Objectory/Cleanroom Specification Practices Integration

Software Technology for Adaptable Reliable Systems

Satellite Control System Requirements

Addendum 1:
COMBIZ SATELLITE CONTROL SYSTEM REQUIREMENTS (ORIGINAL)

Table of Contents

I. COMBIZ Satellite Control System Overview

Contents:

1. Background

COMBIZ is a company that provides its internal and external customers with a satellite data communications service. COMBIZ's satellite communications assets are managed by a Ground Control System (GCS). The GCS is responsible for the health and maintenance of the Satellite Control System (SCS) as well as for scheduling bulk data communication time slots for its customers. The SCS is the primary interface for COMBIZ's satellite bulk data transmission customers who operate satellite data communication uplink and downlink sites.

The COMBIZ's satellite constellation consists of three satellites, each with an 8-hour contact window with one of three GCS ground sites. Thus, there is 24-hour satellite coverage to address all ground control system operations and customer data communication requirements. The three satellites and their hardware and software systems represent the SCS. The three ground control sites represent the Ground Control System.

The GCS directs the SCS activities on the basis of pre-scheduled time slots. Time slots are allocated for maintenance activities and customer data transmission preparation, e.g., pointing a satellite by executing a firing command or updating the SCS's broadcast/location table. Time slots are also allocated for customer data transmission. After system initialization, a maintenance time slot is always performed, followed by a customer data transmission time slot, followed by another maintenance time slot. Maintenance time slots and customer data transmission time slots are performed in alternating order. We refer to the activities performed during a maintenance time slot as a "Manage Satellites" transaction. We refer to the activities performed during a customer data transmission time slot as a "Transmit Data" transaction.

2. Mission

The mission of the Satellite Control System is to manage the system's satellite assets to ensure the reliable throughput of communication packets from uplink to downlink satellite data communication sites within that customer's allotted time slot and to minimize the amount of time required for allocation to maintenance time slots.

3. System Boundaries

The SCS interfaces with ground control sites and customer satellite data communication (uplink and downlink) sites. The SCS receives telemetry and command (T&C) messages from a ground control site of the GCS and receives from the system acknowledgment messages as to whether the commands sent were successfully executed or not. The SCS also receives communication packets from sender communication sites and relays them to receiver communication sites.

The satellite and the hardware and software necessary to accept and process control messages and to receive and forward communication packets are included within the boundaries of the SCS.

The context diagram for the Satellite Control System is shown in Figure 1.
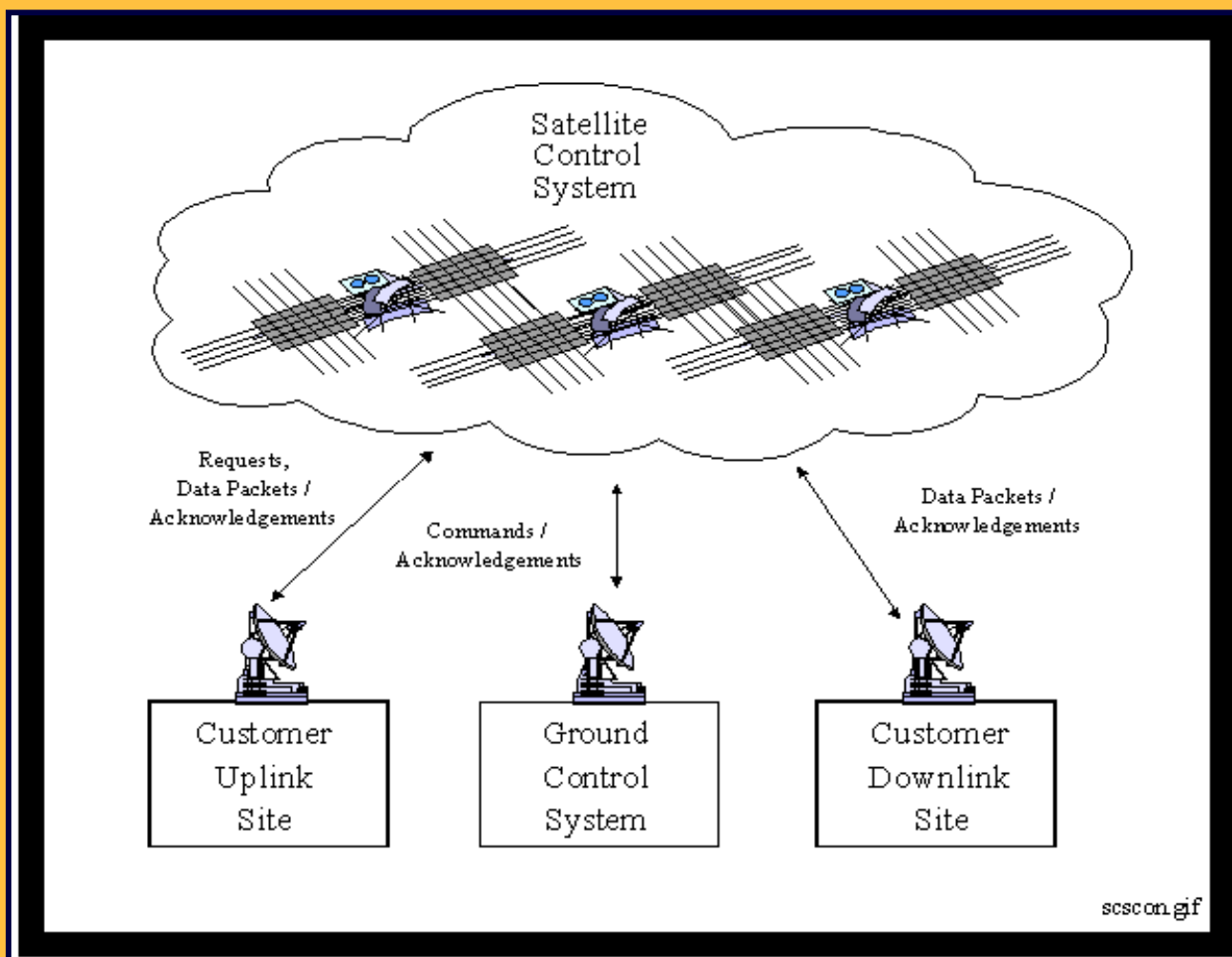

Figure 1. Satellite Control System Context Diagram

II. Terminology

Contents

1. Introduction

This section identifies terms used to describe the SCS.

2. Items

2.1 **Attitude** - refers to the satellite's position, with respect to an artificial horizon, in terms of its yaw (X), pitch (Y), and roll (Z) coordinates.

2.2 **Bandwidth** - is a measure of thoughput, i.e., the number of bytes that can be transferred within a given unit of time. Bandwidth is defined in terms of the speed by which an uplink site may communicate with a downlink site in terms of KPS (kilobytes per second) or MPS (megabytes per second).

2.3 **Data Lock** - refers to an event where a satellite data communications site is able to upload/download data packets with error rates acceptable to transmit data.

2.4 **Site Location** - refers to the geographical coordinates (latitude, longitude) of a satellite data communications site.

2.5 **Space Communication Asset** - refers to a satellite of the SCS, and any related hardware element.

2.6 **Time Slot** - a period of time allocated to perform a scheduled activity. For example, a *maintenance time slot* may be allocated five minutes to execute satellite maintenance commands.

2.7 **Uplink/Downlink Site-SCS Connection** - refers to the successful connection between a satellite data communications site specified as the uplink site to a satellite data communications site specified as the downlink site via the SCS.

3. Acronyms

General Acronyms :

B/L Table - Bandwidth/Location Table

CSDC Site - Customer Satellite Data Communications Site

GCS - Ground Control System

MS Transaction - Manage Satellites Transaction

SCS - Satellite Control System

SDC Site - Satellite Data Communications Site

TD Transaction - Transmit Data Transaction

SCS Input and Output Mnemonics :

Inputs:

IN - Initialize SCS

MG - Maintenance time slot go

HR - Satellite health request

FR - Firing request

BR - B/L table update request

TG - Customer time slot go

UG - Uplink good

UB - Uplink bad

DG - Downlink good

DB - Downlink bad

DI - Data packet in

PB - Packet is bad

TC - Transmission completed

TE - Time slot expired.

Outputs:

INA - Initialize SCS acknowledgment

HA - Satellite health request acknowledgment

FA - Firing request acknowledgment

BA - B/L table update acknowledgment

TGF - Customer time slot go - forwarded

TSCAN - Customer time slot canceled

DO - Data packet out

PBF - Packet is bad - forwarded

TEF - Customer time slot expired - forwarded

TCF - Transmission completed - forwarded.

III. SCS Requirements

Contents:

1. Introduction

This section contains the requirements for the COMBIZ Satellite Control System. These requirements were derived from three sources:

(1) Bruce E. Krell. Developing with Ada: Life Cycle Methods. Bantam Books, New York, New York. 1992.

(2) William C. Cook. "The Wonderful World of Satellites (A Satellite Primer)." 1996. http://www.atek.com/satellite/

(3) "NASA TDRSS Home Page." 1996. http://www530.gsfs.nasa.gov/tdrss/

2. Satellite Control System Requirements

The SCS is responsible for accepting and processing requests and commands from the GCS and returning acknowledgment messages so that the GCS can (1) understand the status of the SCS's satellite assets, (2) ensure that those assets maintain their proper orbit, and (3) ensure that those assets are properly aligned for bulk data transmission.

2.1 Initialize SCS

Before the SCS can be used, it must be initialized by sending it an IN (initialize SCS) command message.

IN1) The SCS shall receive and execute an IN (initialize SCS) command message from the Ground Control System (GCS). When this message is received, the SCS will be initialized.

Note: This message will be sent either to periodically initialize the SCS or to respond to system errors.

IN2) The SCS shall prepare and send to the GCS, an INA (SCS initialized) acknowledgment message that the system has been initialized.

2.2 Manage Satellites

The SCS is responsible for accepting and processing requests and commands from the GCS and returning acknowledgment messages so that the GCS can (1) understand the status of the SCS's satellites, (2) ensure that the SCS satellites maintain their proper orbit, (3) ensure that an SCS satellite is properly aligned (or pointed) to support bulk data transmission, and (4) ensure that customer satellite data communication sites are registered with the SCS in the bandwidth/location table so that an uplink/downlink site-SCS connection can be made.

MG1) The SCS shall process each MG (maintenance time slot go) command message received from the GCS. Receipt of an MG command message by the SCS signals the start of a "Manage Satellites" transaction for a specified maintenance time slot.

MG1.1) An MG command message shall specify the planned maintenance time slot duration.

MG1.2) An MG command message may be received only immediately after an IN command message or after the completion of a "Transmit Data" transaction.

2.2.1 Report Satellite Health

Satellite health information is requested to aid in planning required satellite maintenance.

MG2) The SCS shall process each HR (satellite health request) command message received from the GCS.

MG2.1) An HR command message shall be the first message received after the initiation of each "Manage Satellites" transaction.

MG2.2) The SCS may receive a satellite health request message anytime during a "Manage Satellites" transaction. (Describes order during transaction.)

MG2.3) A satellite health request command message will only be accepted by the SCS during an active "Manage Satellites" transaction. (Describes condition under which an HR may be received.)

MG3) The SCS shall prepare and send an HA (satellite health acknowledgment) message to the GCS in response to an HR (satellite health request) command message.

2.2.2 Maintain Orbit and Direction

Firing commands are prepared to perform orbital corrections such as to re-orient and stabilize a satellite, or to point it to support data transmission.

MG4) The SCS shall process each FR (firing request) command message received from the GCS. Those commands are used to re-orient or stabilize an SCS satellite.

MG4.1) The SCS may receive and process an FR command message after an HR (satellite health request) has been received and processed. (Describes order during transaction.)

MG4.2) An FR command message will only be accepted by the SCS during an active "Manage Satellites" transaction. (Describes condition under which an FR may be received.)

MG5) The SCS shall prepare and send an FA (firing request) acknowledgment message to the GCS indicating the SCS's thruster status after executing an FR (firing request) command message.

Each FA acknowledgment message shall contain a status code.

A status code of 1 shall indicate that the firing command was successful. The acknowledgment message shall also contain fuel pressure data.

A status code of 2 shall indicate that the firing command was unsuccessful. The acknowledgment message shall also contain fuel pressure data. Receipt of a firing command acknowledgment message with a status code of 2 will require a system restart.

2.2.3 Maintain B/L Table

The broadcast/location table must be maintained to ensure that customer data transmission site records are kept up to date.

MG6) The SCS shall process each BR (bandwidth/location (B/L) table update request) command message received from the GCS.

MG6.1) If a BR command message is received and there is already an entry in the B/L table, the current entry will be replaced.

MG6.2) After the SCS is initialized, table entries are made for all active communication sites. If the system is restarted, all B/L table entries must be re-entered.

MG6.3) The SCS has the ability to store 9,999 B/L table entries. Only one sender (uplink) and receiver (downlink) site pair may be specified for service during a "Transmit Data" transaction.

MG6.4) The SCS may receive a BR command message after an HR (satellite health request) command message has been received and processed. (Describes order during transaction.)

MG6.5) The SCS will only accept A BR command message SCS during an active "Manage Satellites" transaction. (Describes condition under which a BR may be received.)

MG7) The SCS shall prepare and send a BA (B/L table updated) acknowledgment message to the GCS indicating the status of the table update.

Each acknowledgment message shall contain a status code.

A status code of 1 shall indicate that the B/L table update command was successful.

A status code of 2 shall indicate that the B/L table is full and that the system should be restarted.

2.3 Transmit Data

The SCS is responsible for forwarding communication data packets from uplink sites to downlink sites. That is enabled by the GCS's informing the SCS of a customer's time slot and providing the bandwidth and location of the uplink site and the downlink site. During a

customer time slot, an uplink site will transmit data to a downlink site via the SCS. The GCS will send a TG (Customer time slot go) command message to the SCS, to enable the SCS to (1) link an uplink site with a downlink site; (2) forward data packets uploaded from an uplink site to a downlink site; and (3) send and receive command and acknowledgment messages to and from the uplink and downlink sites.

The SCS can handle only one customer uplink/downlink session at a time. When that time slot is up, the SCS sets up another link for another customer's specified time slot.

The GCS will inform the SCS when a customer's time slot has expired if the customer uplink site has not completed its data packet transmission and will instruct the SCS to set up another customer's time slot and associated uplink/downlink site-SCS connection.

2.3.1 Establishing an Uplink/Downlink Site-SCS Connection

Once a maintenance time slot is ended, the SCS is ready to receive "Transmit Data" transaction command and acknowledgment messages from the GCS, the uplink site, and the downlink site.

TG1) A TG command message shall specify the (1) the uplink site ID, (2) the downlink site ID, and (3) the planned time slot duration.

TG2) The SCS shall receive a TG (customer data transmission time slot go) command message from the GCS. That signals the initiation of a "Transmit Data" transaction for a specified customer data transmission time slot.

The current "Manage Satellites" transaction shall be terminated when the SCS receives a TG command message.

TG3) The SCS shall look up the entries for the uplink and downlink sites in the B/L lookup table that are specified in the TG command message.

TG3.1) If uplink and downlink site entries are found in the B/L table, the SCS shall forward the TG command message to the uplink site and the downlink sites identified in the TG command message.

TG3.2) If an uplink and/or a downlink site entry is not found in the B/L table, the SCS shall prepare and return a TSCAN (time slot canceled) acknowledgment message to the GCS with (1) a status code of 2 if the uplink site entry is not found, (2) a status code of 3 if the downlink site entry is not found, or (3) a status code of 4 if neither site entry is found.

Report Site Readiness

UG1) The SCS shall receive a UG (uplink good) acknowledgment message if the uplink site is ready to send data.

UG2) A UG may only be received during a valid "Transmit Data" transaction.

DG1) The SCS shall receive a DG (downlink good) acknowledgment message if the downlink site is ready to receive data.

DG2) A DG may only be received during a valid "Transmit Data" transaction.

Connection Attempt Failed

UB1) The SCS shall receive a UB (uplink bad) acknowledgment message if the uplink site is not ready to receive data.

UB2) The SCS shall terminate a customer data communications time slot for rescheduling if it receives a UB from the uplink site. Upon receipt of a UB, the SCS shall prepare and send a TSCAN (time slot canceled) command message with a status code of "0" to the GCS.

UB3) A UB acknowledgment may be received only during a valid "Transmit Data" transaction.

DB1) The SCS shall receive a DB (downlink bad) acknowledgment message if the downlink site is not ready to receive data.

DB2) The SCS shall terminate a customer data communications time slot for rescheduling if it receives a DB from the downlink site. Upon receipt of a DB, the SCS shall prepare and send a TSCAN (time slot canceled) command message with a status code of "1" to the GCS.

DB3) A DB acknowledgment message may be received only during a valid "Transmit Data" transaction.

2.3.2 Uploading and Downloading Data Packets

Once an uplink/downlink site-SCS connection has been made between two customer satellite data communication sites, the uplink site may upload data packets to the SCS and the SCS may forward the uploaded packets to the downlink site. Without such a connection, packet uploading and downloading is not possible.

An uplink/downlink site-SCS connection has been established when:

(1) the SCS as received a TG (Customer time slot go) from the GCS;

(2) the SCS has forwarded the TG (Customer time slot go) messages to the uplink and downlink sites; and

(3) both the uplink and downlink sites have sent the SCS ready messages, i.e., the uplink site has sent the SCS an UG (uplink good) acknowledgment message and the downlink site has sent the SCS a DG (downlink good) acknowledgment message.

DI1) A DI (data packet) shall contain the following data:

(1) the uplink site ID, i.e., uplink_ID;

(2) the downlink site ID, i.e., downlink_ID;

(3) packet ID, i.e., packet_ID; and

(4) packet data.

DI2) The SCS shall receive each DI (data packet in) received from the uplink site if a connection was successfully established between the uplink and downlink sites and the SCS.

The following conditions describe a successful uplink/downlink site-SCS connection:

(1) the uplink and downlink sites both sent UG and DG acknowledgment messages, respectively, to the SCS;

(2) neither the uplink or downlink site has recently sent a UB or DB message; and

(3) the GCS has not sent a TE (time slot expired) message to the SCS to terminate the current customer data transmission time slot.

DI3) The SCS shall forward each DI (data packet in) received from the uplink site to the downlink site.

DI4) A DI may be received only during a valid "Transmit Data" transaction.

2.3.3 Handling Data Packet Errors

The downlink site shall prepare and send the SCS one PB (packet is bad) acknowledgment message for each DI (data packet) it is unable to read.

If the downlink site can read the data packet, no action is necessary.

PB1) A PB (packet is bad) acknowledgment message shall contain the following data:

      (1) the uplink site ID, i.e., uplink_ID;

      (2) the downlink site ID, i.e., downlink_ID; and

      (3) a packet ID, i.e., packet_ID.

PB2) For each bad packet forwarded to the downlink site, the SCS shall receive a PB (packet is bad) acknowledgment message.

PB3) Upon receipt of a PB acknowledgment message, the SCS shall forward it to the uplink site to request a packet replacement.

PB4) A PB message may be received only during a valid "Transmit Data" transaction.

PB5) The SCS shall keep track of each bad packet message uploaded and whether the packet was or was not replaced by the uplink site.

2.3.4 Completing a "Transmit Data" Transaction

After an *uplink/downlink site-SCS connection* has been established, after all planned data packets have been uploaded to the SCS and forwarded, and after all bad packets sent have been replaced, the uplink site may end the "Transmit Data" transaction by sending the SCS a TC (transmission completed) acknowledgment message.

TC1) After the uplink site has completed its data transmission, the SCS shall receive a TC (transmission completed) acknowledgment message from the uplink site.

TC2) Upon receipt of a TC command message, the SCS shall forward it to the GCS.

TC3) A TC command message may be received only during a valid "Transmit Data" transaction.

If each PB message uploaded to the SCS was not canceled by a replacement data packet, the SCS shall ignore the TC command message received from the uplink site because one or more bad packets must still be replaced.

2.3.5 Terminating a Current Customer Time Slot

The GCS may terminate the current "Transmit Data" transaction at any time, by sending the SCS a TE (customer time slot expired) command message. When the SCS receives the TE command message, it ends the current "Transmit Data" transaction.

TE1) The SCS shall receive a TE (time slot expired) command message from the GCS when a customer data transmission time slot has expired.

TE2) Upon receipt of a TE command message, the SCS shall forward it to the GCS.

TE3) A TE command message may be received only during a valid "Transmit Data" transaction.

3. Assumptions

1. All hardware interfaces are transparently handled beneath vendor-developed software interfaces.

2. The SCS will always be capable of being initialized or restarted. Upon successfully restarting, the system will return to the GCS an acknowledgment message with a status code of 1.

If a system restart is executed, the GCS will be responsible for communicating to all sender and receiver sites that the system was restarted. This is not considered a satellite control system function.

3. The clock is internal to the SCS.

4. The header information from a bad data packet will always be able to be read, even though the data portion of the data packet may not.

5. The downlink site will send the SCS only one PB (Packet is bad) acknowledgment message for each DI (data packet) it is unable to read. It is assumed the downlink site will never send two PB acknowledgment messages for the same DI (data packet). If such a case was possible, both PB acknowledgment messages received by the SCS would be forwarded to the uplink site, as each PB would have been preceded by a DI with an equivalent packet_ID.

4. SCS Stimuli and Response Summary

4.1 SCS Stimuli

Table 1 describes the SCS Stimuli and their sources.

Table 1: SCS Stimuli

Source	Stimulus	Description
GCS	IN	Initialize SCS
GCS	MG	Initiate "Manage Satellites" transaction, i.e., open maintenance time slot
GCS	HR	Send "Satellite Health Request"
GCS	FR	Send "Firing Request"
GCS	BR	Send "B/L Table Update Request"
GCS	TG	Initiate "Transmit Data" transaction, i.e., open customer data transmission time slot
UL Site	UG	Send "Uplink is ready"
UL Site	UB	Send "Uplink is not ready"
DL Site	DG	Send "Downlink is ready"
DL Site	DB	Send "Downlink is not ready"

UL Site	DI	Upload "Data Packet", i.e., "data packet in"
DL Site	PB	Upload "Bad Data Packet Received" message
GCS	TC	Upload "Transmission Completed" acknowledgment message
GCS	TE	Send "Transmit Data" transaction - time slot expired

4.2 SCS Responses

Table 2 describes the SCS Responses and their sources.

Table 2: SCS Responses

Sink	Response	Description
GCS	INA	SCS initialized acknowledgment
GCS	HA	Satellite health request acknowledgment
GCS	FA(1)	Firing request acknowledgment: OK=1
GCS	FA(2)	Firing request acknowledgment: ERR=2
GCS	BA(1)	B/L table update acknowledgment: OK=1
GCS	BA(2)	B/L table update acknowledgment: TBL FULL=2
UL & DL sites	TGF	Customer "time slot go" command forwarded
GCS	TSCAN(0)	Customer "time slot" canceled: UL DOES NOT RESPOND
GCS	TSCAN(1)	Customer "time slot" canceled: DL DOES NOT RESPOND
GCS	TSCAN(2)	Customer "time slot" canceled: UL NOT FND=2
GCS	TSCAN(3)	Customer "time slot" canceled: DL NOT FND=3
GCS	TSCAN(4)	Customer "time slot" canceled: UL/DL NOT FND=4
DL site	DO	Data packet out
UL site	PBF	"Bad packet received" message forwarded

GCS	TEF	Customer "time slot" expired acknowledged
GCS	TCF	"Transmission completed" acknowledgment forwarded

5. References

[Krell92] Krell, Bruce E. Developing with Ada: Life Cycle Methods. Bantam Books, New York, New York. 1992.