# La sécurité vis à vis de l'utilisateur final pour réduire les risques, protéger les actifs tout en respectant les normes gouvernementales

**Jérôme Poncharal**

***Solution Architect - Integrated Architecture - Rockwell Automation***

97 Allée Alexandre Borodine
Parc Technologique Woodstock
Bâtiment Douglas 5
F – 69860 Saint Priest
Tel. +33 04 72 38 34 54

**Mots clés :** *cyber-menaces, manufacturier, réseaux, Ethernet*

La découverte de cyber-menaces visant spécifiquement certains systèmes de contrôle a projeté la sécurité industrielle au premier plan dans le secteur manufacturier. Il s'en est suivi une prise de conscience croissante de ces nouveaux risques, capables de perturber le fonctionnement des systèmes de contrôle et de nuire tout autant à la sécurité, la productivité, l'intégrité des actifs ou la confidentialité des informations de l'entreprise.

L'inter-connectivité des systèmes de contrôle, toute aussi importante pour l'industrie, pose de nouveaux défis. Les réseaux de communication industriels comme EtherNet/IP, s'intègrent harmonieusement dans l'infrastructure Ethernet du site de production, communicant lui-même via l'Internet avec les systèmes d'information de l'entreprise. Le rythme de la convergence des réseaux de contrôle et d'information s'accélérant, l'enjeu de la sécurité industrielle consiste à assurer flexibilité et vigilance tout en contrôlant l'ensemble des paramètres. Ce qui est considéré comme une protection adéquate aujourd'hui devra être remis en cause lorsque de nouvelles menaces seront détectées.

Chaque client doit protéger ses actifs. Rockwell Automation dispose des compétences et expertises pour adresser les besoins en matière de sécurité industrielle, réduction des risques et permettre ainsi d'augmenter la disponibilité des systèmes de contrôle.

**Key words :** *cyber-threats, manufacturing, networks, Ethernet*

The discovery of malware that specifically targets some industrial control systems brought industrial security to the forefront in manufacturing. As a result, there is growing recognition of new risks and threats that are capable of disrupting control system operation and adversely affecting safety, productivity and the ability to adequately protect assets, machinery and information alike.

The increasing inter-connectivity of control systems is equally important to industry since new benefits also bring new challenges. Open industrial networks like EtherNet/IP that seamlessly coexist in broader Ethernet systems are being used to link various plant-wide control systems together and connect these systems into expansive, enterprise-level systems via the Internet. As the pace of control system and enterprise network architecture convergence quickens, industrial security depends on staying both flexible and vigilant and successfully controlling as many variables as possible. What is adequate protection today must evolve as vulnerabilities are identified and new threats emerge.

Every customer has something to protect. We have unique capabilities and expertise to address industrial security needs, reduce risk and enable greater operational up-time in control systems.