However, in the case of television cameras, the amount of data generated is very large compared to that produced by other sensors. The cost of authenticating television images would be substantial. A less expensive solution to ensuring data integrity would be to enclose the television camera in a tamper-detecting box. This would ensure that the camera itself and its field of view are not tampered with. Proper shielding of the coaxial cable between the camera enclosure and the video recorder in the central monitoring station, along with a simple sensing circuit to detect attempts to cut into the cable, would be sufficient to detect any effort to interfere with data transmission.

Security of the central monitoring station would be achieved by enclosing data read-out and recording devices in tamper-indicating containers when inspectors are not physically present.

C. Other data security considerations

The integrity of data from sensors cannot always be ensured simply by ensuring the integrity of each sensor and of the transmitted data. For example, load cells and item counters could be manipulated mechanically to produce false data. A weight determination could be made either too high or too low by exerting force mechanically on a load cell when an item was being weighed. For this reason, visual surveillance of the weighing and counting equipment, using closed circuit television, is necessary.

Protection against deceiving a single sensor at a given time would be achieved by co-ordinating the operation of more than one sensor. For example, a projectile on a conveyor belt would trigger an item counter; in turn, signals from the counter would cause the activation of the television surveillance system at key points while also alerting other process monitors along the path of the projectile. Since it would be known what activities and data values are to be expected during the destruction process of the projectile, the appropriate sensors for these activities should give readings within a known range and time period.

Any sensor not recording the appropriate information within the normal time period would cause an alert in the monitoring system. Reactions to such alerts are part of the operating procedures of the inspectors. Such reactions would be determined by categorizing the various possible alerts into levels of significance. In turn, the significance of each alert would be related to the impact it has on the verification system.

Effective monitoring might also be prevented if a key sensor fails to work properly. Therefore, the over-all data collection system for monitoring the destruction of chemical stockpiles must be designed either with redundancy of sensors or redundancy of coverage or both. Redundancy of coverage means that information about any process step can either be collected with the corresponding sensor or it can be deduced from information collected by sensors at other steps of the process; redundancy of sensors means that every sensor is duplicated. Sensor duplication is feasible for inexpensive items such as temperature sensors or flow meters; however, it becomes impractical for such large items as television systems and gas chromatographs. The preferable approach, which is the basis for the procedures described in this paper, is to have redundancy of coverage whenever feasible so that no single monitoring step becomes a critical one. The development, therefore, of the monitoring system involves two major components: secure and reliable sensors and an effective system design.