Secure PLC Coding Practices: Top 20 List

Version 1.0 (15 June 2021)

PLC Security TOP 20 LIST

1. جعل كود ال **PLC** نمطيا

قسِّم كود PLC إلى وحدات ، باستخدام مجموعات وظيفية مختلفة (إجراءات فرعية). ثم اختبر الوحدات بشكل مستقل.

2. تتبع أوضاع التشغيل

احتفظ بـ PLC في وضع RUN. إذا لم تكن PLCs في وضع RUN ، فيجب أن يكون هناك إنذار للمشغلين.

3. اترك المنطق التشغيلي في **PLC** حيثما كان ذلك ممكنًا

اترك أكبر قدر ممكن من المنطق التشغيلي ، على سبيل المثال ، التجميع أو التكامل ، بقدر الإمكان في ال **PLC**. لا يحصل **HMI** على تحديثات كافية للقيام بذلك بشكل جيد.

4. استخدم علامات **PLC** للتحقق من النزاهة

ضع عدادات على إشارات خطأ **PLC** لالتقاط أي مشاكل حسابية.

5. استخدم فحوصات التشفير و / أو سلامة المجموع الاختباري لكود **PLC**

استخدم تجزئات التشفير ، أو المجاميع الاختبارية إذا كانت تجزئات التشفير غير متوفرة ، للتحقق من سلامة كود **PLC** وإصدار إنذار عند تغييرها.

6. تحقق من الموقتات والعدادات

إذا تمت كتابة قيم العدادات والعدادات في برنامج **PLC** ، فيجب التحقق من صحتها من قبل **PLC** للتأكد من معقوليتها والتحقق من الأعداد السابقة هل هي تحت الصفر.

7. تحقق من صحة المدخلات / المخرجات المزدوجه وتنبيهها

إذا كانت لديك إشارات مزدوجه ، فتأكد من عدم تأكيد كلتا الإشارتين معًا. إنذار المشغل عندما تحدث حالات الإدخال / الإخراج غير ممكنه علي ارض الواقع. ضع في اعتبارك جعل الإشارات المزدوجه مستقلة أو إضافة مؤقتات تأخير عندما يكون تبديل اشارات الخرج يسبب ضرر للمشغلات.

8. تحقق من صحة متغيرات إدخال **HMI** على مستوى **PLC** ، وليس فقط في **HMI**

يمكن (ويجب) تقييد وصول **HMI** إلى متغيرات **PLC** إلى نطاق قيمة تشغيلية مقبوله في **HMI** ، ولكن يجب إضافة المزيد من عمليات التحقق ايضا في **PLC** لمنع أو تنبيه القيم خارج النطاقات المقبولة التي تمت برمجتها في **HMI.**

9 . التحقق من ال **indirections**

تحقق من صحة **indirections** عن طريق تسميم نهايات المصفوفة و ذلك لمعرفه **fence-post errors**.

10 . تعيين **register blocks** محدده علي حسب الوظيفة (قراءة / كتابة / التحقق من الصحة)

قم بتعيين register blocks معينة لوظائف محددة من أجل التحقق من صحة البيانات ، وتجنب تدفقات المخزن المؤقت ومنع عمليات الكتابة الخارجية غير المصرح بها لبيانات وحدة التحكم المحميه.

11. أداة للتحقق من المعقولية

ادر العملية بطريقة تسمح بفحوصات المعقولية عن طريق التحقق من القياسات المختلفة.

12. التحقق من صحة المدخلات على أساس المعقولية المادية

تأكد من أن المشغلين يمكنهم فقط إدخال ما هو عملي أو ممكن ماديًا في العملية. اضبط مؤقتًا لعملية ما على المدة التي يجب أن تستغرقها فعليًا. ضع في اعتبارك التنبيه عند وجود انحرافات. تنبيه أيضًا عندما يكون هناك خمول غير متوقع.

13. تعطيل منافذ وبروتوكولات الاتصال غير الضرورية / غير المستخدمة

وحدات تحكم PLC ووحدات network interface تدعم بشكل عام بروتوكولات الاتصال المتعددة الممكنه افتراضيًا. قم بتعطيل المنافذ والبروتوكولات غير المطلوبة للتطبيق.

14._تقييد **third-party data interfaces**

تقييد نوع الاتصالات والبيانات المتاحة ل 3rd party interfaces يجب أن تكون الاتصالات و / أو واجهات البيانات محددة جيدًا ومقيدة للسماح فقط بقدرات القراءة / الكتابة لنقل البيانات المطلوبة.

15._حدد حالة عملية آمنة في حالة إعادة تشغيل **PLC**

حدد الحالات الآمنة للعملية في حالة إعادة تشغيل PLC (على سبيل المثال ، تنشيط جهات الاتصال ، وإلغاء تنشيطها ، والحفاظ على الحالة السابقة).

16._لخص أوقات دورات **PLC** واعرضها على **HMI**

لخص وقت دورة PLC كل 2-3 ثوانٍ وقدم تقريرًا إلى HMI لعرضها عن طريق الرسم البياني.

17._سجل وقت تشغيل **PLC** واعرضها على **HMI**

سجّل وقت تشغيل PLC لمعرفة وقت إعادة تشغيله. اعرض تسجيل وقت التشغيل على HMI وذلك للتشخيص.

18._ سجل توقفات **PLC** الطارئه واعرضها على **HMI**

قم بتخزين أحداث التوقف الطارئ لـ PLC من الأعطال أو عمليات الإغلاق لاسترجاعها بواسطة أنظمة إنذار HMI للتشاور قبل إعادة تشغيل PLC. مزامنة الوقت للحصول على بيانات أكثر دقة.

19. راقب استخدام ذاكرة **PLC** واعرضها على **HMI**

قم بقياس وتوفير baseline لاستخدام الذاكرة لكل وحدة تحكم منتشرة في بيئة الإنتاج واعرضها على HMI.

20. اعتراض السلبيات الزائفة والإيجابيات الزائفة للتنبيهات الحرجة

تحديد التنبيهات الهامة وبرمجة مصيدة لتلك التنبيهات. اضبط الملاءمة لمراقبة ظروف التشغيل وحالة التنبيه لأي انحراف.

About the Secure PLC Programming project

1. جعل كود ال **PLC** نمطيا

قسِّم كود **PLC** إلى وحدات ، باستخدام مجموعات وظيفية مختلفة (إجراءات فرعية). ثم اختبر الوحدات بشكل مستقل.

Security Objective	Target Group
Integrity of PLC logic	Product Supplier

التوجيه

لا تقم ببرمجة منطق PLC الكامل في مكان واحد ، على سبيل المثال ، في الكتلة التنظيمية الرئيسية أو الروتين الرئيسي. بدلاً من ذلك ، قم بتقسيمها إلى كتل وظيفية مختلفة (إجراءات فرعية) وراقب وقت تنفيذها وحجمها بالكيلو بايت.

قم بإنشاء مقاطع منفصلة للمنطق تعمل بشكل مستقل. يساعد هذا في التحقق من صحة الإدخال وإدارة التحكم في الوصول والتحقق من النزاهة وما إلى ذلك.

يسهل الكود المعياري أيضًا اختبار وتتبع نزاهة وحدات الكود. إذا تم اختبار الكود الموجود داخل الوحدة بدقة ، فيمكن التحقق من أي تعديلات على هذه الوحدات مقابل هاش الكود الأصلي ، على سبيل المثال ، عن طريق حفظ الهاش لكل من هذه الوحدات (عندما يكون هذا خيارًا في PLC). بهذه الطريقة ، يمكن التحقق من الوحدات أثناء FAT / SAT أو إذا كانت سلامة الكود موضع شك بعد وقوع حادث.

مثال

يتم فصل منطق التوربينات الغازية إلى "بدء التشغيل" و "التحكم في دوارات دليل المدخل" و "التحكم في صمام التسييل" وما إلى ذلك بحيث يمكنك تطبيق المنطق القياسي بشكل منهجي. يساعد هذا أيضًا في استكشاف الأخطاء وإصلاحها بسرعة إذا كان هناك حادث أمني.

يمكن إعادة استخدام كتل الوظائف المخصصة التي تم اختبارها بدقة دون تغيير (وتنبيهها في حالة إجراء محاولات تغيير) وقفلها ضد إساءة الاستخدام عن طري استخدام كلمة مرور / توقيع رقمي.

Why?

Beneficial for…?	Why?
Security	يسهل اكتشاف الأجزاء المضافة حديثًا من التعليمات البرمجية التي قد تكون ضارة. يساعد في توحيد المنطق والاتساق والتأمين ضد التعديلات غير المصرح بها.
Reliability	يساعد في التحكم في تسلسل تدفق البرنامج وتجنب الحلقات التي قد تتسبب في عدم استجابة المنطق بشكل صحيح أو تعطله.
Maintenance	الكود المعياري ليس فقط أسهل في التصحيح (يمكن اختبار الوحدات بشكل مستقل) ولكن أيضًا أسهل في الصيانة والتحديث. أيضًا ، يمكن استخدام هذه الوحدات في ال PLCs المختلفه ، مما يسمح باستخدام وتحديد الكود الشائع في الPLCs المختلفه . يمكن أن يساعد ذلك موظفي الصيانة في التعرف بسرعة على الوحدات الشائعة أثناء استكشاف الأخطاء وإصلاحها.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic:** TA002 - Execution **Technique:** T0844 - Program Organization Units
ISA 62443-3-3	**SR 3.4**: Software and information integrity
ISA 62443-4-2	**CR 3.4**: Software and information integrity
ISA 62443-4-1	**SI-2**: Secure coding standards
MITRE CWE	**CWE-1120:** Excessive Code Complexity **CWE-653:** Insufficient Compartmentalization

2. تتبع أوضاع التشغيل

احتفظ بـ **PLC** في وضع **RUN**. إذا لم تكن **PLCs** في وضع **RUN** ، فيجب أن يكون هناك إنذار للمشغلين.

Security Objective	Target Group
Integrity of PLC logic	Integration / Maintenance Service Provider Asset Owner

التوجيه

إذا لم تكن PLCs في وضع RUN (على سبيل المثال ، وضع PROGRAM) ، فيمكن تغيير كودها لتتبع وضع RUN. تحتوي بعض PLCs على checksum للتنبيه لتغييرات الكود ، ولكن إذا لم يحدث ذلك ، فهناك على الأقل مؤشر غير مباشر لمشكلة محتملة أثناء تتبع أوضاع التشغيل:

- إذا لم تكن PLCs في وضع RUN ، فيجب أن يكون هناك إنذار للمشغلين. إذا كانوا على علم بأنه من المفترض أن يعمل شخص ما على نظام التحكم ، فيمكنهم التعرف على الإنذار والمضي قدمًا.
- يجب ضبط ال HMI لإعادة تنبيه المشغل بنهاية الوردية حول وجود الإنذار. يجب أن يكون الهدف هو تتبع أي موظفين أو مقاولين في المصنع يقومون بعمل قد يؤثر على العملية.

حالة الاستثناء: إذا كان المصنع في مرحلة الاختبار أو التطوير ، ففكر في تعطيل هذا الإنذار ولكن يجب عزل المصنع عن المستويات الأعلى من الشبكة.

مثال

إذا لم يكن لدى PLC مفتاح لتغيير أوضاع التشغيل ، فمن المستحسن على الأقل استخدام آليات البرامج التي يمكن أن تقيد تغيير رمز PLC ، على سبيل المثال ، حماية كلمة المرور في البرامج الهندسية لقراءة وكتابة رمز PLC.

Why?

Beneficial for...?	Why?
Security	وضع التشغيل (تشغيل / تحرير / كتابة ؛ بالنسبة لـ Allen Bradley PLCs: RUN / PROGram / REMote) يحدد ما إذا كان يمكن العبث بـ PLC. إذا كان مفتاح التبديل في حالة REMote ، فمن الممكن تقنيًا إجراء تغييرات على برنامج PLC عبر واجهات الاتصال حتى إذا كان PLC قيد التشغيل.
Reliability	/
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA009 - Inhibit Response Function **Technique:** T0858 - Utilize/Change Operating Mode
ISA/IEC 62443-4-1	**SI-1** : Security implementation review

3. اترك المنطق التشغيلي في **PLC** حيثما كان ذلك ممكنًا

اترك أكبر قدر ممكن من المنطق التشغيلي ، على سبيل المثال ، التجميع أو التكامل ، بقدر الإمكان في ال **PLC**. لا يحصل **HMI** على تحديثات كافية للقيام بذلك بشكل جيد.

Security Objective	Target Group
Integrity of PLC logic	Product Supplier Integration / Maintenance Service Provider Asset Owner

التوجيه

توفر HMIs مستوى معينًا من إمكانات الكودينك ، والتي تهدف في الأصل إلى مساعدة المشغلين على تحسين التصور والإنذار ، والتي استخدمها بعض المبرمجين لإنشاء الكود كان يجب ان يكون في PLCال ليبقي كامل و قابل للتدقيق.

إن حساب القيم قريبا من الحقل قدر الإمكان يجعل هذه الحسابات أكثر دقة. لا يحصل HMI على تحديثات كافية للقيام بالتجميع / التكامل بشكل جيد. أيضًا ، هناك دائمًا زمن انتقال بين HMI و PLC. علاوة على ذلك ، عندما يكون الرمز في PLC ، ويتم إعادة تشغيل HMI ، يمكنه دائمًا تلقي المجموع / الاعداد من PLC.

على وجه الخصوص ، كود ال HMI يجب ان يتجنب أي شيء يتعلق بوظائف الأمان أو السلامة مثل المتشابك أو المؤقتات أو الحجوزات أو التصاريح.

لتحليل قيم بيانات العملية بمرور الوقت ، يعد مؤرخ بيانات العملية هو الخيار الأفضل من HMI. استخدم الاستعلامات في قاعدة بيانات مؤرخ العملية لمقارنة القيم الإجمالية (على مدى فترة ، على مدى دفعة ، عبر دورة عملية) مع الإجماليات المجمعة محليًا في منطق PLC. التنبيه اذا كان هنك اختلاف كبير في دقه البيانات لا يمكن تفسيره.

مثال

- كود لإنشاء شروط لتمكين / تعطيل الأزرار: يجب ان يكون التحكم في تمكين / تعطيل الإجراءات في طبقة PLC ، وإلا ، يمكن تنفيذ الإجراءات على HMI (أو من خلال الشبكة) في PLC ، على الرغم من عدم استيفائها الشروط (المقصوده).
- يجب عدم وضع الموقتات للسماح بإجراءات للمشغل (مؤقت التأخير لبدء تشغيل المحرك المتتالي ، الموقت للنظر في الصمامات مغلقة / مفتوحة أو توقف المحرك) في طبقة HMI ولكن في PLC الذي يحكم هذا المحرك / الصمام.
- يجب أن تكون عتبات الإنذارات جزءًا من أكواد PLC على الرغم من عرضها على HMIs.
- خزان المياه مع تغيير الكميه: يمكن لـ PLC الذي يتحكم في التدفق داخل وخارج الخزان بسهولة تجميع الكميه (والتحقق من صحة الإجماليات). يمكن لـ HMI القيام بذلك أيضًا ، ولكنها ستحتاج إلى الحصول على القيم من PLC أولاً. قد تحتاج هذه القيم إلى طوابع زمنية دقيقة من أجل الحصول على الإجماليات الصحيحة في حالة زمن الانتقال أو قد تفقد قيمًا في حالة إعادة تشغيل HMI.

Why?

Beneficial for...?	Why?
Security	1. يسمح بالاتساق في التحقق من تغييرات التعليمات البرمجية. يتمتع ترميز HMI بالتحكم في امكانيه تغييره بعيدا عن PLC ، بشكل عام ليس بنفس الدقة (خاصة في مرحلتي البناء والتشغيل) ، ولا يسمح لمالكي النظام بالحصول على رؤية كاملة وحتى فقدان الاعتبارات المهمة. لا تتضمن HMI "الإشارات القسرية" أو قوائم القيم المتغيرة مثل PLCs أو SCADAs ، لذلك يصعب اكتشاف تغييرات مستوى HMI ، ومن المستحيل عمليًا أن تكون جزءًا من خطة إدارة تغيير التفويض. 2. بالنسبة للمهاجم ، من الصعب التلاعب بالمجاميع الموزعة على العديد من PLCs من التلاعب بالمجاميع المحسوبة في HMI. 3. إذا لم يكن جزء من وظائف التمكين / التعطيل موجودًا في PLC ، فقد يتمكن المهاجمون من التلاعب ب PLC و I / O دون الحاجة إلى العمل علي جزء HMI لأن المعلومات المناسبة تم تعتيمها بالفعل على شاشة المشغل.

Beneficial for…?	Why?
Reliability	1. الحسابات تكون أكثر كفاءة ودقة إذا كانت أقرب إلى الحقل. أيضًا ، ستظل الإجماليات والأعداد متاحة في حالة إعادة تشغيل HMI (لا يتم إعادة تشغيل وحدات التحكم المنطقية القابلة للبرمجة كثيرًا وعادة ما تخزن هذه القيم في ذاكرة غير متطايرة). 2. مصادر مختلفة للمدخلات والتشابك قد يعني فشل غير متوقع. يمكن أن تكون هناك تقنيات مختلفة لـ HMIs في المصنع (طبقة SCADA ، ولكن أيضًا لوحات التحكم الميدانية) ، و التغييرات في واحدة منها سوف يفشل نشرها عبر بقية الطبقات ، مما يؤدي إلى تناقضات في التصور وفشل محتمل في التشغيل.
Maintenance	من السهل فهم الترميز ونقله من PLC إلى PLC ، وليس كثيرًا من HMIs إلى HMIs.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.6** : Deterministic Output
ISA 62443-4-2	**CR 3.6** : Deterministic Output

4. استخدم علامات **PLC** للتحقق من النزاهة

ضع عدادات على إشارات خطأ **PLC** لالتقاط أي مشاكل حسابية.

Security Objective	Target Group
Integrity of PLC logic	Product Supplier Integration / Maintenance Service Provider

التوجيه

إذا كان كود PLC يعمل بشكل جيد ولكن فجأة قام بالقسمة على الصفر ، فابحث. إذا كان هناك شيء ما يتصل بنظير إلى نظير من PLC آخر وتقوم الوظيفة / المنطق بالقسمة على الصفر عندما لم يكن ذلك متوقعًا ، فابحث

سيتجاهل معظم المبرمجين المشكلة على أنها خطأ حسابي أو ما هو أسوأ من ذلك ، قد يفترضون أن الكود الخاص بهم مثالي ويسمحون لـ PLC بالدخول في حالة خطأ صعب. أثناء تطوير الكود ، يحتاج المهندسون إلى اختبار وحدات التعليمات البرمجية الخاصة بهم والتحقق من صحتها (مقتطفات أو إجراءات) عن طريق إدخال البيانات خارج الحدود المتوقعة. قد يسمى هذا اختبار مستوى الوحدة.

قم بتعيين مقاطع ذاكرة مختلفة ومقفلة للبرامج الثابتة والمنطق والبروتوكول ستاك. اختبر البروتوكول استاك لحالات إساءة الاستخدام. يمكن أن تكون حالات إساءة الاستخدام شروط إشارة غير مألوفه في رأس الحزمة.

مثال

تعد أخطاء **PLC** الناتجة عن بيانات خارج الحدود شائعة جدًا. يحدث هذا ، على سبيل المثال ، عندما تتسبب قيمة الإدخال في خروج فهارس المصفوفه عن الحدود ، أو أجهزة ضبط الوقت ذات الإعدادات المسبقة السلبية ، أو القسمة على استثناءات صفرية.

ال **flags** المثيره للاهتمام

- القسمه علي صفر
- فائض العداد
- عداد سلبي أو مؤقت مسبق
- تجاوز فحص الإدخال / الإخراج

Why?

Beneficial for...?	Why?
Security	يمكن أن تشمل الهجمات على PLCs تغيير منطقها ، أو تنشيط برنامج جديد ، أو اختبار رمز جديد ، أو تحميل وصفة عملية جديدة ، أو إدخال منطق إضافي لإرسال الرسائل أو تنشيط بعض الميزات. نظرًا لأن معظم PLCs لا توفر فحوصات نزاهة التشفير ، يمكن أن تكون العلامات مؤشرًا جيدًا في حالة حدوث أحد التغييرات المنطقية المذكورة أعلاه.
Reliability	اخذ ال flags علي محمل الجد يمكن ان يجنبك تشغيل ال PLC مع أخطاء البرمجة أو الإدخال / الإخراج. أيضًا ، في حالة حدوث خطأ ، يكون مصدر الفشل أكثر وضوحًا.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic** : TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
ISA 62443-4-1	**SI-2**: Secure coding standards **SVV-1**: Security requirements testing
MITRE CWE	**CWE-128:** Wrap-around **CWE-190:** Integer Overflow **CWE-369:** Divide by Zero **CWE-754:** Improper Check for Unusual or Exceptional Conditions

5. استخدم فحوصات التشفير / أو سلامة المجموع الاختباري لكود PLC

استخدم تجزئات التشفير ، أو المجاميع الاختبارية إذا كانت تجزئات التشفير غير متوفرة ، للتحقق من سلامة كود PLC وإصدار إنذار عند تغييرها.

Security Objective	Target Group
Integrity of PLC logic	Product Supplier Integration / Maintenance Service Provider Asset Owner

التوجيه

A) Checksums

عندما تكون هاشات (التشفير) غير ممكنة ، فقد تكون المجاميع الاختبارية خيارًا. تقوم بعض **PLCs** بإنشاء مجموع اختباري فريد عند تنزيل الكود في أجهزة **PLC**. يجب توثيق المجموع الاختباري من قبل الشركة المصنعة / **integrator** بعد اختبار **SAT** ويكون جزءًا من شروط الضمان / الخدمة.

إذا لم تكن ميزة المجموع الاختباري متوفرة أصلاً في وحدة التحكم ، فيمكن أيضًا إنشاء ذلك في **EWS / HMI** والتحقق منه ، على سبيل المثال ، مرة واحدة يوميًا للمقارنة مع هاش الكود الأصلي في **PLC** للتحقق من مطابقتها. على الرغم من أن هذا لن يوفر تنبيهات في الوقت الفعلي ، إلا أنه جيد بما يكفي لتتبع ما إذا كان أي شخص يحاول إجراء تغييرات على رمز **PLC**.

يمكن أيضًا نقل قيمة المجموع الاختباري إلى سجل **PLC** وتهيئته للإنذار عندما يتغير ، ويمكن إرسال القيمة إلى المؤرخين وما إلى ذلك.

B) Hashes

لا تمتلك وحدات المعالجة المركزية PLC بشكل عام القدرة على المعالجة لإنشاء هاش أو التحقق منها أثناء التشغيل. قد تؤدي محاولة الهاش إلى تعطل PLC. لكن البرنامج الهندسي لـ PLC قد يكون قادرًا على حساب التجزئة من كود PLC وحفظها إما في PLC أو في مكان آخر في نظام التحكم.

مثال

بائعي **PLC** المعروفين بامتلاكهم ميزات المجموع الاختباري:

- Siemens (see example)
- Rockwell

أيضًا ، يمكن استخدام برامج خارجية لإنشاء مجاميع اختبارية:

- Version dog
- Asset Guardian
- PAS

مثال على تنفيذ شركة سيمنز

مثال لإنشاء مجاميع اختبارية في **Siemens S7-1500 PLC**:

يقرأ **GetChecksum-Function Block** المجموع الاختباري الفعلي وباستخدام برنامج نصي خفيف الوزن يمكن تخزين "**SAT-Checksum**" كمرجع. يمكن تخزين الانحراف عن المجموع الاختباري المرجعي باستخدام **Datalog-Function**.

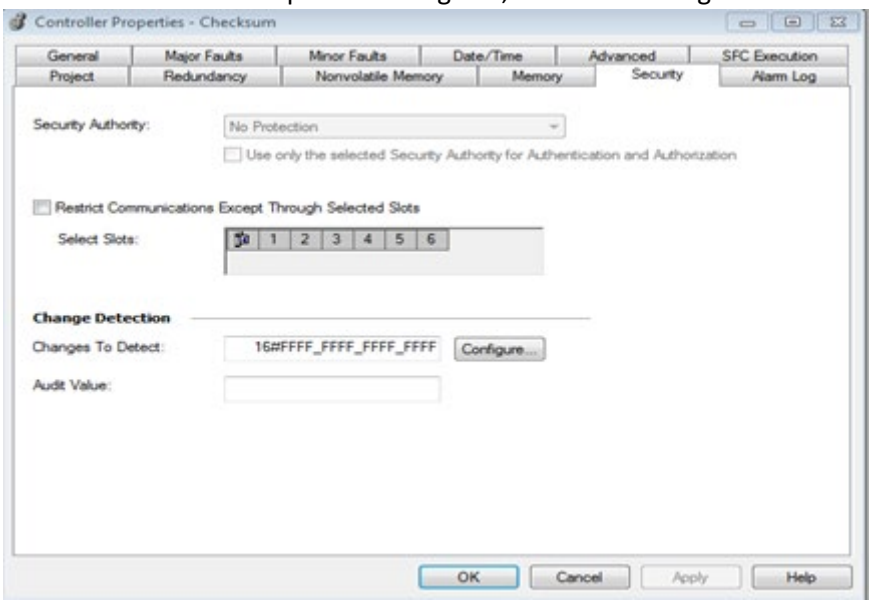
	Date	UTC Time	Referenz	Aktuell
1	11/21/2019	9:55:11	84 2A 76 DF 5B 31 F4 16	FF 2C EA 71 44 D7 81 04
2	11/21/2019	9:57:33	FF 2C EA 71 44 D7 81 04	FF 2C EA 71 44 D7 81 04
3	11/21/2019	9:58:17	FF 2C EA 71 44 D7 81 04	5B 7C 57 7E E2 3E EF C3
4	11/21/2019	9:58:36	FF 2C EA 71 44 D7 81 04	5B 7C 57 7E E2 3E EF C3
5	11/21/2019	9:58:44	5B 7C 57 7E E2 3E EF C3	5B 7C 57 7E E2 3E EF C3

مثال على تنفيذ **Rockwell**:

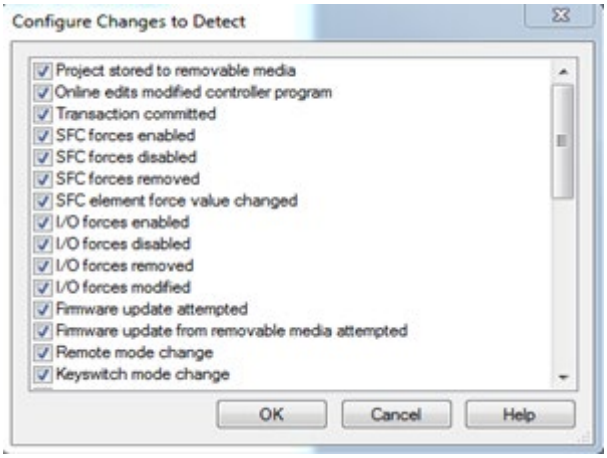
هذا مثال جزئي لكيفية تطوير المنظمة لمستوى من القدرة على اكتشاف التغيير في برنامج ال PLC داخل بيئة ال ICS الخاصة بهم. هذا المثال خصيصًا لـ Rockwell Automation ControlLogix PLC وهو غير كامل؛ ومع ذلك ، فإنه يوضح كيفية استرداد حالة معالج PLC في سجل داخل PLC. بمجرد التسجيل في PLC ، يمكن للمؤسسة استخدامه لإنشاء إنذار configuration changللعرض على HMI ، أو نقل معلومات الحالة الأولية إلى HMI للاتجاه والمراقبة ، أو إرسالها إلى مؤرخ لمعرفتها على المدى الطويل.

توفر هذه الممارسة فرصة ، باستخدام الأدوات والقدرات الحالية ، لاكتساب الوعي الظرفي وذلك عندما تتغير الأصول السيبرانية الهامة. الأمر متروك للمؤسسة لإكمال استخدام هذا المثال بطريقة تعمل بشكل أفضل في بيئتها.

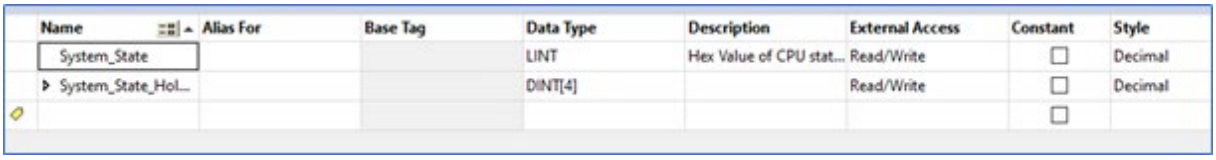
1. From the Controller Properties Dialog Box, select the configure button on “Change to Detect”



2. Within the selection window, choose all items to be monitored

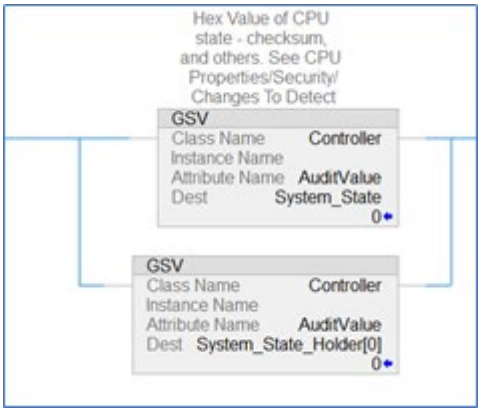


3. Create a Tag to receive the processor state information. This tag can be of type “LINT” or a 2-word array of type “DINT”



Name	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
System_State			LINT	Hex Value of CPU stat...	Read/Write	☐	Decimal
System_State_Hol...			DINT[4]		Read/Write	☐	Decimal
						☐	

4. Use the Get System Values (GSV) instruction to get the processor state information from memory and move it into a Tag that can be used in logic or read at the HMI



Why?

Beneficial for...?	Why?
Security	إن معرفة ما إذا كان قد تم العبث برمز PLC أمر ضروري لملاحظة الاختراق والتحقق مما إذا كان PLC آمنًا للعمل بعد الاختراق المحتمل.
Reliability	يمكن أيضًا أن تكون Hashes او checksums وسيلة للتحقق مما إذا كان) PLC لا يزال) يعمل بكود معتمد من قبل شركة ال integrator / الشركة المصنعة.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA002 - Execution, TA010 - Impair Process Control **Technique:** T0873 - Project File Infection, T0833 - Modify Control Logic
ISA 62443-3-3	**SR 3.4** : Software and information integrity

Standard / framework	Mapping
ISA 62443-4-2	**CR 3.4** : Software and information integrity **EDR 3.12** : Provisioning product supplier roots of trust
ISA 62443-4-1	**SI-1** : Security implementation review **SVV-1** Security requirements testing
MITRE CWE	**CWE-345:** Insufficient Verification of Data Authenticity • **(child) CWE-353:** Missing Support for Integrity Check • **(child) CWE-354:** Improper Validation of Integrity Check Value

6. تحقق من الموقتات والعدادات

إذا تمت كتابة قيم العدادات والعدادات في برنامج **PLC** ، فيجب التحقق من صحتها من قبل **PLC** للتأكد من معقوليتها والتحقق من الأعداد السابقة هل هي تحت الصفر.

Security Objective	Target Group
Integrity of PLC variables	Integration / Maintenance Service Provider Asset Owner

التوجيه

يمكن ضبط المؤقتات والعدادات تقنيًا مسبقًا على أي قيمة. لذلك ، يجب تقييد النطاق الصالح للتعيين المسبق لمؤقت أو عداد لتلبية متطلبات التشغيل.

إذا كانت الأجهزة البعيدة مثل HMI تكتب قيم المؤقتات أو العدادت لبرنامج:

- لا تدع HMI يكتب إلى المؤقت أو العداد مباشرة ولكن انتقل من خلال منطق التحقق من الصحة
- التحقق من صحة الإعدادات المسبقة وقيم المهلة في PLC

من السهل إجراء التحقق من الموقت ومدخلات العداد مباشرة في PLC (دون الحاجة إلى أي جهاز شبكة قادر على فحص الحزمة العميق) ، حيث أن PLC "يعرف" حالة العملية أو سياقها. يمكنه التحقق من "ما" يحصل و "متى" يحصل على الأوامر أو نقاط الضبط.

مثال

أثناء بدء تشغيل PLC ، عادة ما يتم ضبط المؤقتات والعدادات مسبقًا على قيم معينة.

إذا كان هناك مؤقت يطلق الإنذارات في 1.3 ثانية ، ولكن هذا المؤقت مضبوط مسبقًا بشكل ضار على 5 دقائق ، فقد لا يطلق الإنذار.

إذا كان هناك عداد يتسبب في توقف العملية عندما تصل إلى 10000 ولكن تم تعيينها على 11000 من البداية ، فقد لا تتوقف العملية.

Why?

Beneficial for...?	Why?
Security	إذا تمت كتابة الإدخال / الإخراج أو المؤقتات أو الإعدادات المسبقة مباشرةً إلى الإدخال / الإخراج ، ولم يتم التحقق من صحتها بواسطة PLC ، فسيتم التهرب من طبقة التحقق من الصحة لي الPLC ويتم تعيين HMI (أو أجهزة الشبكة الأخرى) على مستوى غير مبرر من الثقة.
Reliability	يمكن لـ PLC أيضًا التحقق من الصحة عندما يقوم المشغل عن طريق الخطأ بضبط مؤقت أو قيم عداد سيئة.
Maintenance	قد يساعد توثيق النطاقات الصالحة لأجهزة ضبط الوقت والعدادات والتحقق من صحتها تلقائيًا عند تحديث المنطق.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic** : TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.5** : Input Validation
ISA 62443-4-2	**CR 3.5** : Input Validation
ISA 62443-4-1	**SI-2** : Secure coding standards **SVV-1** : Security requirements testing

7. تحقق من صحة المدخلات / المخرجات المزدوجه وتنبيهها

إذا كانت لديك إشارات مزدوجه ، فتأكد من عدم تأكيد كلتا الإشارتين معًا. إنذار المشغل عندما تحدث حالات الإدخال / الإخراج غير ممكنه علي ارض الواقع. ضع في اعتبارك جعل الإشارات المزدوجه مستقلة أو إضافة مؤقتات تأخير عندما يكون تبديل اشارات الخرج يسبب ضرر للمشغلات.

Security Objective	Target Group
Integrity of PLC variables Resilience	Product Supplier Integration / Maintenance Service Provider

التوجيه

المدخلات أو المخرجات المزدوجة هي تلك التي لا يمكن أن تحدث فعليًا في نفس الوقت ؛ هم حصريون. على الرغم من أنه لا يمكن تأكيد الإشارات المقترنة في نفس الوقت ما لم يكن هناك فشل أو نشاط ضار ، فإن مبرمجي PLC غالبًا لا يمنعون هذا التأكيد من الحدوث.

من الأسهل إجراء التحقق مباشرة في PLC ، لأن PLC على دراية بحالة العملية أو سياقها. يسهل التعرف على الإشارات المقترنة وتتبعها إذا كانت لها عناوين متسلسلة (على سبيل المثال ، الإدخال 1 والمدخل 2).

سيناريو آخر حيث يمكن أن تتسبب المدخلات أو المخرجات المزدوجة في حدوث مشكلات عندما لا يتم تأكيدها في نفس الوقت ، ولكن يتم تبديلها بسرعة بطريقة تلحق الضرر بالمشغلات.

مثال

أمثلة على الإشارات المزدوجه :

- START and STOP
- التشغيل والإيقاف المستقلان: قم بتكوين البدء والإيقاف كمخرجات منفصلة بدلاً من وجود مخرج واحد يمكنه عمل التشغيل / إلايقاف. حسب التصميم ، لا يسمح هذا بالمشغلات المتزامنة. بالنسبة للمهاجم ، من الأكثر تعقيدًا التبديل بين التشغيل / الإيقاف السريع إذا كان لابد من ضبط خرجين مختلفين.
- Timer لإعادة التشغيل: ضع في اعتبارك أيضًا إضافة مؤقت لإعادة التشغيل بعد إصدار التوقف لتجنب التبديل السريع لإشارات البدء / الإيقاف.
- FORWARD and REVERSE
- OPEN and CLOSE

أمثلة على تبديل الإشارات المقترنة التي قد تكون ضارة:

اذا قبل PLC / MCC إدخالًا منفصلاً ، فإن هذا يوفر خيارًا سهلاً للمهاجم لإحداث ضرر مادي بالمشغلات. قد يكون السيناريو المعروف لتبديل المخرجات لإحداث ضرر هو MCC ، ولكن هذه الممارسة تنطبق على جميع السيناريوهات التي قد يؤدي فيها تبديل النواتج إلى إتلاف. كان اختبار Aurora Generator في عام 2007 الذي أجراه مختبر أيداهو الوطني دليلًا على المفهوم الذي يمكن أن يتسبب فيه التبديل السريع للمخرجات في حدوث ضرر حقيقي ، حيث تسبب تبديل المخرجات غير المتزامنة في تلف قاطع الدائرة.

Why?

Beneficial for…?	Why?
Security	1. إذا لم تأخذ برامج ال PLC في الحسبان ما سيحدث إذا تم التأكيد على كلتا إشارتَي الإدخال المقترنين في نفس الوقت ، فإن هذا يمثل عاملا جيدًا للهجوم. 2. يتم التأكيد على كلتا إشارتا الإدخال المقترنة بالتحذير من وجود خطأ تشغيلي أو خطأ في البرمجة أو حدوث شيء خبيث. 3. هذا يتجنب سيناريو الهجوم حيث يمكن أن يحدث ضرر مادي للمشغلات.
Reliability	1. 1. يمكن أن تشير إشارات الإدخال المقترنة إلى عطل جهاز الاستشعار أو سوء توصيله أو أن هناك مشكلة ميكانيكية مثل مفتاح عالق. 2. يمكن أيضًا التبديل السريع بين البدء والإيقاف عن طريق الخطأ ، لذلك يمنع هذا أيضًا الضرر الذي قد يحدث بدون قصد.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter, T0806 - Brute Force I/O
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
ISA 62443-4-1	**SI-2**: Secure coding standards **SVV-1**: Security requirements testing
MITRE CWE	**CWE-754:** Improper Check for Unusual or Exceptional Conditions

8. تحقق من صحة متغيرات إدخال **HMI** على مستوى **PLC** ، وليس فقط في **HMI**

يمكن (ويجب) تقييد وصول **HMI** إلى متغيرات **PLC** إلى نطاق قيمة تشغيلية مقبوله في **HMI** ، ولكن يجب إضافة المزيد من عمليات التحقق ايضا في **PLC** لمنع أو تنبيه القيم خارج النطاقات المقبولة التي تمت برمجتها في **HMI**.

Security Objective	Target Group
Integrity of PLC variables	Product Supplier Integration / Maintenance Service Provider

التوجيه

يمكن أن يتضمن التحقق من صحة المدخلات عمليات فحص خارج الحدود للقيم التشغيلية الصالحة بالإضافة إلى القيم الصالحة من حيث أنواع البيانات المتعلقة بالعملية.

إذا تلقى متغير في PLC قيمة خارج الحدود ، فقم بتوفير منطق PLC لأي منهما

- أدخل قيمة افتراضية لهذا المتغير والتي لا تؤثر سلبًا على العملية ، ويمكن استخدامها كعلامة للتنبيهات ، أو
- أدخل آخر قيمة صحيحة لتلك القيمة وقم بتسجيل الحدث لمزيد من التحليل.

مثال

مثال 1

تتطلب العملية من المستخدم إدخال قيمة على **HMI** لضغط الصمام. النطاقات الصالحة لهذه العملية هي 0-100 ، ويتم تمرير مدخلات المستخدم من وظيفة إدخال المستخدم على **HMI** إلى متغير **V1** في **PLC**. في هذه الحالة،

1. مدخل HMI للمتغير V1 له نطاق محدود من 0-100 (ديسمل) مبرمج في HMI.
2. لدى PLC منطق تحقق ايضا ينص على ما يلي:

```
IF V1 < 0 OR IF V1 > 100, SET V1 = 0.
```

يوفر هذا استجابة إيجابية لقيمة مفترضة آمنة لإدخال غير صالح لهذا المتغير.

مثال 2

تتطلب العملية إدخال المستخدم لعتبات القياس إلى متغير يجب أن يكون دائمًا ضمن نطاق بيانات **INT2**. يتم تمرير مدخلات المستخدم من **HMI** إلى متغير **V2** في **PLC** ، وهو سجل بيانات 16 بت.

1. إدخال HMI إلى المتغير V2 له نطاق محدود من -32768 إلى 32767 (ديسمبر) مبرمجًا في HMI
2. يحتوي PLC على منطق تحقق ايضا من نوع البيانات يراقب متغير الفائض (V3) ، والذي يوجد بعد V2 مباشرةً في هيكل ذاكرة PLC:

```
IF V2 = -32768 OR IF V2 = 32767 AND V3 != 0,

SET V2 = 0 AND SET V3 = 0 AND SET DataTypeOverflowAlarm = TRUE.
```

مثال 3

مقياس **PV** (قيمة العملية) و **SP** (نقطة الضبط) و **CV** (متغير التحكم) لـ **PID** (وحدة تحكم متناسبة أو متكاملة أو مشتقة) إلى وحدات متسقة أو أولية لإزالة أخطاء القياس التي تسبب مشكلة التحكم. قد يؤدي القياس غير الصحيح إلى حالات إساءة استخدام غير مقصودة.

Why?

Beneficial for…?	Why?
Security	1. بينما توفر HMIs عادةً نوعًا من التحقق من صحة الإدخال ، يمكن للمهاجم صياغة أو إعادة تشغيل الحزم المعدلة لإرسال قيم عشوائية إلى المتغيرات في PLC والتي تكون مفتوحة للتأثير الخارجي (مفتوحة للقيم التي تم تمريرها من HMI ، على سبيل المثال). 2. يتم تسويق بروتوكولات PLC عادةً على أنها بروتوكولات "مفتوحة" ويتم نشرها لعامة الناس ، لذا فإن إنشاء برامج ضارة تستخدم معلومات البروتوكول "المفتوحة" يمكن أن يكون تطويره امرا بسيطا. يمكن أن يحدث ال PLC variable mapping عادةً من خلال تحليل حركة المرور أثناء مراحل الاستطلاع للهجوم ، وبالتالي تزويد الدخيل بالمعلومات الضرورية لإنشاء حركة مرور ضارة إلى الهدف وبالتالي التلاعب بالعمليه بأدوات غير مصرح بها. تضمن قيم التدقيق الاضافيه التي تم تمريرها إلى PLC قبل تنفيذ تلك البيانات في العملية يجب التاكد من نطاقات البيانات الصالحة والتقليل من القيم غير الصالحة في مواقع الذاكرة هذه عن طريق تعيين نطاقات آمنة قسريًا عند اكتشاف قيمة خارج الحدود أثناء ال PLC scan.
Reliability	/
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
ISA 62443-4-1	**SI-2**: Secure coding standards **SVV-1**: Security requirements testing
MITRE CWE	**CWE-1320:** Improper Protection for Out of Bounds Signal Level Alerts

9. التحقق من ال **indirections**

تحقق من صحة **indirections** عن طريق تسميم نهايات المصفوفة و ذلك لمعرفه **fence-post errors**.

Security Objective	Target Group
Integrity of PLC variables	Product Supplier Integration / Maintenance Service Provider

التوجيه

indirection هي استخدام قيمة سجل في سجل آخر. هناك العديد من الأسباب لاستخدام indirections.

أمثلة على indirections الضرورية هي:

- محركات التردد المتغير (VFDs) التي تطلق إجراءات مختلفة للترددات المختلفة باستخدام جداول البحث.
- لتحديد المضخة التي سيتم تشغيلها أولاً بناءً على أوقات التشغيل الحالية.

لا تحتوي PLCs عادةً على علامة "نهاية المصفوفة" ، لذا من الجيد إنشائها في البرنامج ؛ الهدف هو تجنب عمليات PLC غير العادية / غير المخطط لها.

مثال

Instruction List (IL) Programming
يمكن تحويل النهج إلى عدد قليل من الكتل الوظيفية وربما حتى إعادة استخدامه لتطبيقات أخرى.

1. **Create array mask**

Check if the array is binary-sized. If it is not binary-sized, create a mask to the next size up on a binary scale. e.g., if you have a need for 5 registers (not binary-sized):

```
[21  31  41  51  61]
```

define an array of 8:

```
[x  x  21  31  41  51  61  x]
```

Next, take the index value to pick up for the indirection - in this example, it is 3.

Caveat: Index begins at 0!

```
[21  31  41  51  61]
          ^
```

Index: 3

add an offset to it making up for the poisoned end. The offset can be 1 or higher, in this case it is 2:

```
[x  x  21  31  41  51  61  x]
              ^
```

Index including offset: 3 + 2 = 5

and then AND the index including offset with a mask that equals the array size.
In this example the array size is 8, thus index 7, so the mask would be 0x07. The mask makes sure the maximum index you can get is 7, for example:

`6 AND 0x07` would give back 6.
`7 AND 0x07` would give back 7
`8 AND 0x07` would give back 0.
`9 AND 0x07` would give back 1.

This ensures you always address a value in the array.

2. Insert poisoned ends

Poisoning ends is optional. You would be able to detect manipulated indirections without the poisoning, but poisoning helps to catch fence-post errors because you get back a value that does not make sense.

The point is that at index 0 of the array, there should be a value that is invalid – such as -1 or 65535. This is "the poisoned end". Likewise, at the last elements of the array you do the same:

So, for the array above, the poisoned version could look like this:

```
[-1 -1 21 31 41 51 61 -1]
```

3. Record value of indirection address without mask

Then record the value of the indirect address without AND mask and offset:
In this example, you'd record 51 for index 3.

```
[21 31 41 51 61]
          ^
__________
______Index 3
```

4. Execute AND mask and compare values (=indirection validation)

Compare your recorded value to the value after you have done the offset and the AND mask.

4a. Case A: Correct Indirection

First, offset:
Index + Offset = 3 + 2 = 5

Second, mask:
`5 AND 0x07 = 5`

Third, indirection check:

```
[-1 -1 21 31 41 51 61 -1]
                ^
________________
```

Index including offset: `5`
`Value = 51` equals the recorded value, so everything is fine.

4b. Case B: Manipulated Indirection

If you now had a manipulated indirection, let's say 7, let us see what happens:

First, offset:
`Index + Offset = 7 + 2 = 9`

Second, mask:
`9 AND 0x07 = 1`

Third, indirection check:
`[-1 -1 21 31 41 51 61 -1]`
`_____^`

Index including offset: **1**
`Value = -1` does not equal the recorded value and also indicates your poisoned end, so you'd know your indirection is manipulated.

5. **Execute fault / programmer alert**

If this validated value is different from your recorded one, then you know something is wrong. Raise a software quality alarm.

Then, check the indirection value. If it is a poisoned value, you should raise another software quality alarm. This is an indication of a fence-post error.

Why?

Beneficial for…?	Why?
Security	لا تحتوي معظم PLCs على أي ميزة للتعامل مع مؤشرات خارج الحدود للمصفوفات. هناك سيناريوهان يحتمل أن يكونا خطرين يمكن أن ينبعان من أخطاء indirection: أولاً ، إذا أدت ال indirection إلى القراءة من السجل الخاطئ ، فسيتم تنفيذ البرنامج باستخدام قيم خاطئة. ثانيًا ، إذا أدى الindirection الخاطئ إلى الكتابة إلى السجل الخاطئ ، يقوم البرنامج بالكتابة فوق الكود أو القيم التي تريد الاحتفاظ بها. في كلتا الحالتين ، قد يكون من الصعب اكتشاف أخطاء الindirection ويمكن أن يكون لها تأثيرات خطيرة. يمكن أن تكون ناجمة عن خطأ بشري ولكن أيضًا يتم إدراجها بشكل ضار.
Reliability	يحدد الأخطاء البشرية غير الضارة في البرمجة.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
ISA 62443-4-1	**SI-2**: Secure coding standards **SVV-1**: Security requirements testing
MITRE CWE	**CWE-129:** Improper Validation of Array Index

10. تعيين **register blocks** محدده علي حسب الوظيفة (قراءة / كتابة / التحقق من الصحة)

قم بتعيين register blocks معينة لوظائف محددة من أجل التحقق من صحة البيانات ، وتجنب تدفقات المخزن المؤقت ومنع عمليات الكتابة الخارجية غير المصرح بها لبيانات وحدة التحكم المحميه.

Security Objective	Target Group
Integrity of PLC variables	Product Supplier Integration / Maintenance Service Provider

التوجيه

الذاكرة المؤقتة ، والمعروفة أيضًا باسم ذاكرة لوحة التخزين ، هي منطقة يسهل استغلالها في الذاكرة إذا لم يتم اتباع هذه الممارسة. على سبيل المثال ، قد يؤدي مجرد الكتابة إلى سجل "Modbus" خارج الحدود إلى الكتابة فوق سجلات الذاكرة المستخدمة في العمليات الحسابية المؤقتة.

بشكل عام ، يمكن الوصول إلى ذاكرة التسجيل بواسطة الأجهزة الأخرى عبر شبكة PLC لعمليات القراءة والكتابة. يمكن قراءة بعض السجلات بواسطة HMI ، ويمكن كتابة البعض الآخر بواسطة نظام SCADA وما إلى ذلك. كما أن وجود مصفوفات سجل محددة لتطبيق معين يجعل من السهل أيضًا (في وحدة التحكم أو يتم استخدام جدار حماية خارجي) لضبط الوصول للقراءة فقط من اي جهاز / HMI.

أمثلة على الوظائف التي تكون كتل التسجيل المعينة منطقية لها هي:

- قراءة
- الكتابة (من HMI / جهاز التحكم / جهاز خارجي آخر)
- التحقق من صحة الكتابة
- العمليات الحسابية

يساعد ضمان عمليات الكتابة الخارجية للسجلات المسموح بها أيضًا في تجنب أخطاء إعادة تعيين الذاكرة الرئيسية إما بسبب التنفيذ خارج النطاق أو المحاولات الخبيثة. يمكن استخدام كتل التسجيل المعينة هذه كمخازن مؤقتة لعمليات الإدخال / الإخراج ، والمؤقت ، وكتب العداد من خلال التحقق من أن المخزن المؤقت مكتوب بالكامل (لا يحتوي على بيانات قديمة وجزئية جديدة) والتحقق من صحة جميع البيانات الموجودة في المخزن المؤقت.

خلفية:

يتم استخدام الذاكرة الرئيسية وذاكرة التسجيل بشكل مختلف. تُستخدم الذاكرة الرئيسية لتخزين منطق البرنامج المنفذ حاليًا بينما يتم استخدام ذاكرة التسجيل كذاكرة مؤقتة بواسطة المنطق المنفذ حاليًا. على الرغم من أن ذاكرة التسجيل هي ذاكرة مؤقتة ، نظرًا لاستخدامها من قبل المنطق التنفيذي ، فمن المؤكد أنها تحتوي على بعض المتغيرات المهمة التي قد تؤثر على المنطق الرئيسي.

مثال

أمثلة لما يمكن أن يحدث إذا لم يتم تنفيذ هذه الممارسة:
(*Reference: G. P. H. Sandaruwan, P. S. Ranaweera, Vladimir A. Oleshchuk, PLC Security and Critical Infrastructure Protection):*

- تستخدم شركة Siemens عادةً ذاكرة التخزين المؤقت في منطقة العلم بدءًا من العلم 200.0 وحتى العلامة 255.7. إذا تم تغيير جزء صغير في هذه المنطقة ، فهناك احتمال لحدوث عطل خطير في PLC بناءً على أهمية ذلك البت أو البايت.
- افترض أن المهاجم يمكنه الوصول إلى أحد الأجهزة في شبكة PLC وإصابة هذا الجهاز بدودة قادرة على كتابة قيم عشوائية في ذاكرة التسجيل. نظرًا لأن قيم ذاكرة التسجيل تغيرت بشكل تعسفي ، فيمكنها تغيير قيمة الضغط.
- تنفيذ المنطق سيحدد قيمة جديدة بناءً على التغيير وقد يتسبب ذلك في تجاوز النظام هوامش أمانه وربما دفعه إلى الفشل.

أمثلة على تنفيذ هذه الممارسة:

- في حالة وجود منطقة أمان (ولكن يمكن لـ DCS قراءتها) ، يمكن لجدار الحماية تسجيل أي محاولات "كتابة" بقاعدة أن هذه السجلات للقراءة فقط في منطقة الأمان.

- في سيناريو آخر ، يمكن أن يكون هناك بعض السجلات القابلة للكتابة ، والبعض الآخر للقراءة فقط ، ولكن وجود جميع السجلات للقراءة فقط في مصفوفة واحدة يسهل تكوينها في وحدة التحكم (أو جدار الحماية).

Why?

Beneficial for…?	Why?
Security	يجعل من السهل حماية بيانات وحدة التحكم حسب الوظيفة (قراءة / كتابة / التحقق من الصحة). تسهل على جدران الحماية الحساسة للبروتوكول القيام بعملها: تصبح القواعد أبسط لأنه من الواضح جدًا ما هي كتل التسجيل المسموح ل HMI للوصول إليها. يسهل إدارة القواعد (الأبسط) في جدار الحماية. يعد إجراء تغييرات غير مصرح بها على الذاكرة الداخلية المؤقتة ثغرة أمنية يمكن استغلالها بسهولة (By-pass Logic Attack). عندما يتم التحقق من صحة المدخلات والمخرجات إلى PLC routines بشكل صحيح ، يمكن اكتشاف أي تغييرات (من قبل فاعل ضار أو عن طريق الخطأ) بسهولة بدلاً من البقاء في التسلسل المنطقي لفترة طويلة وإلقاء الأخطاء / التسبب في حدوث مشكلات لاحقًا في التنفيذ.
Reliability	يجعل القراءة والكتابة أسرع لأن عدد المعاملات يتم تقليله. حتى التغييرات المصرح بها وأخطاء البرمجة يمكن أن تتسبب في حدوث خلل إذا لم تكن الذاكرة المؤقتة محمية. يمكن أن تؤدي أخطاء الشبكة والاتصالات على الرسائل الطويلة إلى أخطاء غير مقصودة إذا لم يتم التحقق من صحة البيانات قبل المعالجة.
Maintenance	يمكن أن تجعل أخطاء البرمجة التي تسبب في الكتابة في الذاكرة المؤقتة ان تجعل من الصعب العثور على الأخطاء ، لذلك يمكن تجنب المشكلة عن طريق تعيين سجلات محددة للكتابات.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic** : TA009 - Inhibit Response Function, TA010 - Impair Process Control **Technique:** T0835 - Manipulate I/O image , T0836 - Modify Parameter
ISA 62443-3-3	**SR 3.4** : Software and information integrity **SR 3.5** : Input Validation **SR 3.6** : Deterministic Output
ISA 62443-4-1	**SD-4**: Secure design best practices **SI-1**: Security implementation review **SI-2** : Secure coding standards **SVV-1** : Security requirements testing
ISA 62443-4-2	**CR 3.4** : Software and information integrity **CR 3.5** : Input Validation **CR 3.6** : Deterministic Output
MITRE CWE	**CWE-787:** Out-of-bounds Write **CWE-653:** Insufficient Compartmentalization

11. أداة للتحقق من المعقولية

ادر العملية بطريقة تسمح بفحوصات المعقولية عن طريق التحقق من القياسات المختلفة.

Security Objective	Target Group
Integrity of I/O values	Product Supplier Integration / Maintenance Service Provider

التوجيه

هناك طرق مختلفة لاستخدام المعقولية المادية للتحقق من صحة القياسات:

a) قارن بين القياسات المتكاملة والمستقلة عن الوقت
يمكن إجراء فحوصات المعقولية من خلال دمج أو تمييز القيم المعتمدة على الوقت خلال فترة زمنية ومقارنتها بالقياسات المستقلة عن الوقت.

b) قارن مصادر القياس المختلفة

أيضًا ، يمكن أن يكون قياس نفس الظاهرة بطرق مختلفة اختبارًا جيدًا للقبول.لا يجب بالضرورة أن تكون مصادر القياس المختلفة عبارة عن مستشعرات فيزيائية مختلفة ، ولكن يمكن أن تعني أيضًا استخدام قنوات اتصال بديلة (انظر الأمثلة).

مثال

a) قارن بين القياسات المتكاملة والمستقلة عن الوقت

- المضخة المقننة ومقياس مستوى الخزان: يجب أن يساوي التغيير الحجمي التدفق المتكامل.
- موقد في غلاية: يجب أن تساوي الحرارة المضافة من السعرات الحرارية ارتفاع درجة الحرارة.

b) قارن مصادر القياس المختلفة

- استخدام سرعة الهواء والأفق الاصطناعي والسرعة الرأسية والارتفاع في الطائرة لقياس ظاهرة صعود / هبوط الطائرة.
- مقارنة قيم متغيرات العملية من مسجلي البيانات المستقلين (المرتبطة بحلقات 4 –20mA أو ال relay contacts ونقلها عبر قنوات اتصال مستقلة) مع بيانات نظام SCADA (التي تأتي بالطريقة "العادية" من خلال PLC و HMI) والتنبيه على الانحرافات وإيقافها بشكل كبير - القيم المحددة.

Why?

Beneficial for...?	Why?
Security	يسهل مراقبة القيم التي تم التلاعب بها (بافتراض أنه لم يتم التلاعب بجميع أجهزة الاستشعار في وقت واحد).
Reliability	يمنع القبول أو يحدد (للعمل المستقبلي) القياسات التالفة / الخاطئة كمدخلات.
Maintenance	يستبعد الأسباب المادية المحتملة للفشل بسرعة أكبر.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0806 - Brute Force I/O
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
MITRE CWE	**CWE-754:** Improper Check for Unusual or Exceptional Conditions

12. التحقق من صحة المدخلات على أساس المعقولية المادية

تأكد من أن المشغلين يمكنهم فقط إدخال ما هو عملي أو ممكن ماديًا في العملية. اضبط مؤقتًا لعملية ما على المدة التي يجب أن تستغرقها فعليًا. ضع في اعتبارك التنبيه عند وجود انحرافات. تنبيه أيضًا عندما يكون هناك خمول غير متوقع.

Security Objective	Target Group
Integrity of I/O values	Integration / Maintenance Service Provider

التوجيه

a) مراقبة المده المادية المتوقعة

إذا استغرقت العملية وقتًا أطول من المتوقع للانتقال من طرف إلى آخر ، فهذا أمر يستحق التنبيه. بدلاً من ذلك ، إذا تم ذلك بسرعة كبيرة ، فهذا يستحق التنبيه أيض يمكن أن يكون الحل البسيط تنبيه مهلة الخطوة. قد يكون هذا مفيدًا للتسلسل / المهام التي يتم التحكم فيها بخطوة.

على سبيل المثال ، تستغرق الخطوة "نقل الكائن من A إلى B " 5 ثوانٍ من بداية الخطوة حتى يتم استيفاء حالة الانتقال (المستشعر: وصل الكائن إلى B).
إذا تم استيفاء الشرط مبكرًا جدًا أو متأخرًا جدًا ، فسيتم تشغيل مهلة الخطوة.

b) مراقبة النشاط المادي المتكرر المتوقع

يمكن أن يعني فحص المعقولية الفيزيائي أيضًا التنبيه لعدم النشاط المادي غير المعقول: إذا كان هناك توقع لدورة منتظمة متكررة من الأحداث (على سبيل المثال ، الدُفعات والأنماط اليومية) ، فإن مؤقت عدم النشاط سينبه إذا كان من المتوقع أن يتغير شيء (قيم منفصله أو تناظريه) ظل ثابتا لفترة طويلة جدًا.

مثال

a) مراقبة المده المادية المتوقعة

- تستغرق بوابات السد وقتًا معينًا للانتقال من إغلاقها بالكامل إلى فتحها بالكامل
- في مرفق مياه الصرف الصحي ، يستغرق ملء البئر الرطب وقتًا معينًا

b) مراقبة النشاط المادي المتكرر المتوقع

- يجب أن تتنقل عملية التصنيع أو تجميع خطوط الأنابيب بانتظام بين نطاقات التحكم أو أوضاع التشغيل.
- عادة ما يكون لمحطات معالجة مياه الصرف الصحي البلدية دورة نشاط / نمط لمعدلات التدفق المؤثرة.

c) قيد ادخال المشغل ل set points إلى ما هو عملي / ممكن ماديًا.

على سبيل المثال ، سمحت حالة Oldsmar Florida بإدخال عامل التشغيل وهو أ) آلاف المرات أكثر مما هو مطلوب عادةً ب) وهذا غير ممكن فعليًا. حاول تكوين حدود التشغيل في كود PLC حيثما أمكن ذلك بدلاً من استخدام اسكربتات ال HMI.

Why?

Beneficial for...?	Why?
Security	1. يمكن أن تشير الانحرافات إلى أن أحد المشغلات كان بالفعل في منتصف حالة الحركه أو أن شخصًا ما يحاول تزييف الإدخال / الإخراج ، على سبيل المثال ، عن طريق القيام بهجوم إعادة. 2. تسهل تنبيهات الخمول مراقبة وضع التجميد أو الوضع القسري 3. القيم الثابتة التي يمكن أن تكون نتيجة التلاعب بالنظام أو الجهاز.
Reliability	1. تمنحك الانحرافات إنذارًا مبكرًا عن المعدات المعطلة بسبب الأعطال الكهربائية أو الميكانيكية. 2. تساعد تنبيهات الخمول في تحديد القياسات أو حلقات التحكم في النظام التي قد تكون فاشلة (وبالتالي ثابتة) بسبب خطأ مادي في الجهاز أو مشكلة في خوارزمية التحكم المنطقي أو إدخال فاشل / غير لائق لعامل التشغيل .
Maintenance	

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0806 - Brute Force I/O
ISA 62443-3-3	**SR 3.5**: Input Validation **SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.5**: Input Validation **CR 3.6**: Deterministic Output
MITRE CWE	**CWE-754:** Improper Check for Unusual or Exceptional Conditions

13. تعطيل منافذ وبروتوكولات الاتصال غير الضرورية / غير المستخدمة

وحدات تحكم **PLC** ووحدات **network interface** تدعم بشكل عام بروتوكولات الاتصال المتعددة الممكنه افتراضيًا. قم بتعطيل المنافذ والبروتوكولات غير المطلوبة للتطبيق.

Security Objective	Target Group
Hardening	Integration / Maintenance Service Provider

التوجيه

عادةً ما يتم تمكين البروتوكولات الشائعة افتراضيًا على سبيل المثال ، HTTP، HTTPS، SNMP، Telnet، FTP، MODBUS، PROFIBUS، EtherNet / IP، ICMP، إلخ.

تتمثل أفضل الممارسات في تطوير مخطط تدفق البيانات الذي يصور الاتصالات المطلوبة بين PLC والمكونات الأخرى في النظام.

يجب أن يُظهر مخطط تدفق البيانات كلاً من المنافذ المادية على PLC وكذلك الشبكات المنطقية التي يتصلون بها. لكل منفذ مادي ، يجب تحديد قائمة بروتوكولات الشبكة المطلوبة وتعطيل جميع المنافذ الأخرى.

مثال

على سبيل المثال ، تشتمل العديد من PLCs على خادم ويب مضمن للصيانة واستكشاف الأخطاء وإصلاحها. إذا لم يتم استخدام هذه الميزة ، إذا كان ذلك ممكنًا ، فيجب تعطيلها لأن هذا قد يكون ثغره للهجوم.

Why?

Beneficial for...?	Why?
Security	يضيف كل منفذ وبروتوكول تم تمكينه إلى زياده سطح الهجوم المحتمل لـ PLC. أسهل طريقة للتأكد من عدم تمكن المهاجم من استخدامها للاتصال غير المصرح به هي تعطيلها تمامًا.
Reliability	إذا تعذر على PLC الاتصال عبر منفذ أو بروتوكول معين ، فإن هذا يقلل أيضًا من المقدار المحتمل لحركة المرور (المشوهة) ، سواء كانت ضارة أم لا ، مما يقلل من فرص تعطل PLC بسبب حزم الاتصال غير المقصودة / المشوهة.
Maintenance	يؤدي تعطيل المنافذ والبروتوكولات غير المستخدمة أيضًا إلى تسهيل الصيانة ، لأنه يقلل من التعقيد الكلي لـ PLC. ما هو غير موجود لا يحتاج إلى إدارته أو تحديثه.

References

Standard / framework	Mapping
MITRE ATT&CK for ICS	**Tactic**: TA005 - Discovery **Technique:** T0808 - Control Device Identification , T0841 - Network Service Scanning, T0854 - Serial Connection Enumeration
ISA 62443-3-3	**SR 7.6**: Network and security configuration settings **SR 7.7**: Least functionality
ISA 62443-4-2	**EDR 2.13** : Use of physical diagnostic and test interfaces
ISA 62443-4-1	**SD-4**: Secure design best practices **SI-1**: Security implementation review **SVV-1**: Security requirements testing

14. تقييد third-party data interfaces

تقييد نوع الاتصالات والبيانات المتاحة لـ **3rd party interfaces** يجب أن تكون الاتصالات و / أو واجهات البيانات محددة جيدًا ومقيدة للسماح فقط بقدرات القراءة / الكتابة لنقل البيانات المطلوبة.

Security Objective	Target Group
Hardening	Integration / Maintenance Service Provider

التوجيه

في بعض الحالات ، نظرًا لتشغيل الكابلات الطويلة أو التبادل الكبير للبيانات ، تقدم اتصالات البيانات البينية حالة عمل أفضل من تبادل البيانات السلكي الثابت بين طرفين منفصلين.

يجب مراعاة الإرشادات التالية واتباعها حيثما كان ذلك ممكنًا عند تصميم وتنفيذ واجهة تبادل بيانات لطرف ثالث:

- استخدم وحدة اتصالات مخصصة ، إما متصلة مباشرة بـ PLC أو معدات تبادل البيانات التابعة لجهة خارجية ، أو استخدم معدات شبكة مخصصة منفصلة ماديًا عن الشبكة الأساسية لكل طرف.
- يتوفر عنوان MAC للأجهزة المتصلة عادةً في متغيرات النظام لأي جهاز يدعم ICS Ethernet ، مما يجعل من الممكن التحقق من هوية الجهاز باستخدام نهج متعدد العوامل (عنوان IP + رمز صانع MAC = جهاز موثوق به). هذه الممارسة بالتأكيد ليست مضمونه ، حيث يمكن انتحال عناوين MAC و IP ، ولكنها تعمل على رفع مستوى الاتصالات بين أنظمة وأجهزة ICS الموثوقة.
- عند تحديد بروتوكول لواجهات الجهات الخارجية ، اختر بروتوكولًا يقلل من قدرة الطرف الثالث على كتابة البيانات إلى نظام المالك.
- اختر طريقة اتصال ومنفذ اتصال يمنع الطرف الثالث من ضبط جهاز PLC الخاص بالمالك أو معدات تبادل البيانات.
- يجب ألا يكون الطرف الثالث قادرًا على القراءة أو الكتابة إلى أي بيانات لم يتم تحديدها وإتاحتها بشكل صريح.
- استخدم مؤقت المراقبة لمراقبة الاتصالات حتى لا يتم إرسال الأوامر إلى PLC في وضع الخطأ.
- الاتصال التسلسلي: استخدم وحدة اتصال مخصصة لكل واجهة خارجية مع مجموعة محدودة من البيانات. تأكد من أن جانب المالك من الاتصال هو البادئ وأن الطرف الثالث هو المستجيب.
- Ethernet / IP: تسمح بعض وحدات التحكم المنطقية (PLC) لوحدات الاتصال بالعمل كجدار حماية ويمكنها إجراء فحص الحزمة العميق (DPI) ، أو تقييد واجهات وحدة الاتصال للحد من تبادل البيانات لمجموعة فرعية محددة مسبقًا. إذا كانت هذه الميزات متوفرة ، وكان بروتوكول Ethernet / IP قيد الاستخدام ، فتأكد من تمكين الميزات وتكوينها.
- عندما تمنع المتطلبات التشغيلية أو التعاقدية المالك من إنجاز العناصر السابقة ، ففكر في استخدام "مركز بيانات" منفصل (المعروف أيضًا باسم DMZ / proxy) PLC من أجل تخزين البيانات مؤقتًا وحماية المالك من عمليات الكتابة / البرمجة غير المرغوب فيها من الطرف الثالث. تأكد من عدم إمكانية اجتياز اللوحة المعززة لـ PLC من شبكة الطرف الثالث.

مثال

- وحدات خطوط الأنابيب أو وحدات النقل التلقائي للخزانة المؤجرة (LACT) التي تقوم بنقل وقياس الهيدروكربونات أو المياه المتبادلة بين شركة إنتاج أو خط أنابيب في المنبع وشركة خطوط أنابيب وسط مع شبكة أو اتصالات مترابطة متسلسلة تشارك القياس والحالة والمعلومات المتساهلة بين الشركات.
- مزود مياه الشرب الإقليمي (المستورد) الذي يتقاسم معدل تدفق مياه الإقبال الذي يتم تسليمه إلى محطة مياه تابعة للبلدية المحلية.

Why?

Beneficial for…?	Why?
Security	1. الحد من التعرض لشبكات ومعدات الطرف الثالث. 2. مصادقة الأجهزة الخارجية لمنع الانتحال.
Reliability	يحد من القدرة على إجراء تعديلات مقصودة أو غير مقصودة أو الوصول من مواقع أو معدات تابعة لجهات خارجية.
Maintenance	

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA010 - Impair Process Control **Technique:** T0836 - Modify Parameter
ISA 62443-3-3	**SR 7.6**: Network and security configuration settings **SR 7.7**: Least functionality
ISA 62443-4-2	**CR 7.6**: Network and security configuration settings **CR 7.7**: Least functionality
ISA 62443-4-1	**SD-4**: Secure design best practices **SI-1**: Security implementation review **SVV-1:** Security requirements testing

15. حدد حالة عملية آمنة في حالة إعادة تشغيل PLC

حدد الحالات الآمنة للعملية في حالة إعادة تشغيل **PLC** (على سبيل المثال ، تنشيط جهات الاتصال ، وإلغاء تنشيطها ، والحفاظ على الحالة السابقة).

Security Objective	Target Group
Resilience	Product Supplier Integration / Maintenance Service Provider

التوجيه

إذا أمر شيء ما بإعادة تشغيل PLC في منتصف عملية العمل ، فيجب أن نتوقع أن ينتقل البرنامج بسلاسة مع الحد الأدنى من تعطيل العملية. تأكد من أن العملية التي تتحكم فيها آمنة لإعادة التشغيل.

إذا لم يكن من العملي تكوين PLC لإعادة التشغيل بأمان ، فتأكد من أنه ينبهك إلى هذه الحقيقة وأنه لا يصدر أي أوامر جديدة. أيضًا ، في هذه الحالة ، تأكد من أن إجراءات التشغيل القياسية (SOP) تحتوي على تعليمات واضحة جدًا لإعداد أدوات التحكم اليدوية بحيث يبدأ PLC العملية بشكل صحيح.

أيضًا ، قم بتوثيق جميع إجراءات بدء التشغيل ، والإغلاق ، والتحكم الثابت في الحالة ، وإعادة تشغيل نظام التحكم في الطيران.

مثال

/

Why?

Beneficial for...?	Why?
Security	**يقضي على السلوك المحتمل غير المتوقع:** إن أبسط متجه للهجوم لـ PLC هو إجباره على الانهيار و / أو إعادة التشغيل. بالنسبة للعديد من PLCs ، ليس من الصعب القيام بذلك ، لأن العديد من PLCs لا يمكنها التعامل بشكل جيد مع المدخلات غير المتوقعة أو الكثير من حركة المرور. على الرغم من وجود العديد من التشخيصات لإجراءات وحدة التحكم أثناء تشغيلها ، إلا أن كيفية تعاملها مع بدء التشغيل مع عملية قيد التشغيل عادةً ما تكون غير واضحة. قد يكون هذا غير شائع ، ولكنه عنصر أساسي للهجوم إذا أخذنا في الاعتبار السلوك الضار للمهاجم.
Reliability	**تجنب التأخيرات غير المتوقعة:** بعد تشغيل PLC ، و بدأت ال state machine بحالة مع بعض الشروط التي لا تسمح للعملية بالبدء ، ولا يمكن للمشغل تطبيع النظام ، سيحتاج الفني إلى الدخول إلى برنامج PLC لفرض الظروف على الانتقال إلى الحالة المطلوبة لتتمكن من بدء التشغيل. هذا يمكن أن يسبب التأخير وخسائر الإنتاج.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA009 - Inhibit Response Function **Technique:** T0816 - Device Restart/Shutdown
ISA 62443-3-3	**SR 3.6**: Deterministic Output
ISA 62443-4-2	**CR 3.6**: Deterministic Output
ISA 62443-4-1	**SVV-1**: Security requirements testing

16. لخص أوقات دورات **PLC** واعرضها على **HMI**

لخص وقت دورة **PLC** كل 2-3 ثوانٍ وقدم تقريرًا إلى **HMI** لعرضها عن طريق الرسم البياني.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider

التوجيه

عادة ما تكون أوقات الدورات متغيرات نظام في PLC ويمكن استخدامها للتلخيص في كود PLC. يجب إجراء التلخيص لحساب متوسط أوقات الدورة والذروة والحد الأدنى. يجب أن يقوم HMI بتوجيه هذه القيم والتنبيه إذا كانت هناك تغييرات كبيرة.

وقت الدورة هو الوقت الذي يستغرقه حساب كل تكرار منطقي لـ PLC. التكرارات هي مزيج من مخططات السلم (LD) ومخططات كتلة الوظائف (FBD) وقائمة التعليمات (IL) والنص المهيكل (ST). يمكن ضم هذه المكونات المنطقية مع مخططات الوظائف المتسلسلة (SFC).

يجب أن تكون أوقات الدورات ثابتة على PLC ما لم تكن هناك تغييرات على سبيل المثال

- بيئة الشبكة
- منطق PLC
- عملية

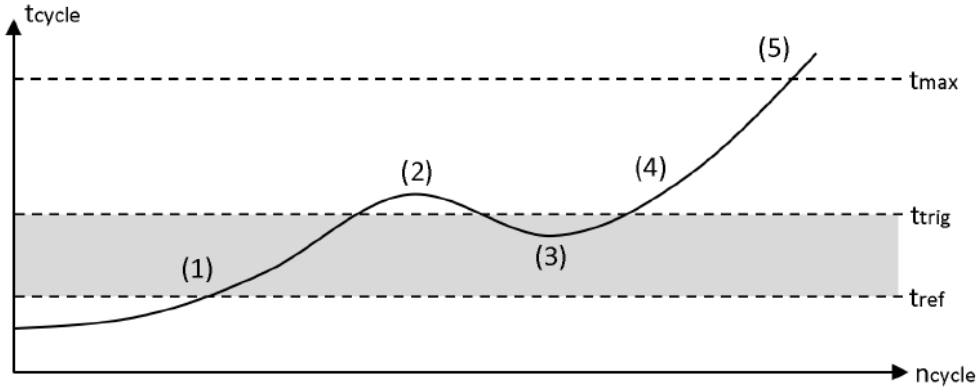
لذلك ، يمكن أن تكون التغييرات غير العادية في وقت الدورة مؤشراً على أن منطق PLC قد تغير وبالتالي يوفر معلومات قيمة لفحوصات السلامة.

يوفرعرض القيم بمرور الوقت باستخدام الرسم البياني طريقة بديهية للفت الانتباه إلى الحالات الشاذة التي يصعب ملاحظتها بمجرد وجود قيم مطلقة.

مثال

تتمتع العديد من وحدات التحكم المنطقية القابلة للبرمجة بمراقبة "أقصى وقت للدورة" على مستوى الأجهزة. إذا تجاوز وقت الدورة القيمة القصوى ، يقوم الجهاز بضبط وحدة المعالجة المركزية على STOP (5).

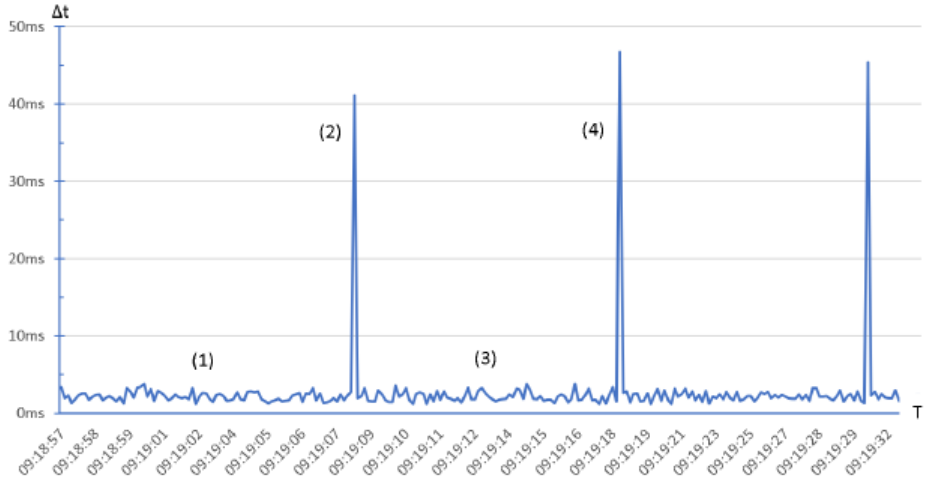
بالطبع ، يدرك المهاجمون هذا الأمر وسيحافظون على كود هجوم المحتمل ضعيفًا قدر الإمكان لتقليل التأثير على وقت الدورة الإجمالي. بالاضافه لبرنامج مراقبة وقت دورة البرنامج ، يُعرَّف وقت الأسطوانة المرجعي tref على أنه وقت الدورة الأساسية. نظرًا لأن التقلبات الصغيرة أمر طبيعي ، يجب تحديد عتبة مقبولة (1،3) يتم تشغيل مراقبة الدورة ، إذا تم تجاوز العتبة (2،4)



يمكن تخزين أي انحراف عن الوقت المرجعي في ملف سجل مثل هذا:

SeqNo	Date	UTC Time	Abweichung
1	2019-11-22	09:05:50.021	40,821ms
2	2019-11-22	09:06:00.069	44,391ms
3	2019-11-22	09:06:10.120	44,994ms
4	2019-11-22	09:06:20.166	40,561ms
5	2019-11-22	09:06:30.211	40,725ms

إذا كانت أوقات الدورات تعرض غلي HMI ، فستظهر أحمال وحدة المعالجة المركزية الثقيلة في لمحة. يوضح الرسم البياني في المثال التالي برنامج PLC مع تعليمات برمجية ضارة يتم تنفيذها بشكل دوري. يوضح الشكل (1،3) تقلبات زمنية مقبولة للدورة ("ضوضاء") أثناء التشغيل العادي ، ويتم تنفيذ كود الهجوم على (2،4) مما يزيد من وقت الدورة.



Why?

Beneficial for...?	Why?
Security	تشمل الهجمات على PLCs تغيير منطقها ، أو تنشيط برنامج جديد ، أو اختبار رمز جديد ، أو تحميل وصفة عملية جديدة ، أو إدخال منطق إضافي لإرسال الرسائل أو تنشيط بعض الميزات. بالنسبة لمعظم PLCs ، فإن فحوصات سلامة التشفير التقليدية غير مجدية. ومع ذلك ، من الجيد التنبيه في حالة حدوث أي من التغييرات المنطقية المذكورة أعلاه. نظرًا لأن أوقات الدورات ثابتة إلى حد ما في ظل الظروف العادية ، فإن التغييرات في أوقات الدورات هي مؤشر جيد على أن المنطق في أحد المكونات المنطقية المذكورة أعلاه قد تغير.
Reliability	راجع الأمان ، ولكن لأسباب غير ضارة.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA002 - Execution **Technique:** T0873 - Project File Infection
ISA 62443-3-3	**SR 3.4**: Software and information integrity
ISA 62443-4-2	**EDR 3.2**: Protection from malicious code
MITRE CWE	**CWE-754:** Improper Check for Unusual or Exceptional Conditions

17. سجل وقت تشغيل **PLC** واعرضها على **HMI**

سجّل وقت تشغيل **PLC** لمعرفة وقت إعادة تشغيله. اعرض تسجيل وقت التشغيل على **HMI** وذلك للتشخيص.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider

التوجيه

تتبع وقت تشغيل PLC

- في PLC نفسه (إذا كان الجهوزية متغير نظام في PLC)
- في PLC نفسه إذا كان يحتوي على MIB-2 / أي تطبيق SNMP
- خارجيًا عن طريق SNMP على سبيل المثال

إذا كان PLC يحتوي على SNMP مع MIB-2 ، وهو أمر شائع جدًا ، فإن OID لوقت التشغيل "(0 sysUpTimeInstance)" هو 1.3.6.1.2.1.1.3. تعد عمليات إعادة ضبط وقت التشغيل مؤشرات مهمة لإعادة تشغيل PLC. تأكد من تنبيهات HMI لأي نوع من إعادة تشغيل PLC .

يعتبر وقت التشغيل المرتبط برموز الخطأ تشخيصات جيدة.

مثال

/

Why?

Beneficial for...?	Why?
Security	إن أبسط متجه للهجوم لـ PLC هو إجباره على الانهيار و / أو إعادة التشغيل. بالنسبة للعديد من PLCs ، ليس من الصعب القيام بذلك ، لأن العديد من PLCs لا يمكنها التعامل بشكل جيد مع المدخلات غير المتوقعة أو الكثير من حركة المرور. وبالتالي ، يمكن أن تكون عمليات إعادة التشغيل غير المتوقعة مؤشرًا على أن PLC يواجه إجراءات غير عادية.
Reliability	تعد عمليات إعادة تشغيل PLC جيدة أيضًا للتشخيص في حالة الفشل ولمراقبة وحدات التحكم المنطقية القابلة للبرمجة التي يتم العمل عليها في أي وقت.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA009 - Inhibit Response Function **Technique:** T0816 - Device Restart/Shutdown
ISA 62443-3-3	**SR 7.6**: Network and security configuration settings
ISA 62443-4-2	**CR 7.6**: Network and security configuration settings
MITRE CWE	**CWE-778:** Insufficient Logging

18. سجل توقفات **PLC** الطارئه واعرضها على **HMI**

قم بتخزين أحداث التوقف الطارئ لـ **PLC** من الأعطال أو عمليات الإغلاق لاسترجاعها بواسطة أنظمة إنذار **HMI** للتشاور قبل إعادة تشغيل **PLC**. مزامنة الوقت للحصول على بيانات أكثر دقة.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider

التوجيه

تشير أحداث الأعطال إلى سبب إغلاق PLC بحيث يمكن معالجة المشكلة قبل إعادة التشغيل

قد تحتوي بعض PLCs على أكواد خطأ من الحالة الأخيرة حيث حدث خطأ في PLC أو تم إيقافه بشكل غير صحيح. سجل تلك الأخطاء ثم امسحها. قد يكون من الجيد الإبلاغ عن هذه الأخطاء إلى HMI كبيانات معلوماتية أو ربما إلى خادم سجل النظام ، إذا كانت هذه الميزات والبنية التحتية موجودة.

تحتوي معظم PLCs أيضًا على نوع من ميزة المسح الأولى التي تولد الأحداث. إنه سلوك تمتلكه جميع معدات PLC تقريبًا في شكل ما. إنه في الأساس علامة واحدة أو أكثر ، أو إجراء معين يتم تنفيذه على أول مسح لـ PLC بعد أن "يستيقظ". يجب تسجيل هذا المسح الأول وتعقبه.

مثال

/

Why?

Beneficial for...?	Why?
Security	تتيح السجلات استكشاف الأخطاء وإصلاحها في حالة وقوع حادث. قبل أن يتم تشغيل PLC ، خاصة بعد مواجهة المشاكل ، من المهم التأكد من أنها جديرة بالثقة.
Reliability	تعد السجلات أيضًا مصادر جيدة لتصحيح الأخطاء إذا لم يكن سبب الحدث ضارًا.
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA009 - Inhibit Response Function **Technique:** T0816 - Device Restart/Shutdown 1
ISA 62443-3-3	**SR 7.6**: Network and security configuration settings
ISA 62443-4-2	**CR 7.6**: Network and security configuration settings
MITRE CWE	**CWE-778:** Insufficient Logging

19. راقب استخدام ذاكرة **PLC** واعرضها على **HMI**

قم بقياس وتوفير **baseline** لاستخدام الذاكرة لكل وحدة تحكم منتشرة في بيئة الإنتاج واعرضها على **HMI**.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider Asset Owner

التوجيه

نظرًا لأن زيادة سطور التعليمات البرمجية في المنطق يمكن أن تؤدي أيضًا إلى زيادة استهلاك الذاكرة في وقت التشغيل ، فمن المستحسن لمبرمجي PLC تتبع أي انحراف عن خط الأساس وتخصيص فئة إنذار لهذا الحدث.

مثال

في Rockwell Allen Bradley PLCs ، يمكن إنشاء خط أساس على وحدة تحكم ويمكن تتبع استخدام الذاكرة باستخدام أداة مراقبة المهام RSLogix 5000. ليس فقط الذاكرة الرئيسية ولكن أيضًا ذاكرة الإدخال / الإخراج وذاكرة السلم / العلامة يمكن تتبعها باستخدام trends.

Why?

Beneficial for...?	Why?
Security	يمكن أن تكون زيادة استخدام الذاكرة مؤشرا على تشغيل PLC للتعليمات البرمجية المعدلة.
Reliability	قد يكون تتبع استخدام الذاكرة للبرامج قيد التشغيل مفيدًا في تجنب إجمالي استهلاك الذاكرة وحالة الخطأ النهائية لوحدة التحكم PLC.
Maintenance	يمكن استخدام تتبع استخدام الذاكرة في ضبط وإيجاد أفضل وقت مسح لوحدة التحكم المراقبة ولكن أيضًا في استكشاف الأخطاء وإصلاحها والمشكلات المتعلقة بالحالات المعيبة.

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic**: TA002 - Execution **Technique:** T0873 - Project File Infection
ISA 62443-3-3	**SR 3.4**: Software and information integrity
ISA 62443-4-2	**EDR 3.2**: Protection from malicious code

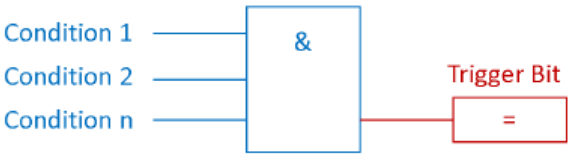
20. اعتراض السلبيات الزائفة والإيجابيات الزائفة للتنبيهات الحرجة

تحديد التنبيهات الهامة وبرمجة مصيدة لتلك التنبيهات. اضبط الملاءمة لمراقبة ظروف التشغيل وحالة التنبيه لأي انحراف.

Security Objective	Target Group
Monitoring	Integration / Maintenance Service Provider

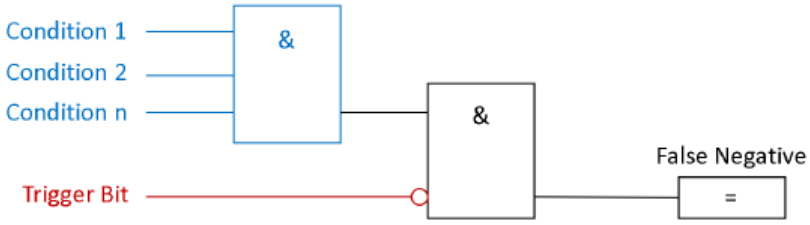
التوجيه

في معظم الحالات ، تكون حالات التنبيه منطقية (صواب ، خطأ) ويتم تشغيلها بشروط معينة كما هو معروض أدناه. على سبيل المثال ، يصبح trigger bit للتنبيه "الضغط الزائد" صحيحًا ، إذا كان الشرط 1 "مفتاح الضغط 1" ، يكون الشرط 2 "قيمة مستشعر الضغط أعلى من الحد الحرج" ، من خلال n. ، هي TRUE.



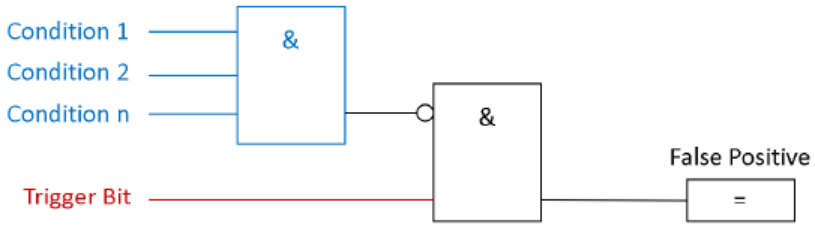
لإخفاء هجوم ، يمكن للخصم أن يقمع بت تشغيل التنبيه ويسبب نتيجة سلبية خاطئة.

تراقب مصيدة السلبيات الخاطئة شروط trigger bit و trigger bit السالبة نفسها. مع هذا الإعداد البسيط ، يتم الكشف عن سلبية خاطئة. انظر الصورة التالية:



في حالات أخرى ، قد يتسبب الخصم عمدًا في نتائج إيجابية كاذبة ، لتقليل انتباه مشغل العملية.

بنفس طريقة المصيدة السلبية الزائفة ، يمكن أيضًا اكتشاف الإيجابيات الخاطئة من خلال مراقبة بتة إطلاق التنبيه وإذا تم استيفاء شروط التشغيل. إذا لم يتم استيفاء الشروط ، ولكن بتة المشغل نشطة ، يتم الكشف عن إيجابية خاطئة: انظر الصورة التالية:



مثال

مثال 1: تقدم شركة **Siemens** في منتجاتها من **Siemens S7-1200 / 1500** خادم ويب مع مجموعة واسعة من الوظائف ، على سبيل المثال عرض حالة **PLC** أو وقت الدورة أو سجلات النطاق. كما أن لديها خيار عرض وتعديل جداول البيانات والمتغيرات. يمكن تعديل حقوق الوصول إلى خادم الويب في إعدادات أجهزة **PLC**. في حالة سوء تكوين حقوق الوصول ، يمكن للخصم الوصول إلى متغيرات **PLC** و **Datablocks**. لإنشاء نتيجة إيجابية خاطئة ، يختار الخصم بت تنبيه تنبيه ويغير الحالة.

مثال 2: في هجوم Triton / Trisys / HatMan ، قمعت التعليمات البرمجية المارقة حالات التنبيه.

مثال 3: هجوم bus-injection يمكن أن يرسل تنبيه إيجابي كاذب إلى عميل SCADA عالي المستوى.

Why?

Beneficial for...?	Why?
Security	يخفف من الإيجابيات الخاطئة أو السلبية الكاذبة لرسائل التنبيه الحرجة التي يسببها الخصم الذي يقوم بتشويش هجومه (على سبيل المثال ، الشفرة المارقة ، حقن الناقل ، العبث بجداول حالة PLC التي يمكن الوصول إليها على خوادم الويب غير الآمنة).
Reliability	/
Maintenance	/

References

Standard / framework	Mapping
MITRE ATT&CK ICS	**Tactic** : TA009 - Inhibit Response Function **Technique:** T0878 - Alarm Suppression
ISA 62443-3-3	**SR 3.5** : Input Validation
ISA 62443-4-2	**CR 3.5** : Input Validation
ISA 62443-4-1	**SI-1** : Security implementation review
MITRE CWE	**CWE-754:** Improper Check for Unusual or Exceptional Conditions

حول مشروع Secure PLC Programming

لسنوات عديدة ، كانت أجهزة التحكم المنطقية القابلة للبرمجة (PLCs) غير آمنة حسب التصميم. عدة سنوات من التخصيص وتطبيق أفضل الممارسات من تكنولوجيا المعلومات أدت إلى بروتوكولات آمنة واتصالات مشفرة وتجزئة الشبكة وما إلى ذلك. ومع ذلك ، حتى الآن ، لم يكن هناك تركيز على استخدام الميزات المميزة في PLCs (أو SCADA / DCS) للأمان ، أو كيفية برمجة PLCs مع مراعاة الأمان. هذا المشروع - المستوحى من ممارسات الترميز الآمن لتكنولوجيا المعلومات الحالية - يسد هذه الفجوة.

من الذي يجب أن يقرأ ويطبق ممارسات Secure PLC Coding؟

تمت كتابة هذه الممارسات للمهندسين. الهدف من هذا المشروع هو تقديم إرشادات للمهندسين الذين يقومون بإنشاء برامج (منطق السلم ، مخططات الوظائف ، إلخ) للمساعدة في تحسين الوضع الأمني لأنظمة التحكم الصناعية. تستفيد هذه الممارسات من الوظائف المتاحة أصلاً في PLC / DCS. هناك حاجة إلى أدوات أو أجهزة برمجية إضافية قليلة أو معدومة لتنفيذ هذه الممارسات. يمكن أن تتناسب جميعها مع برمجة PLC وسير العمل التشغيلي العادي. هناك حاجة إلى أكثر من الخبرة الأمنية والمعرفة الجيدة بـ PLCs المطلوب حمايتها ومنطقها والعملية الأساسية لتنفيذ هذه الممارسات.

ما هو النطاق إذا كانت هذه القائمة / كيف تحدد PLC Coding؟

لتتناسب مع نطاق قائمة ممارسات أفضل 20 ترميزًا آمنًا لـ PLC ، يجب أن تتضمن الممارسات التغييرات التي تم إجراؤها مباشرة على PLC. ما تراه في هذا المستند هو أفضل 20 اختيارًا لعدد أكبر من ممارسات تsecure PLC coding المحتملة. هناك أيضًا مسودة ممارسات إضافية تتعلق بالهيكل العام أو HMIs أو التوثيق. هؤلاء لا يتناسبون مع secure PLC coding، ولكن يمكن أن يكونوا على قائمة مستقبلية في بيئة PLC الآمنة.

ما هي فوائد تطبيق ممارسات Secure PLC Coding؟

من الواضح أن استخدام هذه الممارسات له فوائد أمنية - في الغالب إما تقليل سطح الهجوم أو تمكين استكشاف الأخطاء وإصلاحها بشكل أسرع في حالة وقوع حادث أمني. ومع ذلك ، فإن العديد من الممارسات لها فوائد إضافية تتجاوز الأمن. كما أن البعض يجعل كود PLC أكثر موثوقية ، وأسهل في التصحيح والصيانة ، وأسهل في التواصل ، وربما أصغر أيضًا. علاوة على ذلك ، لا تساعد ممارسات الترميز الآمن PLC المستخدمين في حالة حدوث مهاجم ضار فحسب ، بل تجعل أيضًا رمز PLC أكثر قوة لتحمل التهيئة الخاطئة أو الخطأ البشري.

من يقف وراء هذا المشروع؟

بدأ كل شيء مع Jake Brodsky's S4x20 talk "Secure Coding Practices for PLC's".

بعد المؤتمر ، بدأ ديل بيترسون مشروع أفضل 20. أمضى جايك برودسكي وسارة فلوشس عدة ساعات على الهاتف لتقديم ممارسات الترميز الآمن PLC المقترحة من Jake على الورق. بعد ذلك ، أنشأ Dale و Jake و Sarah منصة في top20.isa.org ، بدعم من ISA GCA ، لهيكلة وجمع مدخلات إضافية من مجتمعات المهندسين وأمن ICS.

استغرقت المناقشات وتوحيد نصوص الممارسة وتنظيم قائمة بأكثر 20 ممارسة ذات صلة حوالي عام ؛ تم تسريع العملية بواسطة Vivek Ponnada الذي بالإضافة إلى المساهمة ومراجعة المحتوى ، قام أيضًا بتنظيم مكالمات منتظمة حتى يتم حل جميع التعليقات على الممارسات ، محمد عبد المعز الصقلي الذي أضاف جميع مراجع المعايير في جهد كبير واحد ، فريق MITER CWE الذي قدم مراجع CWE أخيرًا - دقيقة ، سارة التي جمعت المستند الذي تقرأه الآن ، وجيك ، وديل ، وجون كوسيمانو ، وديرك روترموند ، وجوش روف ، وتوماس رابنشتاين ، وجوس سيرينو ، ووالتر سبيث ، وأجستين فالنسيا جيل أورتيجا ، ومارسيل ريك سين ، والراتيش R ، الذي قدم مدخلات خلال المكالمات العادية.

قائمة المؤيدين

مشروع التشفير الآمن PLC هو ، ولا يزال ، جهدًا مجتمعيًا حقيقيًا ، والذي لم يكن ممكنًا بدون عدد لا يحصى من المساهمين الذين يشاركون بسخاء وقتهم ومعرفة PLC / الأمان. إجمالي 943 مستخدمًا مسجلين على المنصة للمناقشة والمساهمة. فيما يلي قائمة أبجدية لجميع الذين وافقوا صراحة على ذكر أسمائهم. شكرًا لكل من خصص وقتًا لدعم هذا المشروع!

Aagam Shah
Adam Paturej
Agustin Valencia Gil-Ortega
Aitor García Almiñana
Alec Summers
Al Ratheesh. R
Andreas Falk
Anton Shipulin
Arkaitz Gamino
Carlos Olave
Chris van den Hooven
Chris Sistrunk
Christos Alexopoulos
Cris DeWitt
Dale Peterson
Dene Yandle
Dennis Verschoor
Dirk Rotermund
Edorta Echave García
Gananand Kini
George Alex Holburn
Gus Serino
Hakija Agic
Hector Medrano
Josie Houghton
Jozef Sulwinski
Juan Pablo Angel Espejo
Khalid Ansari
Marc Weber
Marcel Rick-Cen
Martin Huddleston
Massimiliano Zonta
Matthew Loong
Matthias Müller
Michael Thompson
Michal Stepien
Miguel Angel Frias
Mohamed Abdelmoez Sakesli
Moon Eluvangal Chandran
Nahuel Iglesias
Nalini Kanth
Narasimha S. Himakuntala
Omar Morando
Oscar J. Delgado-Melo
Päivi Brunou
Peter Donnelly
Peter Jackson
Ravindra Deshakulakarni

Heiko Rudolph	Rick Booij
Isiah Jones	Robert Albach
Jacob Brodsky	Rushi Purohit
Javier Perez Quezada	Sarah Fluchs
J-D Bamford	Sergei Biberdorf
Joe Weiss	Stephan Beirer
John Cusimano	Steve Christey Coley
John Hoyt	Thomas Rabenstein
John Powell	Tim Gale
John Kingsley	Vivek Ponnada
Joseph J. Januszewski	Vytautas Butrimas
Josh Ruff	Walter Speth

Special thanks to these organizations who generously provided infrastructure to use for the project team like domains, hosting, and web design and graphic design: