V. Ensuring the validity of data used for verification

If States are to have confidence that declared stockpiles have been destroyed, they must have confidence that the data used for verification are valid. To ensure validity of the data, inspectors at CAMDS would have to be able to inspect the facility before it began destruction operations and to participate in all calibration of thermocouples, load cells, flowmeters, gas chromatographs, and any other sensors, as well as observe closely their installation and daily operation. (Recalibration of instruments and reinspection of the process equipment would be required whenever the process is shut down for an appreciable time.) Furthermore, safeguards must be incorporated in the sensor systems to protect against efforts to tamper either with the sensors themselves or the data transmitted from them.

A. Equipment security

The security of the monitoring equipment itself would be ensured by a tamper-detecting design of each item. In effect, certain key components, such as signal-generating circuitry, would be enclosed in a box which protects the sensor against mechanical or electronic interference. Attempts to remove the box would disturb microswitches which would set off alarms to alert inspectors; if an attempt were made to cut off a segment of the protective containers without interfering with the microswitches, the tampering would be detected during the visual inspection of the equipment. Tampering with the microswitches would also cause the erasure of information used to "authenticate" the data. ("Authentication" is discussed below.)

Tampering with the sensors might also be attempted through electromagnetic radiation. Protection against this would be accomplished by placing proper shielding inside the tamper-detecting enclosure.

For each sensor, the status of the protective container, as well as the operating status of the equipment, would be monitored electronically by inspectors from the CAMDS control room.

B. Data security

The volume of data generated from the various sensors and transmitted to the inspectors' monitoring station in the CAMDS control room would be small. Measurements would be made infrequently (for example, only once every few minutes). Therefore, a relatively simple data transmission system would be adequate. Either radio frequency or cable transmission links could be used.

To assure the integrity of the data during transmission, the data would be converted from analogue to digital form whenever necessary and an "authentication" scheme would be adopted. Data would not be encrypted, but a unique identifier would be added to each group of data points transmitted. This identifying "tag" would be generated by the monitoring system. Any attempt to alter the data during transmission would be detected at the central monitoring station since it would cause a mismatch between the expected and received "tag". (Although encryption is not necessary in this case, it is a valuable method of ensuring integrity of data which may be useful under circumstances other than those described here.)

The availability of low-cost microprocessors means that such data authentication procedures can generally be carried out without substantially increasing the cost of the monitoring system. Inside the tamper-indicating enclosure of each sensor, a microprocessor would control the data collection function of the sensor, the authentication procedure, and the communications between each sensor and the central monitoring station.