SECURITY CONCERNS

At the time of writing there are no identified security concerns. If confidentiality of data is required within a spacecraft it is assumed it is applied at the Application Layer. For more information regarding the choice of service and where it can be implemented, see reference [D4].

B3 POTENTIAL THREATS AND ATTACK SCENARIOS

Potential threats and attack scenarios typically derive from external communication and are therefore not the direct concern of the SOIS services, which make the assumption that the services operate within a safe and secure environment. It is assumed that all applications executing within the spacecraft have been thoroughly tested and cleared for use by the mission implementer. Confidentiality of applications can be provided by Application Layer mechanisms or by specific implementation methods such as time and space partitioning. Such methods are outside the scope of SOIS.

B4 CONSEQUENCES OF NOT APPLYING SECURITY

The security services are out of scope of this document and are expected to be applied at layers above or below those specified in this document. If confidentiality is not implemented, science data or other parameters transmitted within the spacecraft might be visible to other applications resident within the spacecraft resulting in disclosure of sensitive or private information.

ANNEX C

ACRONYMS

(INFORMATIVE)

CCSDS	Consultative Committee for Space Data Standards
DAP	Device-specific Access Protocol
DAS	Device Access Service
ID	Identifier
MIB	Management Information Base
OSI	Open Systems Interconnection
SAP	service-access-point
SOIS	Spacecraft Onboard Interface Services
UT	underlying transport

ANNEX D

INFORMATIVE REFERENCES

(INFORMATIVE)

[D1] *Organization and Processes for the Consultative Committee for Space Data Systems*. CCSDS A02.1-Y-3. Yellow Book. Issue 3. Washington, D.C.: CCSDS, July 2011.

[D2] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. International Standard, ISO/IEC 7498-1:1994. 2nd ed. Geneva: ISO, 1994.

[D3] *Spacecraft Onboard Interface Services*. Report Concerning Space Data System Standards, CCSDS 850.0-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, June 2007.

[D4] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

NOTE – This document contains no normative references.