Lunar Surface System Avionics Study Final Report

Ted Bonk 2/18/2009
LSS Avionics Sparing Project Agenda

- Introductions (2 hours)
- Study Overview & Results
- Layered Electronics Architecture
  - Sensor/Effectors
  - Local Controllers
  - Supervisor Controller/Safety System
  - Data Buses
  - Functions
  - Software
  - Architecture Concepts
- Dynamic Commissioning
- Abnormal Situation Management

- Wireless Equipment
- Conclusion
- Q&A (15 min)
Avionics, Industrial Automation and Mining provide valuable concepts that are applicable to LSS Elements.

Avionics Concepts

Industrial Automation

Mining

Merge Concepts

LSS

Learnings
The objective of this study is to investigate innovative avionics architectures and sparing strategies that maximize commonality of avionics components while minimizing mass of spares. Critical to deployment of sustainable avionics architecture are reductions including indirect reductions via reductions in power, packaging, and maintenance spares.

NASA stated the following as Technical Challenges in the BAA:
- Severely mass constrained
- Initial deployment to eventually coexist with subsequent generation hardware
- Surface networks are highly sparse by must still be robust

Here are the re-stated design drivers:
- Minimize Power
- Minimize Weight
- Enhance Commonality (Common Spares) for Reuse/Salvage
- Address Maintenance of Equipment
- Maintain Composability & Extensibility

Fewer Spares & Unique Spares
Industrial Automation Building/Mining Concepts in a Standard Framework
Integrated ISHM
Multi Vehicle Equipment
6th Generation Avionics & Sensor Stds
Dynamic Commissioning
ASM
Industrial Controller & IO Design Concepts

- Control Firewall
- Power Bus Bar
- Redundant Digital and Analog I/O
- Integrated Power Subsystem
- IO Rail
- Hotswap Processors & IO Modules
- Fieldbus Interface Module (IO)
- Batteries & Charger
Lunar Control Platform Architecture (Quick Look)

- Enterprise Wide Application Server
- Casual User Secure Read Only Process Display Web Server Public Access
- Desktop Access For e-Server and PHD Headquarters & Centers

- Plant Asset Management LSS Control
- Plant Wide Data Warehouse VAB
- Remote Operations Mission Control
- Advanced Multivariable Control
- Video as a Process Sensor Launch Video

- Control Room Ethernet
- Plant Ethernet
- Redundant & Redundant Remote I/O
- Control Room Ethernet
- Fault Tolerant Ethernet
- Wireless Access LSS Wireless
- Field Operator Connectivity Rovers
- SIL 3 Safety System Robotic Safety Partition
- Redundant & Remote I/O

- Web-based Human Interface LSS Control Center
- Redundant Global Database & Historian Asset Management HAB File System
- Ergonomic Operator Furniture HAB Furniture

- Example Software Applications
  - Asset Manager
  - Video Manager
  - Boundary Management
  - Daily Instructions
  - Production Monitoring
  - Electronic Shift Log
  - Procedure Automation
  - Process Control & Monitoring

- 3RD Party Devices (OPC, Modbus, DH+, and many more!) Lunar Subsystems

- LSS Avionics Concept Study – Final Presentation (2/18/2009)
Top Recommendations/Future Studies

Recommendations

1. Establish Programmatic Approach for Lunar Lander & LSS Electronics Commonality *(Top Recommendation)*
2. Establish a layered LSS Electronics Control Architecture across the vehicles
3. Establish Data Standards to allow data sharing & interoperability
4. IO Equipment/Power Control Integration

Suggested Future Studies

1. Sensor Type, Form Factor & Bus Standardization
2. LSS Equipment Health & Maintenance Approaches
3. Reconfigurable, Reusable LSS Software Architectures
4. Human Interface Standardization
5. Certification Standards
6. Altair and LSS Joint Avionics Development
Recommendation 1 Expansion

- Programs that design equipment for application across multiple vehicles work when ground rules and direction are established at program onset
- Establish leader/follower with structured signoff to address programmatic issues
  - Structure procurement to allow/enforce commonality between programs across vehicles
  - Same requirements lead to different implementations without constant significant effort to bring implementations together
  - Procuring the same parts eliminates that effort

“things that are different are not the same”
LSS
Layered Electronic Architecture
Common Electronics
Across the LSS Vehicles
(First Try)
Architecture Overview Across the Vehicles

LSS Electronics Control Architecture Levels

Level 3
- Production Mgmt
- Maintenance Mgmt
- Resource Mgmt

Level 2
Vehicle Control
- Sequencing
- Directing
- Coordinating
- Health Status

Level 1
- High Rate Control
- Standard IO/Power Control
- Standard Sensor/Effectors

Standard Components
- Std Sensors/Effectors
- Data Concentrators
- Local Controllers
- Supervisor Controller/Safety System
- Data Buses/Data Communications
- Functions
- Software
- File System

Enabled by standard functionality at each level with communications enabled by data standards
Electronic Architecture Components & Layers

Lunar Control Electronics Architecture

Application Specific Processor/IO

Application Specific Processor/IO SWAP is allocated to Subsystem Allocation

GPP Configured as Level 2 Controller

Time Triggered Databus

Wired Connections Disconnected during Element Movement

Local Controller (RIU & RPCs)
Level 1 (No Software)

Data Concentrator

Sensor Effector

Sensor Effector

Sensor Effector

Sensor Power/Signal Bus B

Wireless Sensor/Effector

GPP Configured as Level 3 Controller

File System

Time Triggered Databus

GPP Configured As SCP
For Level 3 Safety

Level 3

Level 2

Level 1

GPP Configured As SCP
For Level 2 Safety

Wireless Power Interface

Local Controller (RIU & RPCs)
Level 1 (No Software)

Sensor Power/Signal Bus A

Wireless Sensor/Effector

GPP Configured As SCP
For Level 1 Safety

Data Concentrator

Sensor Effector

Sensor Effector

Sensor Effector

Sensor Power/Signal Bus A

Wireless Sensor/Effector
## Functions (Space & Industrial Automation Superset)

### Level 3 Functions
- Automation Control Functions
  - Production Mgmt
  - Daily Instructions
  - Procedure Automation
  - Production Monitoring
  - Boundary Management
  - Electronic Shift Log
  - Maintenance Mgmt
  - Procedure Automation
  - Resource Mgmt
  - Asset Manager
  - Alarm System Analysis & Awareness
  - Video Manager

LSS Functions
- Crew Health Monitoring and Medical Systems
- External Environment Monitoring and Protection
- Mission Planning and Operations
- Prognostics, Maintenance and Logistics Management

### Level 2 Functions
- Automation Control Functions
  - Vehicle Control
  - Sequencing
  - Directing
  - Coordinating
  - Health Status
  - Process Control & Monitoring

LSS Functions
- Command and Data Handling
- Communications & Tracking
- Crew Health Monitoring and Medical Systems
- Environmental Control and Life Support
- External Environment Monitoring and Protection
- Guidance Navigation and Control
- Remote and Autonomous Operation
- Surface Navigation
- Thermal Control
- Waste Management

### Level 1 Functions
- Characteristics
  - High Rate Closed Loop Control
  - Standard IO/Power Control
  - Standard Sensor/Effectors

LSS Functions
- Power
- Mobility
- Crew Interface
- Lighting (Part of ECLS)
## Recommendation 2 Impacts

<table>
<thead>
<tr>
<th>Area</th>
<th>Recommendations</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor/Effectors</td>
<td>Standardize Sensor/Effectors</td>
<td>Fewer Spares</td>
</tr>
<tr>
<td>Sensor/Effectors Buses</td>
<td>Use Sensor Buses</td>
<td>Less Wire Weight</td>
</tr>
<tr>
<td>Local Controller/Power Control</td>
<td>Non-Software Controller with 4-6 Card Types, power control &amp; some flexible IO</td>
<td>Less Weight, Fewer Spares, Addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Common Mode SW Faults &amp; Exposure Time</td>
</tr>
<tr>
<td>Supervisor Controller/Safety System</td>
<td>Create General Purpose Reconfigurable Processor for all vehicles</td>
<td>Less Weight, Fewer Spares, Lander Commonality</td>
</tr>
<tr>
<td>Databuses/Data Comm</td>
<td>Integrated Wired &amp; Wireless</td>
<td>Flexibility, Wire Weight</td>
</tr>
<tr>
<td>Functions</td>
<td>Review Mining &amp; Process Control Functions</td>
<td>Look for commonality between vehicles to reduce duplication</td>
</tr>
<tr>
<td>Software</td>
<td>Design Assurance Levels, Multiple SW Environments, Data Standards, Common Software</td>
<td>Reduced Cost, More Flexibility, Increased Safety</td>
</tr>
<tr>
<td>Architecture Capabilities</td>
<td>Implement basic and advanced architectural capabilities</td>
<td>Easier Upgrades, Maintenance, Safety</td>
</tr>
<tr>
<td>Program Structure</td>
<td>Implement Leader/Follower Program</td>
<td>Reuse of Lander Electronics</td>
</tr>
</tbody>
</table>
Sensor/Effectors & Sensor Buses

• Hundreds of sensors/effectors will be needed and maintenance drives the design

• Common Sensor/Effectors
  - Compact, Low Power
  - Easy Maintenance
  - Built-in RM
  - Employ self-packaging
  - Combined Signal & Power Communications
  - Wired & Wireless Versions
  - Common with Lunar Lander?

• Design them once and use on all vehicles and habitat

• Choose an Standard, Open combined Sensor/Effector Bus
  - Sensor Buses save wire weight
  - Address RM/Fault Isolation Aspects

• Altair study shows wiring can be 56% of Avionics weight

• Design them once and use on all vehicles and habitat
Embedded System Comparisons -- Input/Output

- **Vetronics (Airplanes, Spacecraft, Armored Personnel Carriers, etc.)**
  - I/O is built into the vehicle
    - I/O distribution is part of the vehicle design
    - Sensors and actuators are limited to save weight and power

- **Process Control and other Terrestrial Systems**
  - Architectures are hierarchical
    - Regulatory control levels use purpose-built controllers
      - Often redundant to provide availability in case of communications failures
      - May be located remotely to reduce latency in control loops
    - Supervisory and enterprise levels use commercial information technology equipment
      - Conventional IT assets and protocols with modifications for real-time performance and reliability
  - Applications are I/O intensive
    - Some process applications have > 20,000 sensors/actuators
      - Sensors and actuators may be distributed over several miles
    - I/O usually is wired directly to controllers (“home run” wiring)
    - Newer equipment uses multi-drop buses for economy and ease of commissioning
      - Based on standard protocols such as Foundation Fieldbus, Profibus, LONworks, some Modbus
  - I/O is commissioned in the field
    - Older equipment requires manual configuration
      - Device addresses, data ranges and register assignments are manually set during installation
    - Newer equipment provides automatic discovery to minimize field labor
      - Device characteristics are sent by the device on connection
      - Device addresses are dynamically assigned by controllers

- **Lunar Surface System**
  - I/O architecture uses vehicle assets to implement a terrestrial I/O architecture
Local Controllers (Data & Power Control Integ)

• Integration Level of Control & Power
  - Reduces Size, Weight, Power & LCC

• Local Controller (PDU Like)
  - 4-6 Circuit Card Types for Signal & Power
  - Hardware Based Controller due to Common Mode SW Faults & Exposure Time

• Design them once and use on all vehicles and habitat
Data Buses/Data Communications

- Integrated Wired & Wireless Communications
- Time Triggered Protocols
- Ethernet Compatible
- Space Qualified Wireless Parts
- Design them once and use on all vehicles and habitat
Supervisor Controller/Safety System

- General Purpose Computer
  - Reconfigurable Processor
  - Network Switch
  - Wireless Capability

- GPP as Level 2/3 Controller
- GPP as Safety System with different simpler software
- Design them once and use on all vehicles and habitat
Software

• Recommendation Software-1

Establish and use multiple assurance levels for software design, verification and qualification processes to support these levels. This is to reduce initial software cost as well as maintenance costs by only doing the effort as required by the safety analysis.

• Recommendation Software-2

Establish standard software architectures, supporting services and execution environment for all LSS elements supporting: Hard Real-time Environment, Software Real-time Environment and Windows-like or equivalent. This is to allow for software to be developed and hosted in an environment best suited for that application (GN&C in Hard Real-Time & Excel in Windows type OS).

• Recommendation Software-3

Establish common software repositories to eliminate replication of software pieces for multiple vehicles. This is to reduce cost and increase quality by exposing building blocks to wider use and implicit testing.

• Recommendation Software-4

Establish data standards for communications between software in the different sensors, effectors, computing unit (e.g. expansion of OPC - OLE for Process Control to include common vocabulary/taxonomy/ontology). This is to allow for remote data access to remote equipment and reduce IO software development costs.
Architecture Capabilities

• Basic Capabilities
  - Defined roles & responsibilities per layer with defined interfaces to enable upgrades
  - Interfaces that meet open standards to facilitate Third Party Hardware & Software Integration
  - Allow for vehicle unique functions/electronic but required justifications and allocate costs

• Advanced Capabilities
  - Hot Swap & Dynamic Upgrades
  - Integrated System Health Management (ISHM)
  - Reconfigurable Computing
  - Abnormal Situation Management
  - Dynamic Commissioning
Advanced Capability – System Commissioning

- Adapts a system to a specific field environment
  - Installs and configures components to field constraints
    - Installs sensors and actuators
    - Installs communications and power wiring
    - Sets computer parameters and drivers for field devices
    - Inventories devices and configures device addresses and parameters
    - Installs application software and tunes application parameters
  - Tests system operation

- Typically the last step before operational status
  - Always performed in the field
  - Verifies the system meets user needs
  - Must be repeated if major system changes or upgrades occur
LSS Shifts Commissioning Activities to the Field

Most critical activities occur during engineering

More activities (including commissioning) occur in the field so less occurs in engineering

Factory

Field

Vehicular System Life Cycle

Indicates commissioning activity

Indicates factory engineering activity

Indicates field activity

Application Definition

System Design

Product/Subsystem Installation

System Integration

System Test and Tuning

System Qualification / Acceptance

System Operation and Maintenance

System Retirement

Terrestrial System Life Cycle

Reconfiguration for new missions and upgrades increases dependence on field activities

Lunar Surface System Life Cycle

System Upgrade and Retrofit

Application Definition

System Design

Product/Subsystem Installation

System Integration

System Test and Tuning

System Qualification / Acceptance

System Operation and Maintenance

System Retirement

Application Definition

System Design

Product/Subsystem Installation

System Integration

System Test and Tuning

System Qualification / Acceptance

System Operation and Maintenance

System Retirement
Advanced Capability – Dynamic Commissioning

• Extends conventional system commissioning to support evolving field operations in a remote environment
  - Provides flexibility to adapt to changing conditions
    - Build-out of lunar habitations and communications
    - Mission evolution
  - Uses standard and reusable components to minimize field configuration effort
    - Standard computers for economy and interchangeability
    - Multi-purpose I/O architecture for flexibility
    - Standard sensors and actuators for simplicity and reuse
    - Prewired I/O to simplify hardware installation
    - Dynamic device discovery and configuration to minimize manual configuration of device addresses and parameters
    - Standard communications to minimize time spent in harsh environments
  - Supports commissioning with software
    - Unified database of process points to manage data aggregation and distribution
    - Automated discovery and provisioning software to eliminate manual data entry
    - Standardized software for data visualization and control
Abnormal Situation Management

• An abnormal situation is a disturbance or series of disturbances in a system with which the control system is unable to cope, and which requires operator intervention.

• Abnormal Situation Management, like general emergency management, is achieved through Prevention, Early Detection, and Mitigation of abnormal situations, thereby reducing unplanned losses that can include lost time, loss of equipment, or loss of life.

• The “Paradox of Automation” is that the very automation we design to manage complexity may reduce the operator’s awareness and limit opportunities to reinforce their knowledge. When the automated system is unable to handle a problem the operator may lack the situation awareness or skill required to for correct intervention.

“In systems where a high degree of hardware redundancy minimizes the consequences of single component failures, human errors may comprise over 90% of the system failure probability.”

Recipe for Disaster

Sub-System Silos

- Communications subsystem identifies loss of communication and initiates autonomous diagnosis and repair
- This temporarily disrupts communication to the returning crew, so they do not receive the distress signal, and do not know their shortest route is blocked
- The disabled crew member is put at high risk
Shared Situation Awareness

**Resource Optimization**

- **A**
  - The crewmember in EVA distress has highest priority

- **C**
  - The communications subsystem holds requests unrelated to mobile crews and related vehicles

- **B**
  - The returning crew is routed to the landing area where they can access oxygen reserves and assist the distressed crewmember

Returning Crew – Low O₂

Tri-Athlete (Lost Communication)
Benefits of ASM and Human-Centered Design

• In the environment of a lunar mission there is a staggering array of systems and personnel who are likely to be operating simultaneously to achieve potentially conflicting goals.

• ASM design principles address the human-in-the-loop in a comprehensive manner
  - appropriate context sharing and common understanding of the hierarchy of goals and threats
  - appropriate separation of concerns (environment, transport, research work product) with carefully arbitrated rules of priority
  - resource optimization through well arbitrated human and automation collaboration

In the design of the lunar base, the human is the most variable, unpredictable, and intractable component within the control network.
Wireless Sensors & Effectors

**Safety**
Eliminate Hazards
$20B losses per year in US Petrochem Industry

**Reliability**
Reduce Downtime
Millions lost per year due to unplanned production losses

**Efficiency**
Reduce Costs
Improve Productivity
Ease of Installation
Process optimization
Wireless Sensors in a Refinery (Find the LSS Parallels)

- Video Monitoring
- Pressure
- Safety Shower Monitoring
- Leak Detection
- Level
- Temperature
- Mobile Operator
- Mobile Communication
- Asset Tracking
- People Locator
- Video Monitoring
- Emission Monitoring
- Fire & Gas Detection
- Mobile Inspector
- Emission Monitoring
- Physical Security
- Terminal Automation
- Extended Control Network
- Mobile Operator

DOE Contract: Wireless and Sensing Solutions for Improved Industrial Efficiency
Honeywell Project: Wireless Networks for Secure Industrial Applications
Four Networks (3 Wireless, 1 Wired) Tied Together

Applications
- Wireless Server Tools
  (Security, DCT/NMT & OPC Server)
- DCS Client or other Client (OPC DA/AE, Modbus Serial, Modbus TCP)

Wireless Mesh Network
- XYR 6000 Wireless Devices
- ISA 100.11a Clients
- Wi-Fi Clients
  - Video Cameras
  - Mobile Station PKS

Applications
- Wi-Fi Clients
  - Wireless Gauge Reader
  - Collaboration Camera
  - IntelaTrac
  - WiFi Laptop

Applications
- Instant Location System
- Video Cameras
- Mobile Station PKS

Applications
- Mobile Station PKS
- WiFi Laptop
- IntelaTrac
- WiFi Gauge Reader
- Collaboration Camera

Applications
- Video Cameras
- Mobile Station PKS
- WiFi Gauge Reader
- Collaboration Camera

Applications
- Instant Location System
- Video Cameras
- Mobile Station PKS
- WiFi Gauge Reader
- Collaboration Camera
Wireless Equipment Specifications

MultiNodes/Mesh

• Capacity
  - 22 Multinodes Per Mesh
  - 100 Transmitters/Gateway
  - 2200 Transmitters/Mesh

• Classifications
  - Class I Div 2

• Power
  - 24VDC Power
  - 110 VAC Power Supply Available
  - Solar Power Options

• Range
  - Up to 3000 ft from Multinode
    • Further Distances with Directional Antennas

• Antennas – Standard Omni-Directional, Directional, High-Gain and Remote

• Operating temperature: - 40° to + 75°C

• Interfaces
  - Configurable Modbus TCP Server
  - HART Gateway

Sensors Transmitters

• Types
  - Pressure
  - Differential Pressure
  - Temperature
  - Corrosion
  - HLAI (High Level Analog Input)
  - Discrete Inputs

• Classifications
  - Class I Div I

• Battery Life
  - Up to 10 Years

• Range
  - Up to 2000 ft from Multinode

• Reporting Rate
  - 1, 5, 10 and 30 Second Reporting

• Antennas – Standard Omni-Directional, Directional, High-Gain and Remote

• Operating temperature: - 40° to + 75°C
Conclusions
Conclusions

• We expected to find a level of synergy and we were surprised by the amount and applicability.

• Industrial Automation, Building Control and Mining Industries have many applicable technologies/concepts for LSS
  - In some case, the technologies are further advanced than in Aerospace (Wireless Sensors & Sensor Buses)
  - Not everything is directly applicable due to size, weight & environment but these are workable

• Using the combination of knowledge, we answered the BAA questions, made recommendations and suggested studies/technologies, programmatic suggestions

The real strength came from combining concepts and capturing lessons learned from multiple industries --

No one has the market cornered on good ideas.
Questions
Backup
Technology Needs
Technology Roadmap

NASA TECHNOLOGY CHALLENGES
- Weight
- Commonality
- Integrated Maintenance
- Composability

Power
-Reusability
-Salvage
-Extensibility

Constellation Program Driving Needs
LSAM
- Cycle 2 BAA
- LDAC-3
- LDAC-4
LSS

Standards
- Data Standards
- Hardware Standards

Avionics
- Miniaturization
- Power Reduced Electronics

Power Distribution
- Radiation Environment Study
- Wireless Power Eval Study

RAD Hard Components
- Radiation Hard MEMS/Gyro Study
- Space Qualified Wireless Components

Packaging/Connectors
- High Density IO Connectors
- Common RU & RPC

IO & Power Control
- Reconfiguration

Integ Technologies
- Cert Process

Test Laboratories
- Lunar Dust Laboratory

Legend:
- Milestone
- Decision

Study Type:
- BAA
- Other
- Parts
- Customer
- Capital
- Program

Avionics Equipment
- Processing Elements & Networks
- Integrated IO/Power Control
- Dust Proof Connectors
- Nav. Components

POTENTIAL APPLICATIONS
- Lunar Habitat
- Chariot Crew Mobility Chassis
- Pressurized Rover
- Power and Support Unit
- Heavy-Lift Mobility

Figure 3.1 Assumed functional hierarchical computer control structure for an industrial plant (continuous process such as petrochemicals).

## Purdue Model Responsibility

**Figure 3-4 Factory automation model.**

<table>
<thead>
<tr>
<th>IPW LEVEL NOTATION</th>
<th>WG1 LEVEL</th>
<th>HIERARCHY</th>
<th>CONTROL</th>
<th>RESPONSIBILITY</th>
<th>BASIC FUNCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NULL</td>
<td>6</td>
<td>ENTERPRISE</td>
<td>CORPORATE MANAGEMENT</td>
<td>Achieving the mission of the enterprise and managing the corporate</td>
<td>CORPORATE MANAGEMENT</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>FACILITY/PLANT</td>
<td>PLANNING PRODUCTION</td>
<td>Implementation of the enterprise functions, and planning and scheduling the production</td>
<td>PRODUCT DESIGN &amp; PRODUCTION ENGINEERING</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>SECTION/AREA</td>
<td>ALLOCATING AND SUPERVISING MATERIALS &amp; RESOURCES</td>
<td>Coordinate the production and supporting the jobs and obtaining and allocating resources to the jobs</td>
<td>PRODUCTION MANAGEMENT (Lower Level)</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>CELL</td>
<td>COORDINATE MULTIPLE MACHINES AND OPERATIONS</td>
<td>Sequencing and supervising the jobs at the shop floor, and supervising various supporting services</td>
<td>SHOP FLOOR PRODUCTION (Cell Level)</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>STATION</td>
<td>COMMAND MACHINE SEQUENCES AND MOTION</td>
<td>Directing and coordinating the activity of the shop floor equipments</td>
<td>SHOP FLOOR PRODUCTION (Station Level)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>EQUIPMENT</td>
<td>ACTIVATE SEQUENCES AND MOTION</td>
<td>Realization of commands to the shop floor equipments</td>
<td>SHOP FLOOR PRODUCTION (Equipment Level)</td>
</tr>
</tbody>
</table>

NOT INCLUDED BECAUSE OF WIDE DIFFERENCES OF EQUIPMENT AND FUNCTIONS BETWEEN DIFFERENT INDUSTRIES.
