**Introduction**

Security Professionals were suddenly brought face to face with the hopelessness of the situation on 11 September 2001 and again on 13 December 2001. This hopelessness was not due to their failures but due to the sheer ability of a committed terrorist to turn even a routine device into a weapon of terror and also to press ahead and break through physical barriers. There was a sudden realization that you not only have to be good but you have to be exceptionally good to be able to beat a criminal at his game. Genesis of both these cases and attacks was failure of Access Control systems and inability of existing systems to stop the forcible grabbing of access.

Obviously like in all hopeless situations, the Security professionals are turning to technology to provide solutions to plethora of their problems from tracking, to cyber crime to access control. At the same time they are quite aware of the fact that technology alone will not provide all the solutions. The search is on for new and Intelligent Security Solutions using latest in Sensor technology, Image Processing, Computing and Communications.

Let us today talk about and understand the criticality of the most important and most crucial of the security philosophy, **Access Control**. We will also see the methodology of translating this philosophy into deliverables and finally at integrating this philosophy with other processes like Integrated Building Management and Automation Systems (BM & AS). It is inevitable that in these discussions we will look at technology as not only solutions enabler but also as the driving force for modernization and optimization.

**What is Access Control Philosophy in the contemporary settings?**

I will not spend any time on elaborating on challenges for security managers world over. The severity and depth of impact of uncontrolled, unauthorized and unmonitored access to any assets and specially those assets which control more assets is quite obvious to all of us. Any failure to control, restrict and monitor access will result into massive disruptions, damages and losses. The fact that such perpetrators of crime are likely to posses sophisticated weapons and devices and will be committed to press the attack to its logical end makes the situations even more challenging and potent.
Under these circumstances what will be our philosophy for planning the access control systems and methods? What tools and equipment will be used? I will flags following as the guiding marks for this exercise:

1. In the changing scenario efforts will now have to be made to screen and control access as early as possible and as far away as possible from the real assets. Thus the barrier where such devices are to be fitted and used should be at the outermost periphery of the establishment. This will allow sufficient distance and time to be created between at attempt to break thorough the barrier and the real assets to be protected.

2. Such access control devices will have to be monitored and watched not only manually but also using electronic surveillance and recording devices. This will allow the Security Head to not only control the access but also to record and analyze all attempts of successful as well as unsuccessful crossing of the control barrier.

3. The Access Control devices must be made more intelligent and with at least some diagnostic and logic capability to generate signals associated with any abnormal events or routines. These signals should then be routed to generate sufficient and appropriate responses from other parts of the set up. Typically any attempt to force the barrier or jump over the barrier should generate audio and video alarm and also capture picture of the culprit that can be later used to proceed against him.

4. The Access Control devices must be integrated with all other electronic security network and to and from signals should be managed intelligently. Such integration must be ensured to deliver real time responses and data sharing.

5. Access Control devices must also be integrated with Building Management & Automation System. This will enable data capture abilities of the intelligent access control devices to be used for multiple tasks in the BMS.

6. All information used by Access control systems to allow or deny entry must be drawn from a centralized database. Stand alone systems can be compromised vary easily.

7. It would be advisable to make decisions of Access Control based on data that is getting updated in real time rather than one time entered data. Need and advantages of this are obvious.

8. All data captured in the Access Control systems must be archived and saved for later day analysis. Such archived data and trending from this should form basis for generating logic of Access Control decisions.

9. Access Control Systems will have to be designed both in hierarchically ordered and organized in circular fashion with each higher or inner level implementing higher level of control.
**New Security Control Trends**

The new trends in the way the systems are conceptualized, designed, built and implemented will try and cater for the above principles. The challenge for the Security professionals will be to provide management and integration backbone for the solutions. They will have to take a fresh look at the permissible peripheries and controlled areas. Selective controls and restrictions will have to be tailored into corporate ethos and culture. Delays and lines may have to be disguised to look like deliberate time given to customers to absorb the corporate image before they are ushered in. They will also have to learn to use more automated and remotely managed tools for faster processing of entry and exit requests without sacrificing the human factor in surveillance.

Let us now translate these principles into actual deliverables for the modern and integrated Access Control systems. The list below is neither complete nor exhaustive but definitely covers all the important deliverables.

1. Real time segregation of persons and vehicles seeking entry
2. Time based access control and entry restrictions
3. Exit controls
4. Selective access control within a large area
5. Dynamic updating and tasking of the system
6. Data archiving, trending and tracking
7. Intelligent image processing, tracking and access control
8. Links to other Management, Personnel and BM Systems
9. Material movement tracking and accounting system
10. Connectivity to remote monitoring and archival sites
11. Multi locational systems
12. Information exchange and updating over web and other communication channels

**Access Control Devices**

Obviously the solutions are well beyond the manual as well as existing devices used for access control. More intelligent and smart devices will have to be brought in. These will have to be backed up by real time data processing capabilities and image processing.

The new generation devices will use technologies that will be able to leverage advantages offered by web solutions linking huge and continuously updated databases to the point of entry and exit gadgets. At the same time the information and data carried on the cards, gadgets or simply the code number will be upgraded. Thus these devices will be technically superior and advanced to be able to offer the desired solution.
I will not go into more technical and device specific discussions as this will be covered separately. I will only like to mention that as of now large number of technologies and solutions are available in the market. What is most important is to ensure that these devices and technologies are implemented as part of a complete business process and not in stand alone manner. My experience suggests that such attempts always end up in failures.

**Software Solutions**

As is being accepted in all other areas of applications, hereafter software solutions will have to be deployed in conjunction with the hardware to make the hardware deliver all our expectations discussed above. It is quite obvious that the hardware solutions have reached upper limits of their capability and we can not extract anything more out of them.

Software Solutions that will have to be brought into play for this enablement must use power of the new packages and also the potential of communication and web technologies. Deliverables for these solutions can be listed as under:

1. Real time connectivity to all the access control stations and readers. This may be through hard wired or remote nets.
2. Compatibility with all technologies used for access control devices
3. Ability to integrate devices and equipment of different generations including legacy systems if any
4. Ability to integrate manual component of Access Control systems
5. Large data storage and processing capability
6. Data archiving and trending
7. Distributed architecture for faster and real time processing of requests
8. Connectivity to other devices and equipment like Alarm panels, CCTV, etc.
9. Image processing and image matching
10. Web enabled and net connectivity
11. Configurable on real time basis
12. Integrated deployment
13. Emergency Call Management Capabilities
Integration of Access Control Systems with BM & AS

As spelt out earlier the intelligent access control systems will be able to capture large data on real time basis for both personnel as well as material. It will be very easily possible to stream this data into the BM & AS on real time basis. Such streaming will help both the systems and management tools. What will be most crucial again will be to ensure that such streaming follows the business processes for both and does not create conflict situations where further intervention will be required.

There are host of obvious advantages in such linking up. I will list just a few major ones out of these.

1. BM & AS will get real time and continuously updated data that will be used for calculation of loads, utilities and other services.

2. Strengthening of Security delivery by use of Access Control system will allow the BM & AS to be kept more distributed rather than centrally controlled.

3. Data Storage and Trending capabilities of these software can be used to study the efficacy of BM & AS.

4. These capabilities can also be used for calculating seasonal or other variations and planning for the same in BM & AS.

5. At the ground level the Access Control data pertaining to entry and exit control can be used for switching on and off certain distributed facilities like say lighting or stand alone AC units.

Conclusion

Let me conclude by saying that the complex challenges for Security Management are getting even more complex and potent as the would be culprits are getting smarter, deadlier and more committed. One major challenge is to deny effectively access to such would be criminals by using the intelligent Access Control systems discussed above. If we can achieve this objective we would have gained a finite advantage over the criminals in the game of security.