Doorman at the Server Cabinet

Turck's IM12-CCM monitors the relevant ambient variables of control cabinets – regardless of whether in industrial applications or for protecting IT systems at utility companies and infrastructure facilities

Whether in industry, banking or energy supply applications: Control cabinets and protective enclosures can be retrofitted in an instant with the IM12-CCM in order to meet the requirements of the IT security law

On July 2, 2015, the IT security law came into force in Germany with the aim of increasing the security of IT systems. Not only in the IT sector but also in critical infrastructure installations, such as for electricity and water supply, finance, health and food production. The law applies wherever malfunctions or failures may result in dramatic economic, national and social consequences.

The first implementation of the IT security law, which came into force on May 3, 2016, requires compliance from the energy, information technology, telecommunication, water and food sectors. These sectors are primarily required to increase the security of their information technology and forward a message to the responsible authorities in the event of an attack on their IT system. Reporting is mandatory as soon as a company has more than 500,000 consumers. The law here stipulates explicitly that all IT systems that are essential for the functioning of the critical infrastructure must be protected by a minimum level of security standards.

Energy suppliers, water works, water drainage companies, information technology as well as food manufacturers are now required to create a safety concept for their IT systems. Other sectors such as finance, transport, traffic and health will probably be incorporated in 2017. Manipulation protection from direct access to the control level via the control cabinets is an important point in these safety concepts.

Manipulation protection

It is precisely here where Turck's cabinet guards of the CCM family show their strength. Any control cabinet containing instrumentation, as required in the operation of a critical infrastructure, is exposed to a certain degree of risk of manipulation. Any unauthorized person could gain access here to the control level or also switch off the safety systems. The cabinet guards of the CCM series also reliably monitor the closure of the door and can then prevent or indicate any manipulation.

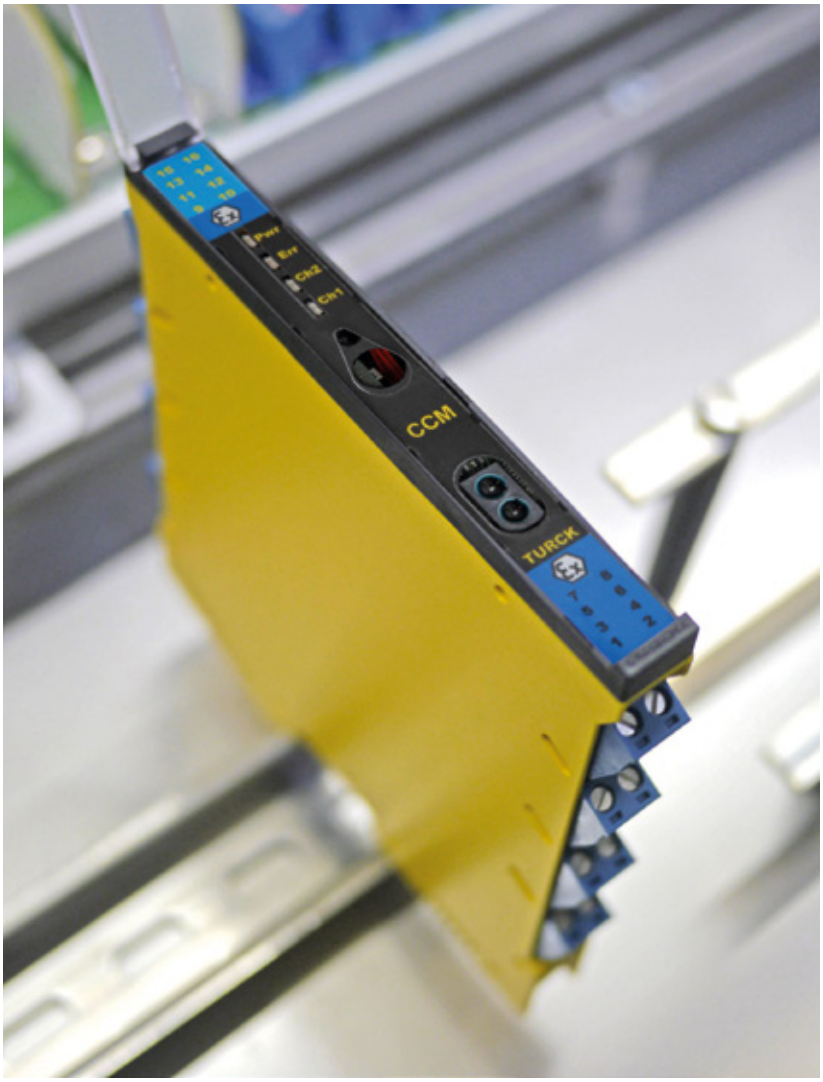
Besides the IMX12-CCM, which was launched a year ago for use in explosion hazardous areas, Turck is now offering a second model, the IM12-CCM, for use in non-Ex areas. Thanks to their slim design, the cabinet guards are easy to retrofit and are difficult to manipulate. The DIN-rail devices can be integrated quickly in existing infrastructure systems. A simple switch contact is enough to indicate an alarm and has a 24 volt power supply.

A certain degree of security can naturally be achieved by simple means, such as with locks or door position switches. However, these solutions are easy to circumvent with very simple means and therefore do not sufficiently meet the requirements of the IT security law. A simple lock, for example, does not offer any direct indication of opening or manipulation.

With an IO-Link interface and master/slave mode, the new member of the CCM cabinet guard series is ideal for factory automation and IT security

QUICK READ

Turck's IM12-CCM cabinet guard can monitor temperature, humidity and the correct door closing in the control cabinets used in the manufacturing industry. The device can be retrofitted easily and reliably offers protection from any manipulation at the control cabinet. This makes also it suitable for protecting IT systems, as required by the IT security law for critical infrastructure facilities.



The IMX12-CCM launched a year ago is primarily designed for use in the Ex area thanks to its intrinsically safe 2-wire isolating transducer interfaces

The IM12-CCM model in particular is suitable for the tasks covered by the IT security law. The device can not only monitor the distance to the door, but also the closure of the door via a connected reed contact. This provides additional security since both security functions can only be defeated simultaneously with great difficult. Besides the door closure, the IM12-CCM and its counterpart for the Ex area also monitor humidity and the temperature in the control cabinet. They also indicate to the controller with a simple switch signal the exceeding of taught limit values.

With larger control cabinets, one location is not enough for monitoring. This applies both to door closure as well as temperature monitoring, since the temperature in the control cabinet can develop unevenly. In this case, the use of two devices is recommended. In order to avoid having to use several input channels in a PLC, it is possible to operate two IM12-CCM devices via an interface in master-slave mode. In this case, the master operates as the data collector of the slave and processes the data to determine the limit values.

Which cabinet guard is the right one?

As the IM12-CCM model is not designed for the Ex-area, unlike the IMX12- CCM model, it can be supplied with 10 to 30 VDC and is equipped with different interfaces. The new device is provided with an IO-Link interface for setting parameters. The IO-Link channel enables all process parameters to be read as measured values. They are then processed via an IO-Link master such as TBEN and Profinet/Profibus in the higher-level system. As with the IMX12-CCM, FDT software such as Pactware can be used alternatively for setting the parameters.

Both devices are equipped with an internal data logger. Thanks to its integrated real-time clock, the IM12-CCM can even store the data with a time stamp. Users read the stored data via the IO-Link interface. The device saves data for up to two years. In the event of a power failure, the clock power supply backup is implemented without the use of batteries. If the device is connected via IO-Link, the measured values can also be written to a memory continuously. This can also continue over a long period. Gradual changes in internal temperature and humidity can then be detected more easily in order to identify the cause.

Author | Klaus Ebinger is Director Product Management Interface Technology
More Info | www.turck.com/ccm
Webcode | more11771e

Detecting gradual changes

Humidity is often a problem in enclosed systems and should therefore be measured continuously as part of the condition monitoring system. The protection provided by control cabinets can decrease as the period of operation or the load increases. This can either be due to mechanical damage, the aging of the sealing material, defective ventilation systems or negligence such as incorrect closure. It is often gradual processes, such as continuously increasing humidity, that eventually lead to the failure of installed equipment. These effects can often only be detected over a long period. Turck's control cabinet guards also detect these long-term trends and notify the control level when limit values are exceeded.