Document Number : DP-MS-89-309

PAPER

The design and implementation of an Intrusion Path Analysis (IPA) function came about as a result of the upgrades to the security systems at the Savannah River Site (SRS), near Aiken, South Carolina. The stated requirements for IPA were broad, leaving opportunity for creative freedom during design and development. The essential elements were that it: be based on alarm and sensor state data; consider insider as well as outsider threats; be flexible and easily enabled or disabled; not be processor intensive; and provide information to the operator in the event the analysis reveals possible path openings. The final design resulted from many and varied conceptual inputs, and will be implemented in selected test areas at SRS. It fulfils the requirements and: allows selective inclusion of sensors in the analysis; permits the formation of concentric rings of protection around assets; permits the defining of the number of rings which must be breached before issuing an alert; evaluates current sensor states as well as a recent, configurable history of sensor states; considers the sensors' physical location, with respect to the concentric rings; and enables changes for maintenance without software recompilation.

IPA is realtime process which receives its sensor information from a network of minicomputers that are widely distributed at SRS. These satellite, data-gathering computers are paired to avoid single points of failure to ensure that field sensors are always monitored and their statuses analyzed. Typically, one geographical region or area is covered by a pair of satellite computers for the sensor monitoring and controlling functions related only to intrusion detection (another pair of computers is used for each area to regulate authorized worker and visitor access within the area). IPA operates on a large mainframe computer which is networked to the satellite areas for realtime message passing. The mainframe is therefor a single point of reporting/analysis for all of SRS's intrusion detection assets, and is the logical platform for IPA to be performed and reported.

The initial design involved commingling an existing tree structure, one for each satellite area, central to the entire Electronic Safeguards and Security System (ESS), with data needed for IPA processing. After careful study, the design goals were met, with only minor changes to the tree structure. All sensors which are included in a ring must appear to the right (in the tree) of the assets which they protect. This also gives a natural left-to-right orientation

of sensors with respect to the depth of the sensor within the concentric rings (Reference Figures 1-1 and 1-2). Building perimeters can be rings of protection, as can building floors or rooms. It was further defined that breaches of rings are based upon any non-secure sensor status (Access, Mask, Alarm, Disable) within that ring. The area computers have the ability to change the reporting status of each sensor. An Alarming sensor is one which has been physically tripped by some action in the field. A Disabled sensor is one which is not reporting, possibly because of maintenance or failure. The remaining non-secure states which IPA considers are closely related. An Accessed sensor does not report alarms to the guards at the workstations, but does report if it is tampered with. A Masked sensor is one which has had its inputs disabled by a guard, usually because of frequent alarms being reported for a known, non-threatening reason.

Anytime a sensor state change is detected, in any of the satellite areas, IPA considers this change. The first processing consideration is whether the sensor node is to be considered for IPA processing. This inclusion or exclusion for each sensor is accomplished by using a byte array, one element per node. Each node in the tree contains pointers, with respect to its position in the tree, to the sibling node on its right, parent node, and first child node. These pointers are used by IPA during the search for breached rings. The pointer for the sibling node on the right is conditionally used to represent the beginning of another outer ring in the tree. The actual sensor nodes, ones corresponding to field sensors, contain additional information about their type, current status, alarm priority, etc. The IPA process may be configured as to the number of rings which must be breached in order generate a Path Alert. These thresholds of breaches are loaded at initialization of the IPA process for each area.

Exceptional processing is performed for the outermost ring of protection, the perimeter. The perimeter can generally be described as a multi-layered fence, divided into sectors of coverage, using different sensor technologies in each layer of a given sector (Reference Figure 1-3). The frequency of false alerts is decreased because, in the perimeter, sectors are considered breached only when more than one layer is non-secure, either in the same sector or adjacent sectors. This approach also helps to minimize the effects of weather conditions such as heavy winds, snow, or rain on the exterior sensors. It also helps IPA to avoid 'crying wolf' to the guards, thereby lending more credence to each Path Alert which IPA generates.

Rings, other than the perimeter, are breached based upon simple non-secure sensor(s) existing within a ring during a time window. The recent history of candidate sensors is

tracked using a table of records. A sensor becomes a member of the candidate table upon leaving the secure state, and is removed from the table only after its time window expires; that is, the desired amount of history has elapsed. The sensors which become members of this table have their "time-remaining" field updated at regular intervals, based upon an operating system timer. The time window is a configurable item, which is loaded at process initialization, and is easily changed to better suit security needs for a given area.

Once the number of breached rings reaches the defined threshold, operators are informed of the existence of a Path Alert on two graphics displays, which provide two levels of detailed maps of the area being monitored. The maps show the perimeters; buildings; floors; rooms; and the actual sensors at varying levels of magnification. The workstation operator can control the level of detail shown for each map via a touch screen interface to the host processor. The sensors involved in the Path Alert are visibly distinguished to the operator by the appearance of cross-hatching over the normal sensor color, which represents status. This cross-hatching remains in effect as long as the preset number of rings remains in the table, i.e., the involved sensors are still non-secure or are within the time window since becoming secure. When the number of such rings falls below the threshold, the cross-hatching is removed from all sensors in that alert group. If a sensor status (color) changes while a member of the alert group, the cross-hatching remains in place until the group falls below threshold, regardless of the underlying current status.

This uncluttered presentation of alerts allows the operator's pattern recognition abilities to adjudge the proper response, while still presenting the sensors' true status. Preserving actual sensor status is important because this data is crucial to the operator, so IPA information must not obscure it. The current design also notifies the operator with a textual warning message in the pending action queue, which requires only acknowledgement. This assures that the alert is not lost through the usual operator activities. Reports are also available to the operator to further clarify characteristics of the involved sensors. Note that the existence of a Path Alert does not force action (except simple acknowledgement) nor does it prevent the operator from exercising options necessary to perform his duties; rather, it notifies the operator of a situation involving increased risk. The operator may request, via workstation interaction with the host, closed circuit television views of involved sensors in order to allow further realtime review of the situation.

Let us consider two scenarios to illustrate the concepts presented thus far. The first considers an outsider

incursion, and the second examines an insider excursion. Initially consider all sensors secure, with no recent history of being non-secure (Reference Figures 1-1 and 1-2). Assume an alert threshold of three non-secure rings for issuing a Path Alert.

Scenario 1 : Outsider Incursion

o IPA is awaiting an event, either a sensor state change or the operating system timer request signalling that it has expired.

o A non-secure state is received for sector 1 sensor 1A.

o IPA checks to see if this sensor is included for IPA processing. It is, so IPA checks for non-secure states in different layers of sector 1 or its adjacent sectors.

o The search reveals none. IPA processing returns to the wait state.

o A non-secure state is received for sector 1 sensor 3C.

o IPA determines that sector 1 of the perimeter should be added to the candidate table for path alert consideration. The non-secure state which sector 1's sensor 3C reported, as well as the time of receipt are also saved for reporting purposes.

o IPA receives a non-secure state for building 10's shell sensor 3C. It is included for IPA consideration so it is added to the candidate table.

o At this point two rings have elements which have reported non-secure statuses within our time window. Since our configurable threshold is three rings and our table only contains two elements, IPA does not search further and returns to its wait state.

o Building 10's Material Access Area sensor 4D reports a non-secure status. IPA adds it to the table and discovers that at least three members now exist in the table. This meets our alert threshold. However, these do not necessarily exist within different concentric rings. Further analysis must seek to verify this possibility.

o IPA performs searches upward from each active zone in the table to see if it can find non-secure statuses in three successively larger rings.

o IPA begins the search with the first active zone in its sequential table and traverses upward from there. At each level a check is performed to see if the immediate right hand node's pointer value indicates another ring. If it

does, IPA checks to see if that over-head node has had any sensors subordinate to it which are in our candidate table. If it does, we have a breached ring.

o The search beginning with building 10's sensor 4D indicates that three rings are breached and a Path Alert should be issued. The innermost, breached ring in this scenario includes building 10's sensor 4D, the middle ring includes building 10's shell sensor 3C, and the outermost ring includes sector 1 with its multiple layers being non-secure.

o These sensors now become visibly distinguished by crosshatching on the workstation's graphics displays. The distinction remains until at least one of the member sensors has been secure for the given time window. When this occurs, all of the Path Alert sensors, within the group, have their cross-hatching removed. An element is also placed in the pending action queue and a hard-copy report is generated to the operator.

Scenario 2 : Insider Excursion

In this scenario the non-secure states are not received in a clear sequence, but the analysis can be done nevertheless. Consider that non-secure states are reported, within our time window, for the following sensors : sector 1 1A, sector 2 2B, room 1 2F, room 2 1E. Which will result in the issuing of two distinct Path Alert groups. One with Room 1 2F as its base, and the other with Room 2 1E as its base.

o When sector 1 1A, sector 2 2B, room 1 2F, and room 2 1E are received the processing occurs as described in scenario number one, above. These sensors are marked as active in the IPA candidate table, but no search is warranted.

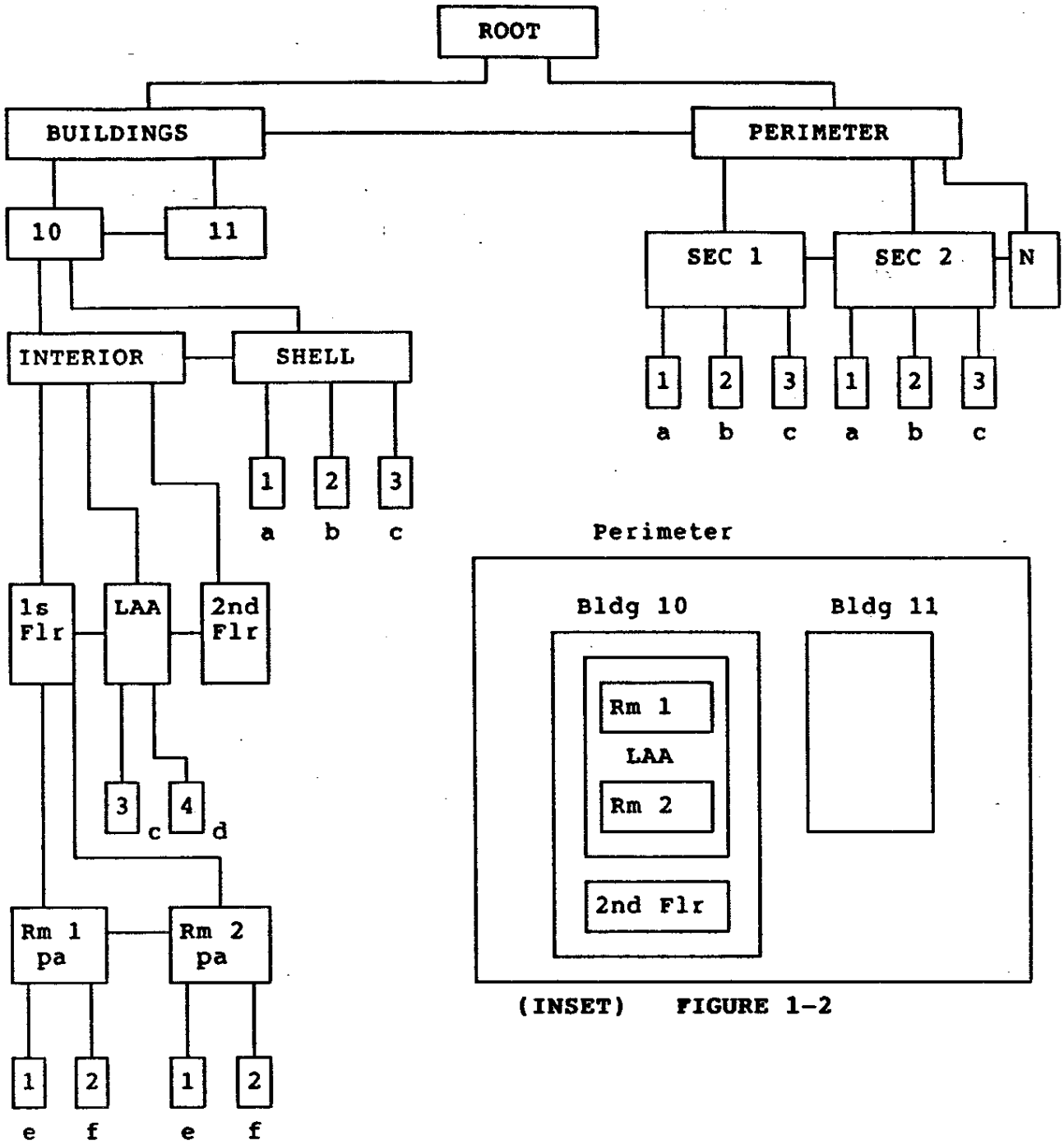
o When building 10's shell sensor 3C reports a non-secure status it is added to the table and a search is performed.

o Neither the searches beginning with our candidate sector sensors nor the search beginning with Building 10's shell sensor 3C yield paths, but the searches starting at both Room 1 2F and Room 2 1E indicate paths.

o These Path Alert groups are now distinguished to the operator just as in scenario 1.

The design and implementation of the IPA algorithm affords the operators and security monitoring personnel significant information, with minimal additional overhead, which could lead to the prevention of possible undetected losses of protection. Most security monitoring systems depend upon the handling of discrete events sequentially in

order to assure protection. The IPA processing provides a recent history (to detect slow incursion/excursion) for multiple-event conditions. It is believed that this capability will be especially helpful when sensors are placed in non-secure modes for long periods of time (extending across operator shifts) or when temporary relief personnel are employed for short periods of time, and no time is available for an awareness 'learning curve'.



(INSET) FIGURE 1-2

Scenario 1

Sector 1 1-A
Sector 1 3-C
Bldg 10 Shell 3-C
Bldg 10 LAA 4-D

Scenario 2

Sector 1 1-A
Sector 2 2-B
Room 1 2-F
Room 2 1-E
Bldg 10 Shell 3-C

FIGURE 1-1

SAMPLE PERIMETER FENCE

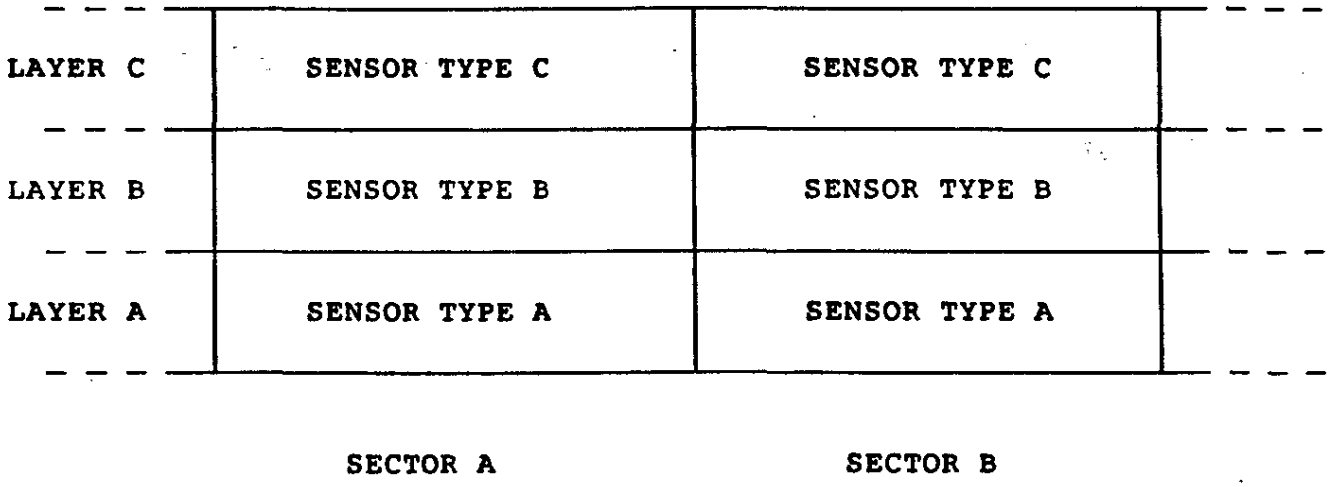


FIGURE 1-3