

# Cyber security for pipeline control systems

Cyber security for pipeline control systems

February 2009 (article)

Eric Byres, CTO of Byres Security Inc., has published an article about cyber security and pipeline control systems in Pipeline and Gas Journal.....

ARTICLE EXTRACT:

## CYBER SECURITY AND THE PIPELINE CONTROL SYSTEM

Feb 2009, Pipeline & Gas Journal. Eric Byres, CTO of Byres Security, published an article about cyber security and pipeline control systems where he describes several actual cyber security incidents that have had significant impacts on pipeline companies. These incidents include:

-

Computer sabotage to the Petroleos de Venezuela, S.A. that interrupted tanker loading

-

A Trojan horse attack on the Trans-Siberian gas pipeline that disrupted gas supplies and foreign currency earnings for the Soviet Union for over a year

In the article Eric goes on to describe several causes of cyber security problems, such as:

-

Misunderstanding of SCADA security risk by management.

For example, managers may assume that the Information Technology (IT) group automatically looks after SCADA security, whereas this is rarely the case.

-

The assumption that all cyber security problems arise from outside the company, or that SCADA systems can be protected by a single perimeter firewall, whereas many incidents are caused by secondary pathways into the control network.

-

Improper SCADA network design that allows application data a "free ride" on the control network, with negative effects on control network security.

Finally, the article goes onto describe how the ISA-99.02.01 standard helps companies get SCADA security under control. Effective security is achieved by multiple levels of defence, such as the Zone Level Security™; provided by the Tofino Industrial Security Solution.

[Read the full article online](#)

[Download the article](#)