IEC 62443-4-1 Development Process Certification

Target of Evaluation:
Security Development Lifecycle Process

Company:
Trihedral Engineering Limited
Bedford, Nova Scotia
Canada

Contract Number: Q21/03-062
Report No.: TRI 2103062 R001
Version V1, Revision R1, March 10, 2022
Shalom Nazir, David Johnson

1 Management summary

This report summarizes the results of the security assessment conducted by *exida* between December 2021 and March 2022, of the Security Development Lifecycle Process used by Trihedral Engineering Limited to create and maintain the products or systems defined in the scope section of this document. The audit was conducted remotely. This assessment was carried out in accordance with the exida Security Development Process (eSDP) Certification criteria for determining compliance with IEC 62443-4-1.

The result of this assessment indicates the products or systems listed in the scope section are developed and maintained using a process compliant with the IEC 62443-4-1 requirements to Maturity Level 2 (Managed). At this maturity level, the service provider has the capability to manage the delivery and performance of the of the service according to written policies.

Table of Contents

Purpose and Scope

This report summarizes the results of the security assessment of the Security Development Lifecycle (SDL) Process used by Trihedral Engineering Limited performed by *exida*. This assessment applies to the following SDL process:

- Security Development Lifecycle Process

This process is used in developing the following products: VTScada

Artifacts that demonstrate adherence to the standard, are collected from a variety of products developed using the Security Development Lifecycle.

This report should allow the user to understand the following about the organization:

- This organization develops and maintains products using a development lifecycle that considers security in each phase and is therefore capable of developing secure products.
- This organization has a process to respond to and fix security vulnerabilities in a timely fashion
- This organization has a process for anyone to be able to report a security vulnerability on one of its products
- This organization documents user guidelines on how to ensure that its products or systems are being operated in the most secure manner.
- These processes are compliant with the requirements of IEC 62443-4-1 to Maturity Level 2 (Managed).

2 Project Management

2.1 Roles of the parties involved

Trihedral Engineering Limited	Manufacturer of the products defined in the scope section
exida	Accredited IEC 62443-4-1 Certification Body. Performed the security assessment according to the requirements of IEC 17065 (Conformity assessment -- Requirements for bodies certifying products, processes and services)

2.2 Standards and Literature used

The services delivered were performed based on the following standards / literature.

[N1]	IEC 62443-4-1: 2018 Edition 1.0	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

2.3 Reference documents

2.3.1 Documentation provided by Trihedral Engineering Limited

A list of documents supplied by *exida* are included the *exida* Security Case [R1]. Client supplied documentation used for this assessment are covered by Non-Disclosure Agreement and is not generally available for user inspection.

2.3.2 Documentation generated by *exida*

[R1]	*exida* Security Case	Documents compliance arguments and evidence for all requirements from IEC 62443-4-1
[R2]	Trihedral IEC_62443-4-1 Assessment Report V1R1.docx, 2022-03-07	eSDP Certification Report for Trihedral Engineering Limited (this report)
[R3]	Trihedral IEC_62443-4-1 ML 2 Certificate V1R1	eSDP Certification

3 Results of the Certification Assessment

3.1 Practice 1 – Security Management (SM)

Pass
The Trihedral Engineering Limited processes were reviewed from a management perspective with a focus on security. This included reviewing the content of the security management plan for various projects, as well as confirming that the processes include a clearly documented development lifecycle. Security training programs were reviewed, and all software developers and testers were trained per the project security plan.

All aspects of the code management were checked assuring that what was delivered to the customer is what was developed and tested. Any tools that assisted in the Software Configuration Management (SCM) process were checked for proper usage. Processes to modify the code showed traceability throughout the modification.

3.2 Practice 2 – Specification of Security Requirements (SR)

Pass
The security development lifecycle calls for security requirements to be documented as part of the overall product requirements. Trihedral Engineering Limited' processes for identifying system scope and boundaries were present. Product artifacts were examined and found to accurately document scope both physically and logically, and to clearly identify and document security requirements.

Example security requirements were reviewed and the environment where the equipment is expected to be installed was documented along with any perceived vulnerabilities or security threats of this environment.

Basic security functions were included along with the target Security Level. The process included a requirement review procedure, which included ensuring that all stakeholders were invited to the review meeting and a checklist to help ensure requirements meet common characteristics such as being clear and concise, verifiable, testable and feasible.

Security functions of the products were clearly defined as product requirements. All security requirements were reviewed by project personnel for feasibility, reasonability, completeness, and clarity.

The Trihedral Engineering Limited security development lifecycle calls for creation, analysis, and management of a Threat Model. The process called for the threat models to be updated periodically when the design changes and new threats are identified.

3.3 Practice 3 - Secure by Design

Pass
The Trihedral Engineering Limited process for designing a new product required the creation and a review of the product architecture. Examples of items specifically checked:

- Software Partitioning

- Interfaces
- Data Flows
- Network design
- Protocols
- Trust Boundaries

In addition, the security development lifecycle called for the attack surface to be clearly documented and attack surface reduction performed to limit the points of attacks on products. Several projects were audited and found to have security architecture documents which included the required information.

Also, the design process calls for a defense in depth strategy to be developed. This strategy helps ensure that if part of the system is compromised other layers of defense are in place to protect the system and make it more difficult for attackers to achieve their objective.

3.4 Practice 4 - Secure Implementation

Pass

The Trihedral Engineering Limited security development lifecycle includes standards and guidance on the development of code, and were reviewed for:

- Coding standards that discuss security concerns
- Banned code constructs and functions that pose a security risk

Implementation reviews are held to ensure that the standards and guidance is followed during the implementation and that security requirements have been met at the implementation level.

Static code analysis is performed to ensure that the coding standard is being followed and to identify and address potential security vulnerabilities in the code.

3.5 Practice 5 - Security Verification and Validation Testing (SIT)

Pass

The development process called for fuzz testing to be done on all interfaces that cross a trust boundary. Some example projects were audited, and it was found processes were in place that outlined how Communication Robustness Testing (CRT) was performed involving automated test case generation and protocol fuzzing. Automated testing was applied to both standard and proprietary protocols. Mitigations of known vulnerabilities were tested along with abusive test cases designed to expose new vulnerabilities. Vulnerability testing is done to identify potential vulnerabilities in the software and this includes software, known vulnerability scanning, attack surface analysis and penetration testing.

In addition to product functional testing the Trihedral Engineering Limited security development lifecycle included validation planning focused on the security requirements. In the audited projects, all procedures, test cases, and results were documented as well as all security requirements were validated by one or more tests. Discrepancies are tracked in a bug tracking system.

3.6 Practice 6 – Management of security related issues

Pass

The security development lifecycle includes management processes that track and manage vulnerabilities. These processes ensure that any security vulnerabilities found are examined to determine the root cause and to eliminate the problem. In addition, their processes called for incorporating lessons learned back into existing processes to reduce the possibility of repeat occurrences.

When a vulnerability is found external to the organization, there is a process in place that provides several means for the customer or other external party to report a security issue. When vulnerabilities are resolved, there is a process for notifying customers of the fixes.

The Trihedral Engineering Limited security development lifecycle provided for a managed response to vulnerabilities reported from external sources. This was outlined in a detailed procedure that described all the response steps involved after a vulnerability had been reported. This process linked to the modification and deployment processes that outlined development and timely release of security fixes. In addition, a process described a proactive approach for raising the awareness of new vulnerabilities and addressing them before they impacted field equipment.

3.7 Practice 7 – Security Update Management

Pass

Trihedral Engineering Limited has a process in place to deliver security updates to customers when vulnerabilities are found and fixed. This includes security updates for Trihedral Engineering Limited products as well as for third party products that are incorporated into Trihedral Engineering Limited products as components or are components that Trihedral Engineering Limited products must integrate with. The process includes testing of these security updates to ensure that they are compatible and developing methods to deliver updates securely.

3.8 Practice 8 - Security Guidelines (DSG)

Pass

Installation manuals for administrators and end users were reviewed. These all provided guidance on installation setup along with product setup. Of critical importance were user setup instructions detailing roles and authorization along with authentication rules. Information was also available on what prerequisites were needed to plug the equipment into the process network. The security guidelines were reviewed and were found to provide instructions on how to harden the system to ensure that it was configured in its most secure state.

4 Summary Results of Certification Assessment

This report summarizes the results of the security assessment of the Trihedral Engineering Limited Security Development Lifecycle Process according to eSDP criteria.

The result of this eSDP audit indicates the documented security development lifecycle complies with the relevant requirements from IEC 62443-4-1 to Maturity Level (ML) 2. ML 2 means that the company has the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it.

In addition, some of the products covered by this process were audited to confirm that all new development and modifications to these products were performed using this process. This does not imply that any product examined was fully compliant with the requirements, as products may have been developed prior to the company's security development lifecycle being used. However, this does demonstrate that security is being considered as products are modified, and that Trihedral Engineering Limited has the capability to develop compliant products in the future.

5 Terms and Definitions

ANSI	American National Standards Institute
CDV	Committee Draft for Vote
CRT	Communications Robustness Testing
DSG	Document Security Guidelines
EDSA	Embedded Device Security Assessment
eSDP	*exida* Security Development Process Certification
ISCI	ISA Security Compliance Institute
SCM	Software Configuration Management
SDL	Security Development Lifecycle
SDLA	Security Development Lifecycle Assessment

6 Status of the document

6.1 Liability

exida retains the right to change information in this report without notice.

exida believes the information in this report to be reliable and accurate but it is not guaranteed. Using and relying on this report is at your sole risk. *exida* is neither liable nor responsible for any loss, damage or expense arising from any omission or error in this report.

exida GIVES NO WARRANTIES, EXPRESS OR IMPLIED. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY *exida* IN NO EVENT SHALL *exida* BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This report does not constitute a recommendation, endorsement or guarantee of any of the hardware or software products tested or the hardware and software used in testing the products.

The certification does not guarantee that there are no defects or errors in the products. It does not guarantee that the products will meet your requirements, expectations or specifications or that they will operate without interruption.

This report does not imply any sponsorship, endorsement, affiliation or verification by or with any company mentioned in the report.

All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners. No endorsement, sponsorship, affiliation or involvement in either the testing, the report or *exida* is implied nor should it be inferred.

6.2 Revision History

Revision	Date	Author	Details
V0R1	04/03/2022	Shalom Nazir	Initial draft
V1R1	08/03/2022	Shalom Nazir	Finalized document

6.3 Future Enhancements

At request of client.

6.4 Release Signatures

S Shalom Nazir, Evaluating Assessor

David Johnson, Certifying assessor