NOAA GOES Data Collection System - Standards and Certification Workshop

Spring Technical Working Group 2023

William A. “Skip” Dronen Jr.
NOAA GOES DCS Program Manager

National Environmental Satellite, Data, and Information Service

April 2024

DCP Commanding

- Current Concept
  - DCP Command is selected, cued, and executed from the DADDS user interface (see current specification for draft list of commands)
  - Commands are cued to be sent to DCPs configured to “listen” at specific times
    - Scheduled DCPs could “listen” briefly after a scheduled transmission
    - Random-only DCPs could be programmed to “listen” using a logic intended
  - Command acknowledgment sent via the current DCPR Random Channel method
- What Problem is this Solving?
  - Remote access to DCPs is a logistical challenge for many users making dynamic changes essentially impossible/impractical.
  - Current system inhibits responses to RFI and reassignments to maximize UHF CS2 spectrum.
  - DCPC offers potential for users to perform remote commands for DCP management (firmware queries, device reset, sensor reset, etc.)
  - DCPC offers manufacturers and option for improved remote management.

DCP Commanding

- How it will work
  - GOES DCS completes current effort to update DADDS and produce a communication specification
    - Additional features to be discussed/considered/proved
  - Complementary DCP Prototyping effort produces a reference design for industry
    - Likely the need for NOAA or users to collaborate on testing to confirm capability.
  - New DCPC capable DCPs are submitted for DCS certification and deployed
- **Demonstration**

DCP Commanding

- Security
  - Security in overall system design vs. a specific feature (scrambling/encryption)
  - GOES is an open system. GeoXO will be an open system. DCPR is already susceptible to intentional disruption.
    - Data integrity (not security) is a function of making the system more robust and mitigating unintentionally disruption.
    - The only data subject to protection is PII stored in DADDS, which is protected by compliance with IT Security measures required by the US Department of Homeland Security.
  - Underlying assumption is the DCPC disruption would be accidental.

DCP Commanding

- Security (cont'd)
  - System operation may inherently provide integrity simply by its design, making accidental "commanding" a low possibility
    - A second DCPC ID would be protected within DADDS. The user would protect the ID as their organization required.
    - DCPs would only "listen" per the programming selected (user or NOAA TBD)
    - DCP Commands are sent via Frequency Hopping Spread Spectrum. The hopping pattern may be public but the odds of an accidental FHSS signal matching the ID in the DCPC protocol are assumed to be incredibly low.
  - Use of encryption (key management) may be overwhelming.
  - Use of additional scrambling is a possibility that has not been explored.

DCP Commanding

- Timeline

Questions, Contacts, and References

Questions?

- Program Manager - William “Skip” Dronen William.dronen@noaa.gov
- Customer Account Manager – Letecia Reeves letecia.reeves@noaa.gov
- DCS Help Desk **(757) 824-7450**

- Program Website
  - https://www.noaasis.noaa.gov/GOES/GOES_DCS/goes_dcs.html
- DADDS
  - https://dcs1.noaa.gov/
- System Diagram
  - https://dcs1.noaa.gov/documents/NOAA%20DCS%20Mar%202020.pdf
- Certified manufacturers
  - https://dcs1.noaa.gov/documents/GOES%20DCS%20Certified%20Venders.pdf