

Selecting an effective Perimeter Security System



Perimeter security is about deterrence, detection, denying, delaying and defending against intrusion. It is the first layer of security against intrusion.

Various technologies and solutions are available for perimeter protection:

- A simple physical barrier - RCC compound wall or chain link fence.
- A physical barrier with illuminators.
- A physical barrier with cameras mounted on top.
- A physical barrier with thermal imaging cameras mounted on top.



Fence mounted cameras



Thermal cameras

- A chain link fence with vibration sensors.
- A chain link fence with a detection system using fibre optic cable.
- A physical barrier with an electrified fence mounted on top.
- A self standing electrified fence.
- Use of cameras with auto-tracking capability.



Electrified fence



Virtual trip wire

- Video analytics.
- A combination of some or all of the above technologies and solutions depending on the perceived threat.

Selection criteria

The following steps must be followed in order to select an effective perimeter protection system:

- Conduct a 'threats, risk and vulnerability' assessment of the site.
- Recognize the threat level and the potential for future escalation or otherwise. Some sites may need a mere fence that will deter potential intruders while other situations may require a fence with mounted cameras.
- Study the environment around the site – the landscape, flora, fauna and the topography. **Quite often the topography can provide natural protection and sometimes a potential source of vulnerability.**
- Study the climatic conditions and its effect on the different types of systems available.
- Understand the local regulations and the social acceptance of some of the protection systems e.g. Electrified fences may not find acceptance in some cases
- Check for the presence of high voltage power lines in the vicinity and the possibility of electromagnetic interference that may affect specific technologies.
- Some sites e.g. oil rigs or process plants may require the technology to be intrinsically safe.
- Some threats may require a covert (hidden or buried) system in addition to a 'in your face' deterrent.
- **Where the threat perception is high and/ or the asset critical, it may be necessary to take a layered approach and deploy multiple technologies.**
- Use video analytics as it acts like a force multiplier and considerably enhances the effectiveness of the security staff.
- **For the perimeter protection system to be effective it must integrate seamlessly with the overall security strategy.** This is a very important factor in selecting the system and the technology.

Conclusion

- The integration and layering of different perimeter intrusion detection technologies offer customers the most dramatic improvements to site security.
- **An integrated solution acts as an efficient and effective force multiplier.**
- Combining cost-effective technologies reduces nuisance alarms.
- **The latest technology and / or the costliest solution may not necessarily be the most effective solution.**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX