Authentication and data quality monitoring with Safeguards HPGe detector systems

Twomey, T. R., Bingham, R. D., Keyser, R. M.
ORTEC, PerkinElmer Instruments, Inc
801 South Illinois Avenue
Oak Ridge, TN 37831

Abstract

Authentication of the spectrum from a detector is important in remote monitoring applications, Safeguards monitoring and other critical measurement situations. Data quality is also important and the data quality monitoring here refers to the physical and electrical parameters of the detector, such as detector temperature, consistency of the high voltage, consistency of the low voltage preamplifier power, and preamplifier overload condition. All of these parameters can adversely affect the spectrum, both in peak areas and resolution. A detector system has been developed to provide both of these capabilities. The detector is controlled and monitored from the special features of the spectrometer. The authentication is accomplished with two codes. The first code is the serial number of the detector and the second code is a pseudo-random value stored in the detector at the beginning of data collection and verified at the end of data collection. The high voltage supply is integral to the detector. The value of the high voltage applied to the detector can be read by the spectrometer. The detector module also detects any change in the voltage and records an error if the change exceeds limits. The detector temperature is monitored and can be read by the spectrometer. If the temperature exceeds a set level, an error is recorded. The supply voltages are monitored at the detector. The detector module detects any change in the voltages and records an error if any change exceeds limits. By using the detector and spectrometer combination, the spectrum produced is known to have come from the specified detector and that all operating parameters were stable and valid during the data collection time.

Introduction

The quality, quality assurance and authentication of the recorded gamma-ray spectrum is becoming increasingly important as nuclear spectroscopy is being used as a tool for investigation or monitoring of processes rather than as a tool for nuclear research studies. The spectra collected in the former cases often can not be repeated (one-time events) and the results of the analysis of the spectrum can have significant consequences. To ensure the spectra collected are of the highest possible quality and reliability the data acquisition system should provide for monitoring of those instrument parameters critical to data quality. This monitoring function may also be used to detect indicators of impending failure so that they can be corrected before a complete failure has occurred.

The quality assurance of the spectra is also important so that the analysis of the results can be justified or defended, if necessary, or explanations for abnormal results made. To accomplish this,

the parameters and values monitored during the data collection should be stored with the spectrum in an easily retrievable manner.

In Safeguards and treaty verification such as the CTBT, an additional aspect is present. There is the possibility that an organization might attempt to substitute a spectrum for the one actually acquired by the detector, or acquire the spectrum on an "imposter" detector, malevolently substituted to mislead the monitoring agency into thinking material was still present after it had been diverted, or that no activity was present when in fact activity was present.

To assure that the spectrum data stored in memory did, indeed, originate from the intended detector, it is necessary to monitor the connection between the detector and the collection/control device. This can be done by both the exchange of bit-codes before and after the data collection and by the monitoring of the detector hardware conditions. Any failure of these tests can be recorded with the spectrum. In addition, some tamper-evident hardware devices should be installed to ensure physical integrity.

To accomplish these objectives, the system shown in Figure 1 was developed. The major components are: the digiDART, the HPGe detector with SMART-1 interface and the software.

DigiDART MCA

The digiDART digital portable MCA is described fully and its spectroscopic performance demonstrated in a previous paper[1]. It is the first digital, portable MCA with on-board spectrum display and data storage. It has integrated into it the necessary functionality to "serve" and support an "Intelligent" HPGe detector in order to implement the functions described in the Introduction above. The Intelligent HPGe detector developed by ORTEC is marketed under the name SMART-1.

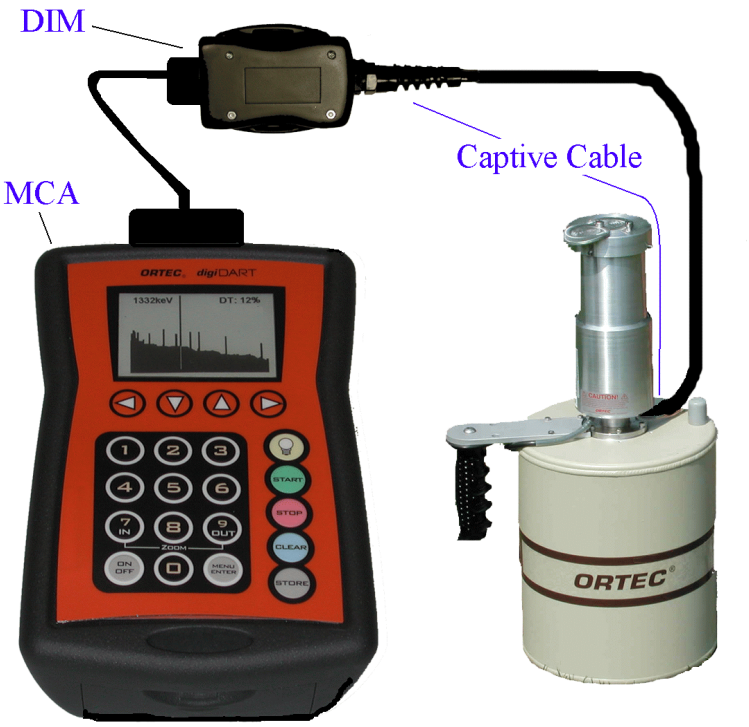

Figure 1 The digiDART and SMART-1 HPGe system

SMART-1 HPGe Detector

A SMART-1 detector incorporates a controller module which monitors the detector signals, the controller signals and voltage levels and responds to commands from the digiDART. It is "hard-wired" or permanently connected to the detector preamplifier. There is a single cable between the Detector pre-amplifier housing and the controller module, both of which may be fitted with anti-

tamper seals if required. This provides physical integrity between the detector itself and the electronics which monitor it. The SMART-1 HPGe detector controller module provides the following functions:

High voltage for the detector
High voltage to be actually set on detector
High voltage on/off control
High voltage shutdown control
High voltage monitoring
Recommended high voltage for this detector
Detector temperature monitor
Preamplifier overload state
Low voltage monitoring for ± 24 V and ± 12 V
Detector serial number
Storage of start/stop code number

The high voltage for the detector is generated in the controller module. This ensures there are no connectors between the detector and the high voltage supply. Both the controller module and the detector pre-amplifier housing may be moisture- and security-sealed. This has the added advantage that no high voltage cables are run for long distances. There are no exposed connectors carrying high voltage. A bias shutdown interlock automatically removes the high voltage if the detector temperature increases above the safe limit. The high voltage can be enabled and disabled in the controller module by command from the connected MCA, such as the digiDART. The recommended value of the voltage is read from the controller module by the MCA. The MCA sets the high voltage value to be used – normally to the recommended value, but it can be a different value. The value of the high voltage supplied to the detector is constantly monitored via the controller module. If the value varies by more than 200 V from the specified value, the high voltage error status is set to true. The status remains true until reset by the MCA even if the high voltage returns to normal. This approach of "latching" the parameters helps with both aspects of quality assurance, data quality and tamper proofing.

The IEEE recommended low-voltage preamplifier power is supplied by the controller. The voltages are constantly monitored individually. If the value of any voltage varies by more than 2 V from the specified value, the corresponding low-voltage error status is set to true. The status remains in error until reset by the controller even if the voltages return to normal. If the controller module is unplugged, all of the voltages will be set to error status. The status is retained in the controller module and can be read when power is reapplied.

The detector temperature is determined using the thermal element near the detector crystal. The output of the thermal element controls the high voltage shutdown and can be displayed by the controller in degrees Kelvin.

The preamplifier overload signal indicates when the preamplifier has gone into overload. This is an indication that the countrate is very high or the detector is warming up. This is the signal that drives the LED on the endcap of most detectors. If the preamplifier goes into overload for longer than a

set time, any time during the data collection, the error status is set to true. The status remains in error until reset by the controller even if the preamplifier recovers from the overload condition.

The detector serial number is stored in the module when the detector is made at the factory. The serial number can be read at any time by the controller. The serial number is unique to the detector, and is read only.

The controller module can accept a numeric code from the MCA at the start of an acquisition, retain it, and return it to the controller at the end of the measurement.

Control by the digiDART portable MCA

The digiDART provides the following for the detector controller module.

High voltage set value
High voltage on/off control
Start/stop numeric code
Serial number monitor
Status monitor and display

The digiDART can display the following, or provide to the controlling software running on an attached computer.

Amplifier settings (gain, pole zero, risetime, flattop, signal input polarity, preamplifier type)
ADC settings (conversion gain, LLD, ULD, gate)
Presets
Stabilizer settings
Firmware revision level
Serial number
Status of the state of health of the SMART module.
Detector temperature

These parameters can also be provided to a remote computer over a physical or wireless network via the ORTEC "CONNECTIONS" network environment[2].

The high voltage set value is set on the MCA input screens or computer dialogs by the user and then set into the module by the digiDART. This is the normal working voltage of the detector and should be the recommended bias value returned from the module. The high voltage is not turned on until enabled by the controller (and the shutdown is not active).

At the start of every spectrum acquisition, the MCA generates a pseudo-random number and sends this number to the controller module. Both the MCA and the controller module retain this number. When the acquisition stops, either from a preset condition being met, or by the user, the MCA reads the number from the controller module. The internally-stored number and the re-read number are

compared. If the two values do not agree, the security error status is set to true in the MCA. The status is stored with the spectrum. It remains true until the next clear operation in the MCA. If the computer is not connected, the security error status is displayed on the MCA screen. Otherwise the status is viewed on the computer or across the network.

The status of all the functions monitored by the controller module is read by the MCA and displayed on the integral display. It is also stored with the spectrum when the spectrum is stored internally.

The MCA internal settings are set by the operator and will be unique to the operation of a specific detector in a specific data acquisition. For example, the amplifier gain, pole zero, flattop and other settings will be different for each detector and spectrum type. These values are saved with the spectrum when it is saved internally or read by the software.

The MCA firmware level and serial number (different from the detector serial number) can also be read by the software.

The MCA Control Software ("MCA Emulator")

The desired result of the data collection is to have an authentic spectrum of data which are quality-assured. To accomplish this the MCA control software has access to all of the above status values, spectrum data, MCA settings and serial numbers.

The spectrum file structure use in MAESTRO and other ORTEC CONNECTIONS software is an open expandable format which currently contains all the values discussed above. This enables the user of the spectrum to verify the data collection settings and the status of the MCA and SMART-1 detector during the acquisition. The structure of the file is given in the ORTEC file manual.

An example of part of the file is shown in Figure 2.

4.11.12. Hardware Parameters Records

Record 1

Word Number	Type	Use
1–4		Validity flag, each bit corresponds to a single entry. 1 = valid contents, 0 = unused for this record. Bits are counted from the right, starting with 1. The bit number corresponds to the word number; i.e., if preset real time (word 5) is valid, then bit 5 and 6 are 1.
5	R*4	Preset real time in seconds
7	R*4	Preset live time in seconds
9	I*4	Preset counts
•		
•		
•		
23	I*2	Amplifier coarse gain
24	R*4	Amplifier fine gain as the value of the multiplier seen on the MAESTRO display
26	R*4	Amplifier fine offset in fractional channels
28	I*2	Gain stabilizer adjustment amplifier gain setting as the value from the MCB
29	R*4	Start channel for gain stabilizer region
31	R*4	Stop channel for gain stabilizer region
33		Gain stabilizer mode; 0 = Gauss, 1 = peak
34		Gain stabilizer on/off; 1 = on, 0 = off
35	I*2	Zero stabilizer adjustment setting as the value from the MCB
36	R*4	Start channel for zero-stabilizer region
38	R*4	Stop channel For zero-stabilizer region
40		Zero stabilizer on/off; 1 = on, 0 = off
41	R*4	Shaping time constant in microseconds (as reported)
43	I*2	Preamplifier type; 0 = resister, 1 = TRP
44	I*2	PZ valid; 0 = no, 1 = yes

Conclusion

A scheme for the quality assurance and authentication of the raw data gathered by a Gamma-Ray spectrometer has been implemented and presented. The system includes monitoring of sensitive functions, serial number recording, device monitoring by exchange of random codes, and complete storage of all data with the spectrum. Although initially implemented for a portable assay system, this scheme could be extended to other configurations.

References

1.Bingham, R. D., Keyser, R. M., Twomey, T. R., Performance of a portable, Digital-Signal-Processing MCA with Safeguards Germanium Detectors

2. R.M Keyser and T.R Twomey Networks and *Connections* in the Counting Room, ESARDA 21st Annual Meeting Sevilla, Spain 1999.