

The CNI2000 Intruder Detection System (CNI2000-IDS) protects critical national infrastructure such as electricity substations, water reservoirs, oil rigs, gas pipelines, container terminals, and telecom towers. The CNI2000-IDS does this by detecting interference with or intrusion into access points such as hatches, infrastructure doors and covers.

The CNI2000-IDS utilizes a range of commercial off-the-shelf sensors to instantly detect and verify intrusions which are then transmitted to manned event logging Alarm Receiving Centers and mobile personnel. False alarms are minimized by incorporating multiple sensors and technology-based sequential verification which removes or minimizes human operator fallibility in interpreting a potential alarm.



The CNI2000-IDS unique wireless and/or wired design translates into a rapidly installed, low running cost, technically superior solution able to operate in the most hostile environments, including extreme temperatures, humidity, and corrosion. The CNI2000 open technology platform enables integration with existing systems such as GUI, SCADA, CCTV and access control via RS232 and independent connectivity with GSM/GPRS and/or global satellite network.

The advanced architecture of the CNI2000 platform enables customization of the CNI2000-IDS with a range of options, including:

- Analog or digital sensors of all types
- Wired, wireless, or hybrid configurations
- Covert or overt installations
- Standalone or integrated with cctv cameras, access control, quality monitoring, UAVs etc.
- Fixed or transportable units
- Single or multiple communication links to command and control centers
- Security or safety or multi-purpose applications
- Civilian or military standards for a full range of operating environments
- Integrate with other CNI2000 systems (CNI2000-CBRNE, CNI2000-EM)

Options include:

- Distress signals
- Remote reset
- Self diagnostics
- Solar power
- Site management reporting