Nuclear measurement solutions for safety and security.


DCM-C5 Camera


NAS Reader

NGSS

Evolutionary Safeguards Surveillance

CANBERRA

NGSS

The NGSS is a modular, fully scalable surveillance system that records and makes easily accessible authenticated and encrypted surveillance data only to safeguards authorized personnel while minimizing the possibility of a loss of surveillance.

Fully adapted to the challenging safeguards environment, the NGSS consists of the complete surveillance infrastructure needed to make use of image and state-of-health data for the drawing of safeguards relevant conclusions. Visual evidence of events is recorded and processed in a front-end camera and stored locally or forwarded to a Data Consolidator (DC) unit where data is stored locally and/or forwarded via a remote monitoring connection. At the back-end, review software allows for the analysis of image files with automatic processing and tools for inspector safeguards relevant review. The whole system was designed for ease of use and maintenance with a modular infrastructure that allows for simpler inventory management, uncomplicated (plug-and-play) exchanges of units in the field, and easier upgrade as new technologies become available.

At its most basic level NGSS consists of a single camera taking, authenticating, and storing surveillance data. In extended systems, multiple cameras are connected to data consolidation servers that receive, store, and in remote monitoring applications forward data.

The design of NGSS balances requirements for robust equipment in a wide range of environmental conditions and security considerations in potentially hostile installations with the need for easy to use and cost-effective solutions. In order to meet these challenges, NGSS has been designed with the following features:

- Integration of all security critical components into one tamper indicating assembly and advanced data security adhering to Agency-defined practices for encryption and authentication;
- A short Picture Taking Interval (PTI) and support for high resolution and color images;
- Secure Ethernet communications backbone;
- Backwards compatibility with existing surveillance equipment and designed to be easily implemented as Joint-Use-Equipment (JUE) for multiple safeguards users;
- Modular, scalable system components to simplify installation, configuration, maintenance and logistics;
- Long term sustainability using components and software systems that provide continued availability;
- Components optimized for low power consumption and high reliability under harsh environmental conditions (including radiation) to insure continued surveillance without need for frequent technical service or maintenance intervals.

> ***NGSS consists of cameras and servers taking, authenticating, and storing surveillance data.***

CANBERRA

FUNCTIONAL OVERVIEW

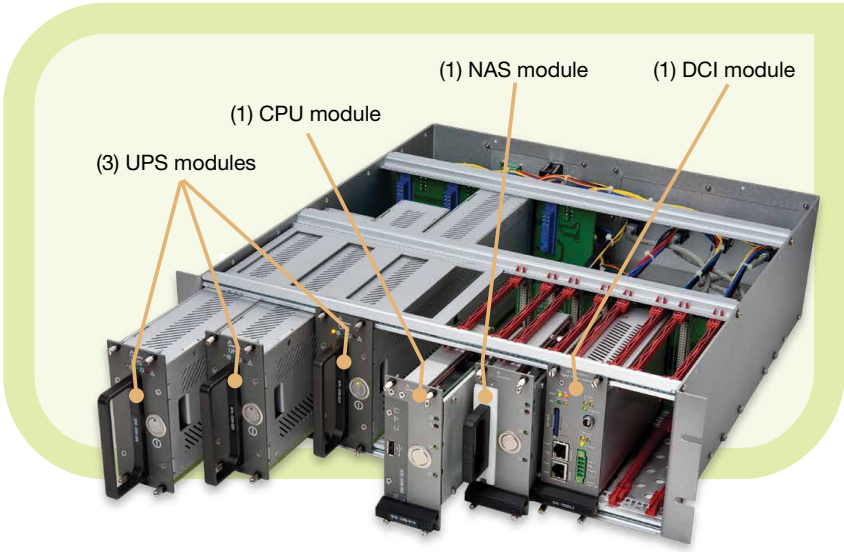
The NGSS follows a modular and scalable approach.

The system consists of **DCM-C5 Camera** modules (scalable from 1 to 32 cameras) connected to a **Data Consolidator (DC)**. Each individual camera module corresponds with a **Digital Camera Interface (DCI)** located on the DC that is responsible only for this one camera. The DCI polls data from the camera, sends it over the DC Ethernet network to a removable **Network Addressable Storage (NAS)** unit, and provides power to that camera. A **Central Processing Unit (CPU)** module monitors all network traffic, handles system cross-triggering signals, and supervises remote data transmission via a VPN box or other modem.

Each module has its own **Uninterruptible Power Supply (UPS)** that is only responsible for the module it is assigned to. The NGSS **Graphical User Interface (GUI)** allows interfacing, set-up and maintenance. The NAS drives can be removed from the NGSS DC and installed in an external **NAS Reader** appliance for mounting the drive on a host computer for data transfer and local storage or direct review. Through remote communication or through physical swapping of media, safeguards files can be uploaded and then reviewed on a Review Station equipped with the **General Advanced Review Software (GARS)**. This system infrastructure prevents single point of failures; if a system module fails, all other channels in the system continue operation as normal.

HARDWARE OVERVIEW

DATA CONSOLIDATOR CHASSIS



Preventing loss of surveillance has been a chief concern for the design of NGSS. To that effect the NGSS records data in three places: on an SD-Card located in the camera, on an SD-Card located in the DCI, and on the NAS. Ideally, safeguards inspectors only remove the NAS during scheduled inspections and replace it with an empty media, but in case data stored on the NAS are corrupted, data can be recovered by removing the appropriate SD-Card either from the DCI or the camera.

Figure 1 below, provides a functional overview of the NGSS architecture.

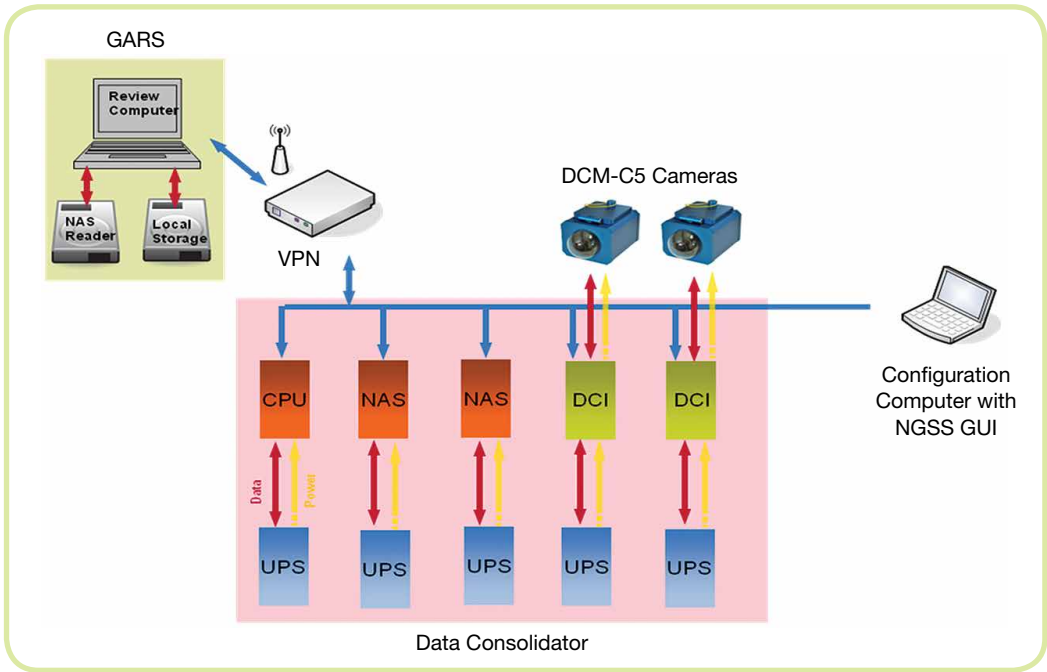


Figure 1: NGSS Functional Overview.

The system depicted in Figure 1 consists of two cameras and two NAS. The blue lines depict Ethernet connections between units, red lines are data channels and yellow lines indicate power connections. Note that the system also includes a PC for system configuration and a Virtual Private Network (VPN) connection for remote data collection. All Ethernet paths utilize the TCP/IP protocol with Transport Layer Security (TLS). The light red shaded areas depict equipment installation in an unsecure facility. The light green shaded area depicts the secure facility required for review of surveillance data.

The new **DCM-C5 camera** has been developed to support NGSS requirements. The DCM-C5 camera packages image data with corresponding State-of-Health (SoH) information then authenticates and encrypts the data package and sends it to the Data Consolidator. Camera images are secured with RSA 1024 encryption and DSA2K authentication. The DCM-C5 camera has been designed to allow independent, stand-alone operation. MPEG video data is authenticated then encrypted before being stored on DCM-C5 SD media.

Video authentication is achieved through digital signing of the data which consists of image content and date and time. The algorithm used is the Digital Signing Algorithm (DSA). Key pairs (public and private) are generated in the DCM-C5 with a selectable key length of up to 2048 bits. All video channels are signed with the DCM-C5's own key, which can be unique to every DCM-C5. The signatures can be verified by everyone knowing the public key of the DCM-C5. The NGSS system is backwards compatible to also allow for connectivity with DCM-14 cameras.

DCM-C5 Camera

> ***The NGSS follows a modular and scalable approach.***

The **Data Consolidator (DC)** facilitates system configuration, monitors network status, and supervises long-term data storage and remote data transmission. The DC consists of one CPU, one or more Network Attached Storage (NAS) devices, a Digital Camera Interface (DCI) module for each camera, at least one Ethernet switch and an Uninterruptable Power Supply (UPS) for each module. The CPU, NAS units and DCIs are networked together via the Ethernet switch. The DC includes a Graphical User Interface (GUI) for configuration and maintenance. Access to this web browser requires a valid crypto-token. In extended systems, multiple cameras are connected to data consolidator (DC) servers that receive, store and, in remote monitoring applications, forward data. The DC provides primary camera power via the communication and power cable that runs from the DCI to the camera, supplied by the UPS and powered by AC mains. The DC also provides short-term backup power via the UPS batteries for the cameras in case of loss of AC mains. The camera contains its own long-term battery backup for extended power outages.

The NGSS web-based **Graphical User Interface (GUI)** is designed to support system configuration, monitoring and maintenance. The web site is designed to run with a touch-screen interface and provides an on-screen virtual keyboard where user input is required. The GUI utilizes a common template to ensure the user is given a consistent environment in which to do required work and navigational elements allow quick and intuitive workflows between tasks. Time information is displayed as the system time of the DC. Communications between the NGSS GUI and the NGSS DCM-C5 cameras are protected with an IAEA approved TLS Proxy Server that is running on the PC along with the web browser. Use of the proxy allows the GUI to be browser-independent.

Figure 2: GUI Camera Parameters Page.

Data Review Software for a Windows® XP host with **General Advanced Review Software (GARS)**. GARS functions have been enhanced and extended to support review of NGSS files. Data can be transferred to local storage in a secure facility using an optional VPN connection. Alternatively, the surveillance data can be removed from the NGSS and mounted in the secure facility via a media reader such as the NAS reader that supports mounting of NAS modules on a host PC. Surveillance data can only be reviewed by use of the appropriate encryption certificates issued for the particular data set or camera. GARS is the interface for Safeguards data review for the NGSS system. GARS has been designed to facilitate efficient review of digital images in a secure environment from a variety of IAEA supported surveillance systems. Primary functions include the creation of review files and reports, decompression of surveillance images, motion detection analysis, image authentication and configuration of surveillance preferences.

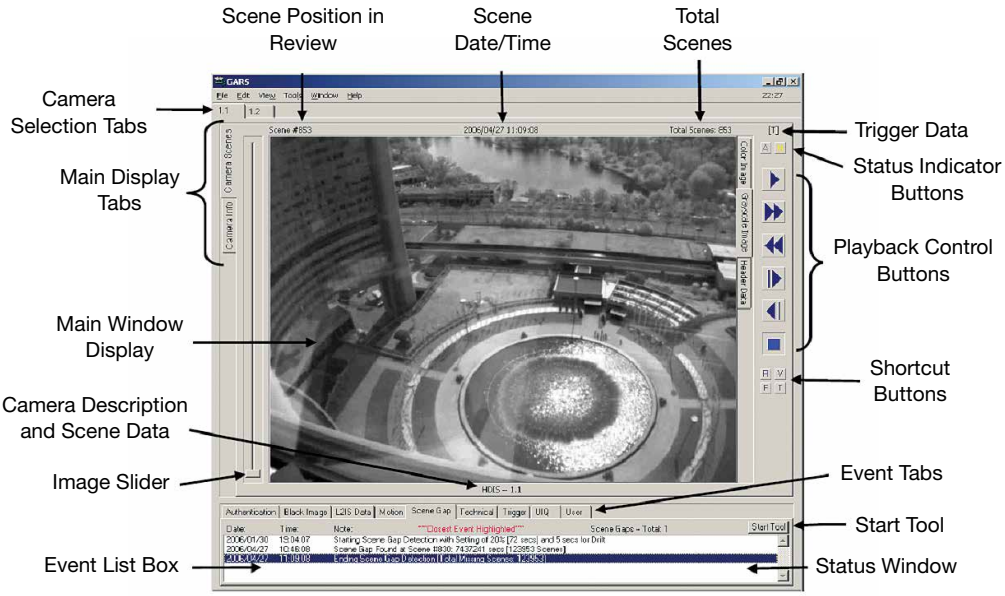


Figure 3: GARS Main Window Functions.

MODES OF OPERATIONS

Standalone Camera Operation

- The DCM-C5 camera has been designed to allow independent, stand-alone operation. In stand-alone mode, safeguards data can be retrieved from the camera's SD card.

Unattended Operation

- The NGSS is designed to operate in an unattended mode while ensuring integrity of safeguards data. Each NGSS module (DC, DCI, CPU, NAS, Ethernet switch) and each camera has a battery backed-up power source and safeguards data is stored redundantly on multiple media.

Local and Remote Data Transfer

- In facilities where a Virtual Private Network (VPN) is installed, operators can upload NGSS data from the NAS to local storage in a secure facility for data review.
- Alternatively, the storage media (NAS and SD cards) are designed to be transportable to a secure facility for data review.

CANBERRA

ISO 9001
SYSTEM
CERTIFIED

Measurement Solutions for Nuclear Safety and Security

For more information please visit: **www.canberra.com** C38714 - 02/2017