



ENGINEER
NEXT
NIDays

The logo features the words "ENGINEER" and "NEXT" in a bold, white, sans-serif font, stacked vertically. A yellow graphic element, resembling a stylized 'N' or a folded ribbon, is positioned between the two words. Below this, the word "NIDays" is written in a smaller, white, sans-serif font, enclosed within a white rectangular border. The entire logo is set against a blue background with diagonal stripes in various shades of blue, orange, and green.

Gestion des sécurités et de la synchronisation avec LabVIEW sur cibles embarquées

Jean-Philippe BRAUD
Gérant – Architecte LabVIEW
Phalanx

Sommaire

- Phalanx
- Les sécurités
 - Solutions réseau
 - Solutions Physique
 - Solutions OS
 - Solutions Applications
- Synchronisation de plusieurs systèmes
 - Matériels cRIO et PXI
- Questions

Phalanx

Phalanx

Nos valeurs :
Qualité et Transparence

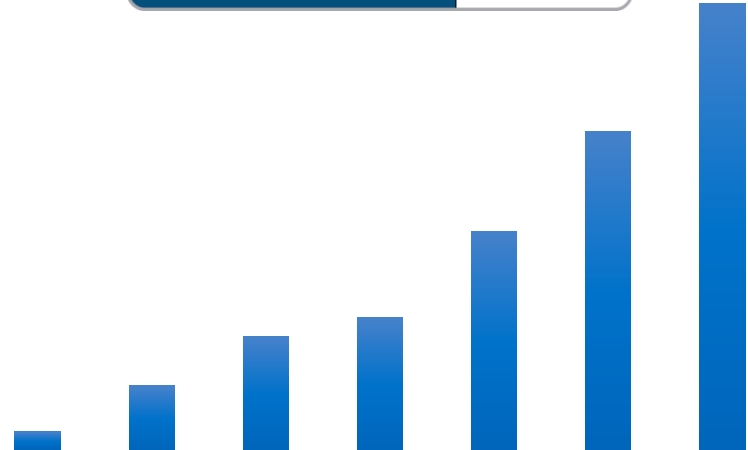


NATIONAL INSTRUMENTS

LabVIEW™

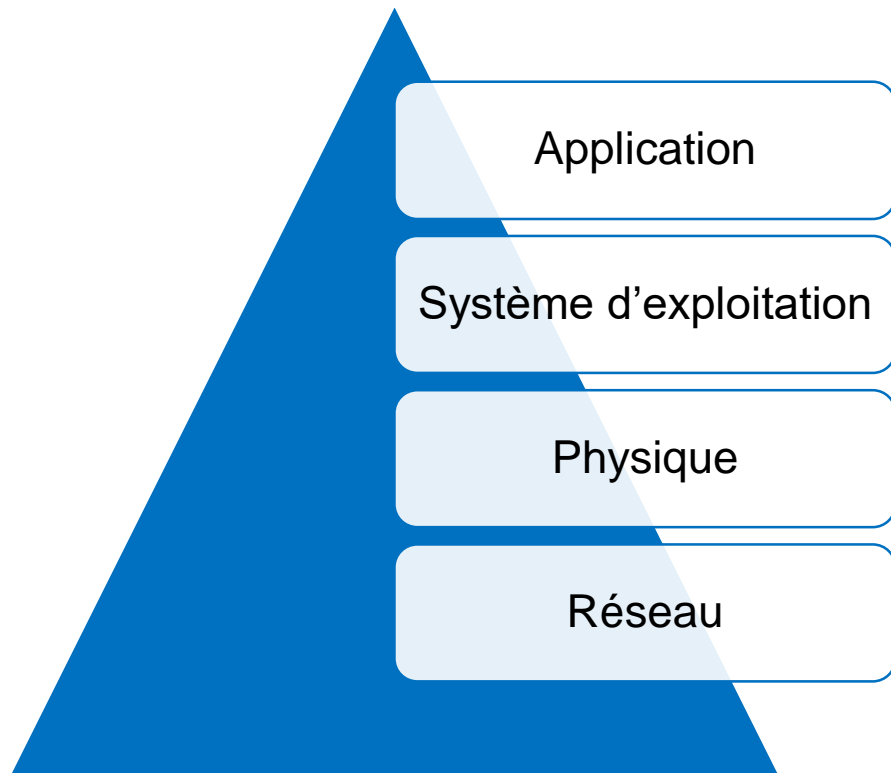


Alliance
Partner

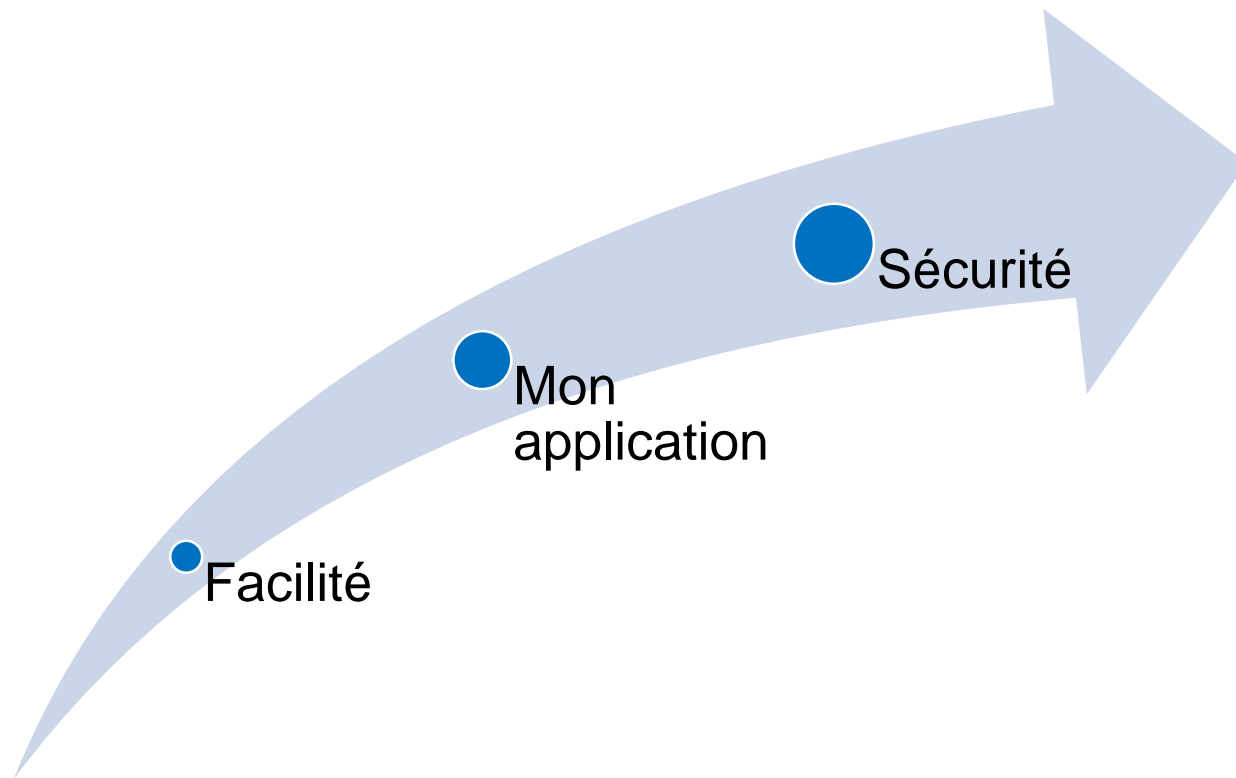


Les sécurités

Niveaux de sécurités



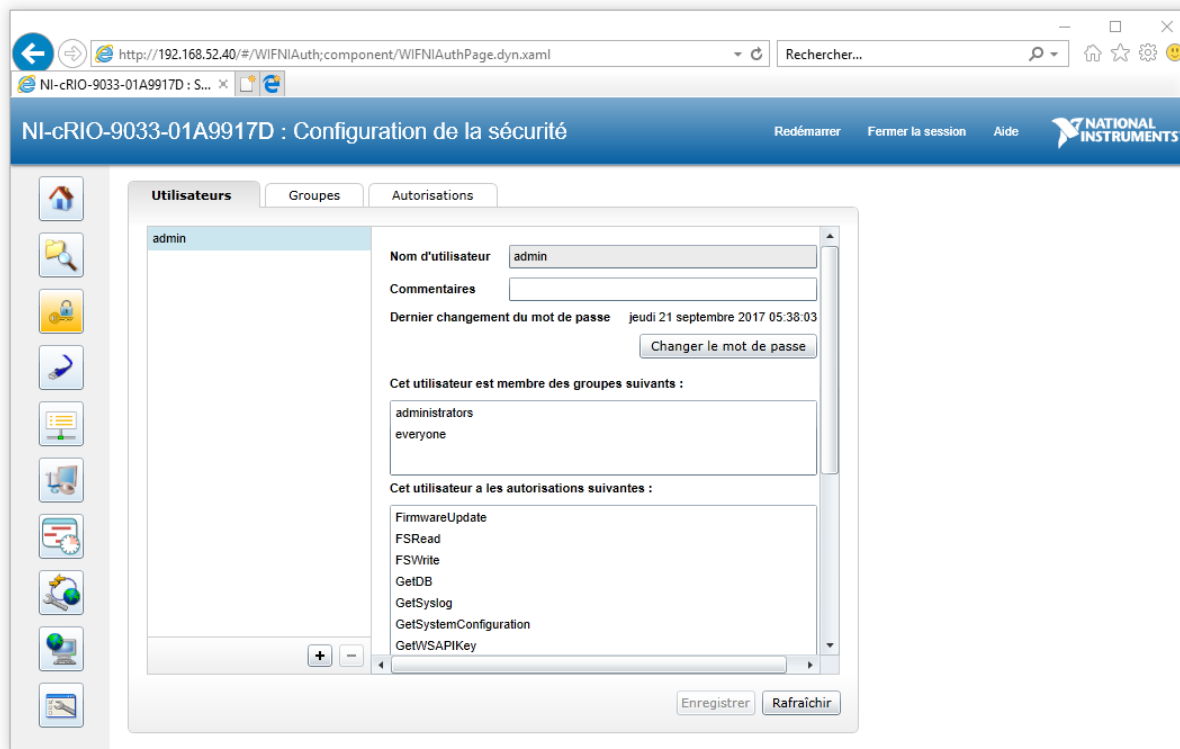
Niveau de risque



Réseau

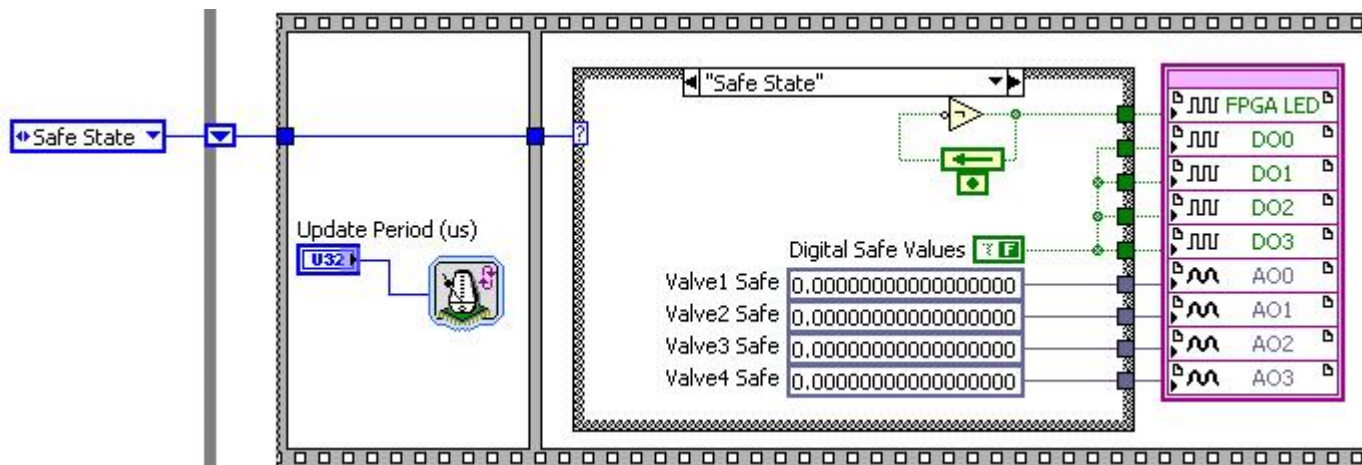
- Choisir un **Firewall** sur le PC de supervision
- Installer les **updates** du système d'exploitation
- Créer des **comptes utilisateurs (NIAuth)**
- Accès **VI serveur**
- **NI Auth** – comptes sur cible
- **SSL**
- Arrêt du **serveur FTP**
- Choisir un **réseau PC-cibleRT interne**

Réseau - Web configuration tool



Physique

- Limites FPGA
- Chien de garde et mise en sureté

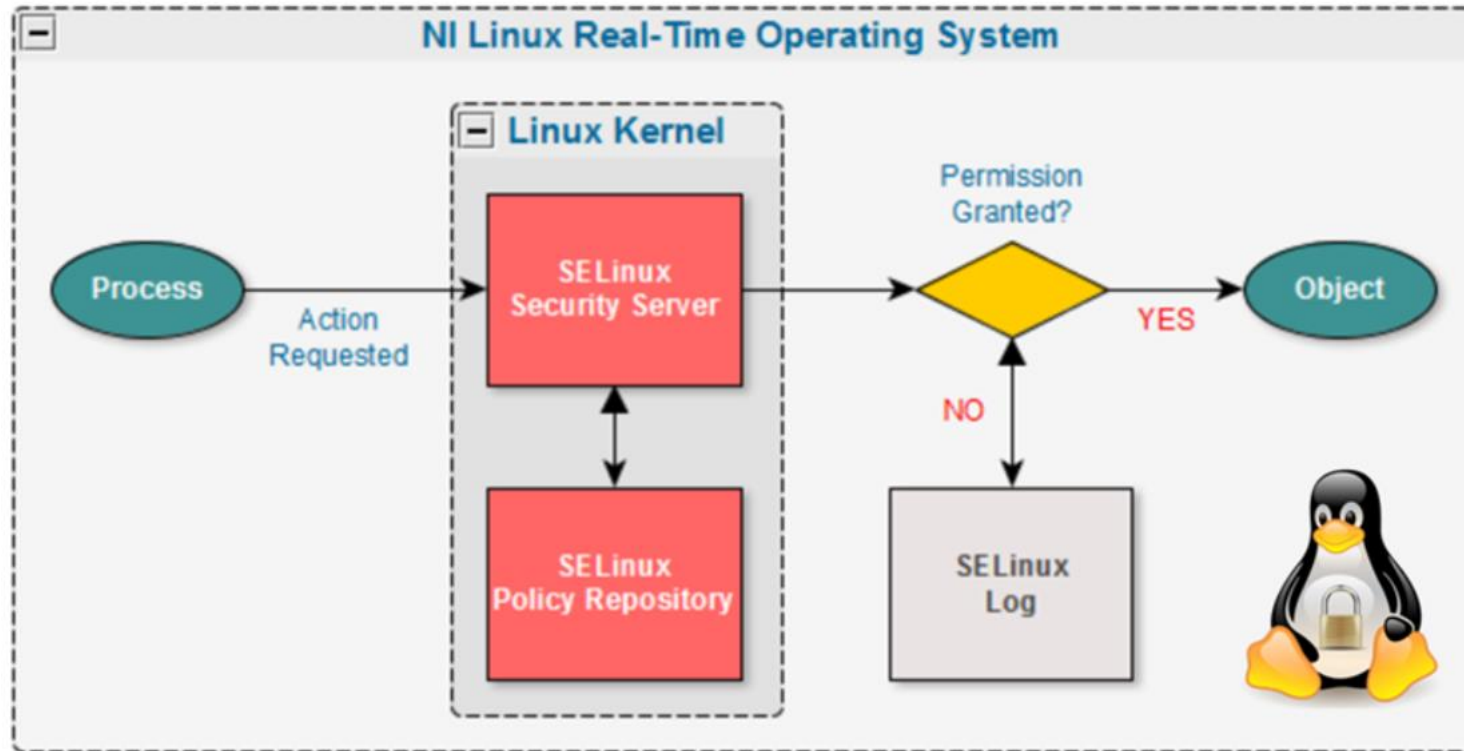


Système d'exploitation - Malware

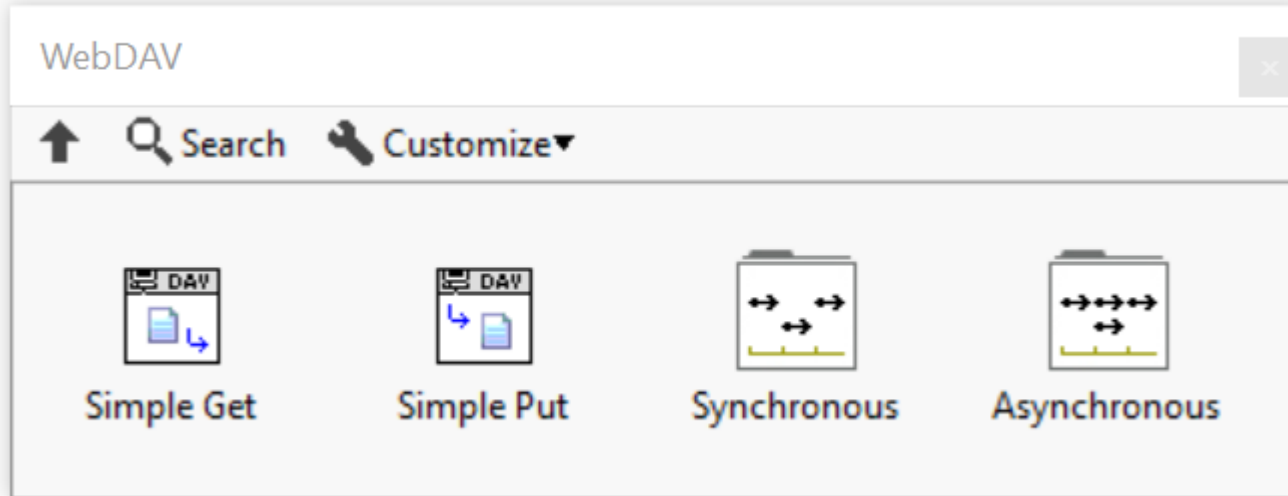
- Protection contre les Malwares
 - Linux RT construit avec OpenEmbedded framework + YOCTO
 - Fait par NI, Google, Intel, ARM
 - Pas de malware connu, mais méfiance

The report noted that 99.99 percent of all Linux malware was delivered over the web during the first quarter, with only eight of 419,367 coming in via email or by FTP. This is due to the majority of attacks hitting IoT devices, which rarely have access to email, but are always connected to the web.

Système d'exploitation - SELinux

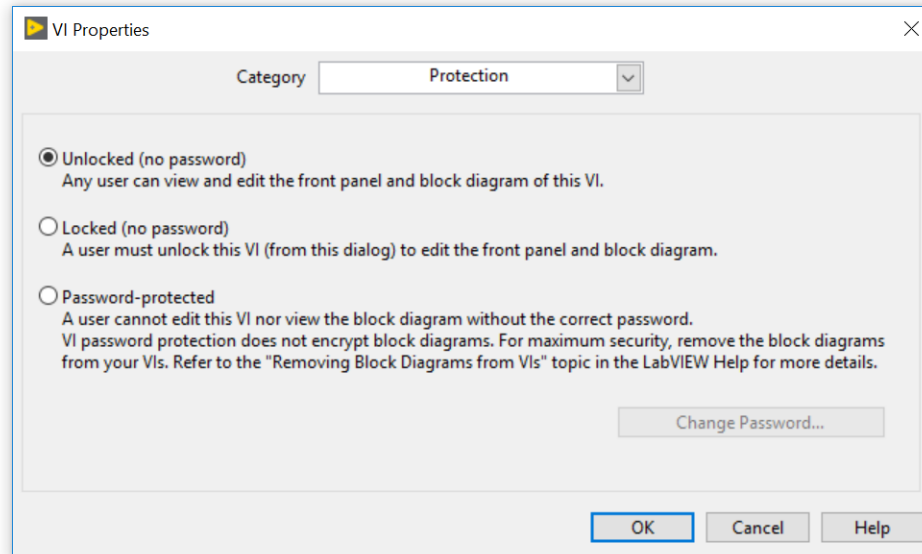


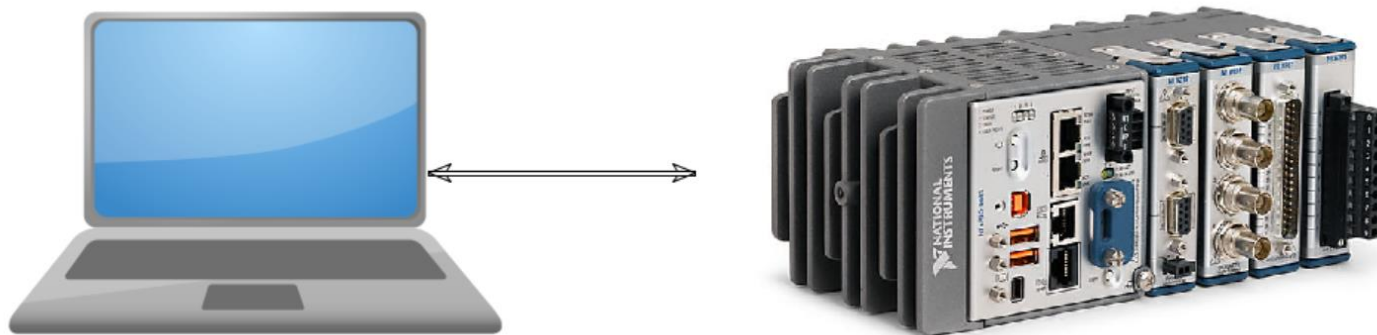
Système d'exploitation - WebDav



Application

- Mot de passe des VIs : « P4\$sword »
- Créer des exécutables – EXE et RTEXE





Exemple de configuration courante chez Phalanx

- Le PC est protégé avec anti-virus et Firewall, ouvert sur le port et l'IP du compact RIO
- Le compact RIO dispose d'un « chien de garde » pouvant le mettre en état de sécurité si un défaut est détecté.
- Le cRIO n'est pas connecté au réseau général, mais sur un second port Ethernet du PC.

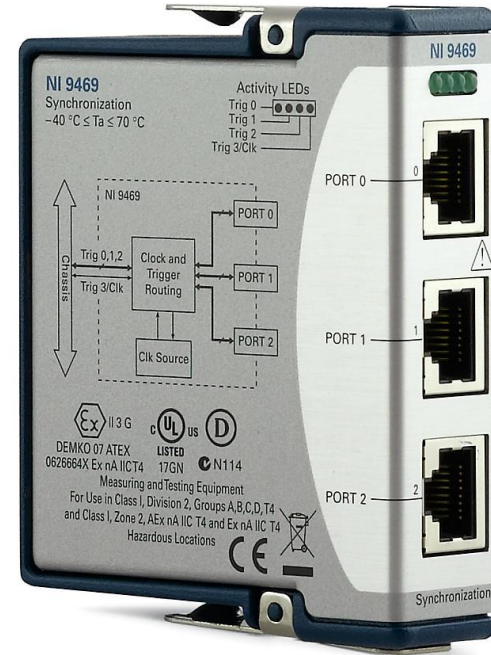
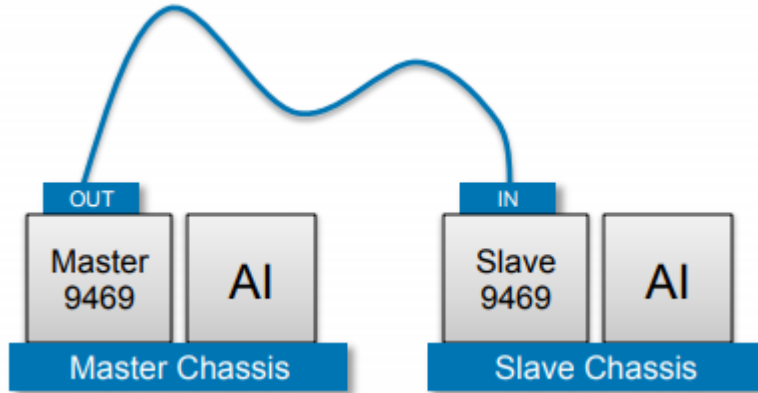
... Et bien d'autres

- Désactiver les ports USB (MS)
 - Limiter l'accès physiquement (barrières, salle fermée)
 - Changer les ports de communication par défaut
-
- Mais aussi assurer la communication vers les autres automates si l'automate maître détecte un problème...

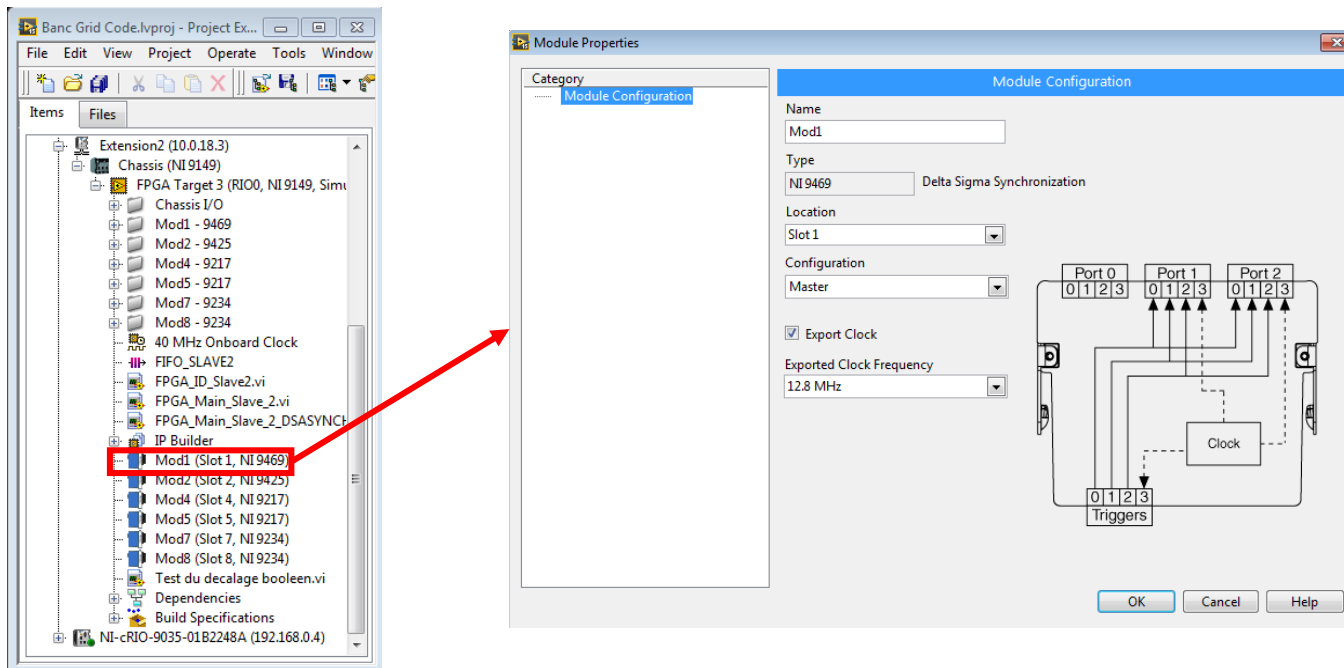
Synchronisation de plusieurs automates

Synchronisation de multiples châssis

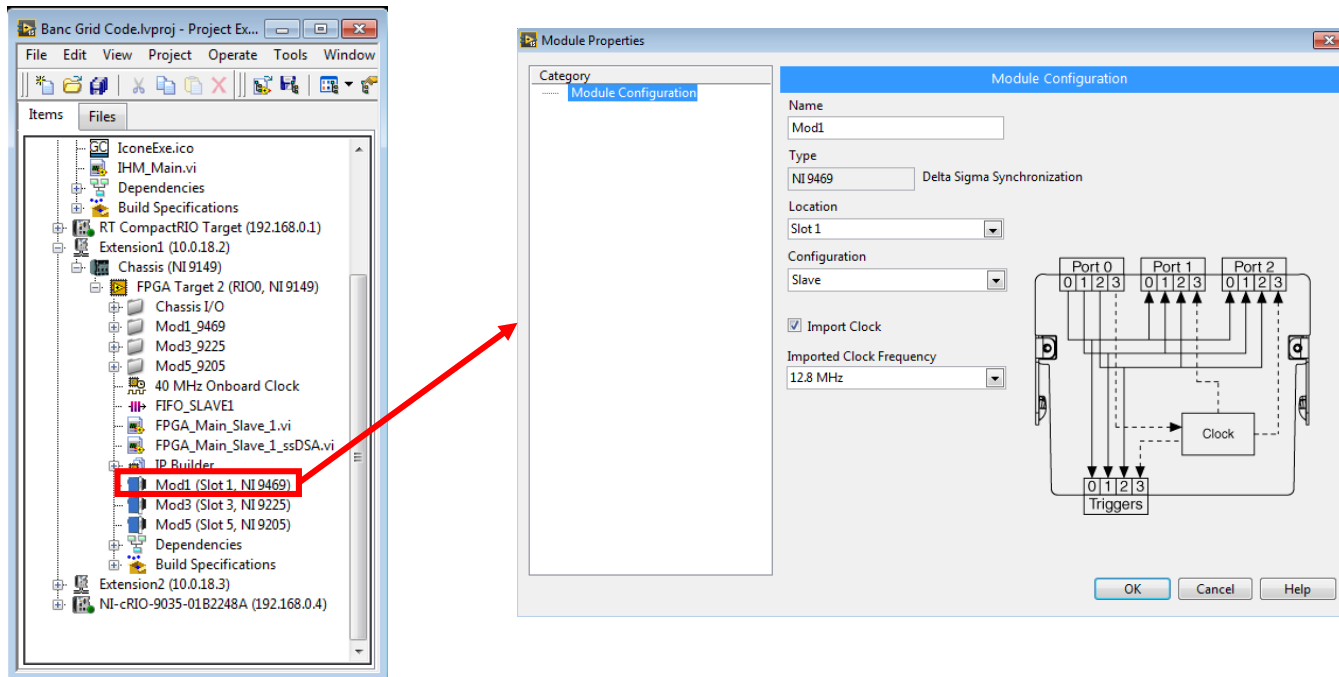
- Synchroniser l'horloge
- Synchroniser le top départ



Synchronisation du lancement des acquisitions

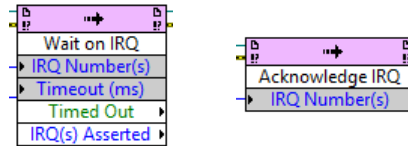


Synchronisation du lancement des acquisitions



Synchronisation du lancement des acquisitions

- Utilisation des IRQs (Interrupt Request)
- Côté RT, utilisation de nœuds de méthode FPGA



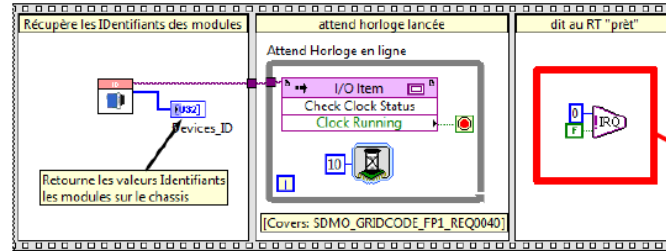
- Côté FPGA, utilisation de VI « Interrupt »



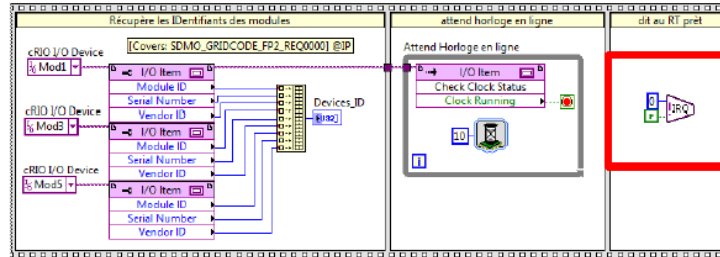
- Ouvrir le projet LabVIEW et analyser le code

Synchronisation IRQ – FPGA et RT

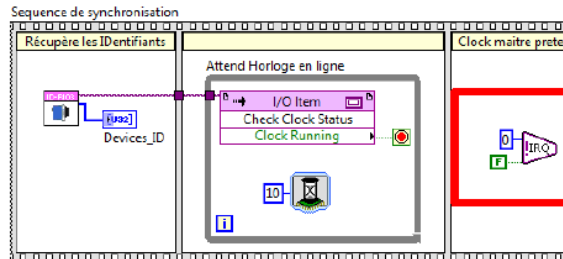
FPGA 1 – châssis maître
avec module de
synchronisation esclave



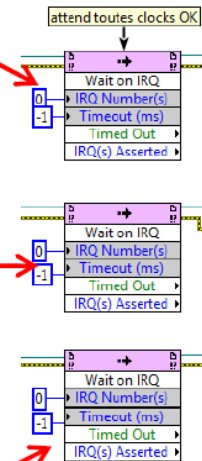
FPGA 2 – châssis
d'extension avec module
de synchronisation esclave



FPGA 3 – châssis
d'extension avec module
de synchronisation maître



Partie hôte – Temps
réel compactRIO
Maître



Synchronisation – autres moyens

- Serveur NTP -> 10ms
- Synchronisation GPS -> 100ns (pas de fil)
- IRQ et 9469 -> 4,98ns/m de cable

Conclusion

A retenir

- Définir les besoins de sécurité du système final en amont de développement
- Intervenir sur les 4 niveaux de sécurité en parallèle
- Si besoin, choisir une méthode de synchronisation adaptée à la précision recherchée.

SELinux – <http://www.ni.com/white-paper/52729/en/>
Exploits sur Linux - <https://www.scmagazine.com/linux-malware-gaining-favor-among-cybercriminals/article/671935/>

Questions ?

Jean-philippe.braud@phalanx.fr

06 87 45 15 77

Restez **connectés** pendant et après NIDays



ni.com/communaute-francophone



facebook.com/nifrance



twitter.com/nifrance



youtube.com/nifrance