ISASecure® SDLA

Assessment Report

Target of Evaluation:
Security Development Lifecycle Process

Company:
Valmet Automation Oy
Tampere
Finland

Contract Number: Q22/05-333
Report No.: VAL 2205333 R001
Version V1, Revision R1, November 15, 2022
David Johnson, Bill Thompson

Table of Contents

1 Management summary

This report summarizes the results of the surveillance security assessment conducted by the ***exida*** between August and November of 2022, of the Security Development Lifecycle used by Valmet Automation Oy for the development lifecycle activity defined in the scope section of this document. This assessment was carried out in accordance with the ISASecure® Security Development Lifecycle Assurance (SDLA) 3.0.0 Certification criteria as documented in SDLA-300 [N1], for ISASecure as requested by the client. The assessment was performed by:

exida
80 N. Main Street
Sellersville, PA 18960

The result of this ISASecure audit indicates the development lifecycle activity as described in the scope section employs a process compliant with the IEC 62443-4-1 requirements as evaluated under the ISASecure SDLA program

As a process audit this does not automatically certify any product that is developed using this process. When product certifications are conducted, only product artifacts must be assessed, no process reviews will be needed.

2 Purpose and Scope

This report summarizes the results of the security assessment of the secure product development lifecycle (SDL) Process used by Valmet Automation Oy performed by ***exida***. This assessment applies to the following SDL process:

- Valmet Automation Oy Security Development Lifecycle Process Version 2.0 or later

This certification applies to the Automation Systems Business Line, for development performed at all locations. As stated in the Valmet Automation Oy Security Development Lifecycle Process Version 2.0 or later, development activities in these organizations for all products in the commercial product line that offer a wireless or Ethernet connection, are subject to the SDL.

For requirements assessed using a full SDLA evaluation, artifacts as required by SDLA-312 that demonstrate adherence to the IEC 62443-4-1 standard, are collected from a variety of products developed using the secure product development lifecycle.

This report should allow the user to answer the following questions:

- Can this organization develop products that can be used securely and are capable of being certified to the CSA (Component Security Assurance) or SSA (System Security Assurance) programs?
- Does this organization have a process to respond to and fix security vulnerabilities in a timely fashion?
- Does this organization have a process for anyone to be able to report a security vulnerability on one of its products?
- Does this organization document user guidelines on how to ensure that its products or systems are being operated in the most secure manner?

3 Project Management

The assessment was performed by:

exida
80 North Main Street
Sellersville, PA, USA 18960

3.1 Roles of the parties involved

Valmet Automation Oy	Manufacturer of the products defined in the scope section
exida	Performed the security assessment according to ISCI approved methods

3.2 Standards and Literature used

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

[N1]	SDLA-300, Version 1.9, June 2020	ISA Security Compliance Institute – Security Development Lifecycle Assurance – ISASecure certification and maintenance of certification requirements
[N2]	SDLA-100, Version 2.0, June 2020	ISA Security Compliance Institute — Security Development Lifecycle Assurance – ISASecure certification scheme
[N3]	SDLA-312, Version 5.7, June 2020	SDLA-312 ISCI Security Development Lifecycle Assurance - Security Development Lifecycle Assessment v5.5
[N4]	ANSI/ISA-62443-4-1	ANSI/ISA-62443-4-1-2018 Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements
[N5]	IEC 62443-4-1:2018	IEC 62443-4-1-2018 Security for industrial automation and control systems Part 4-1: Secure product development life-cycle requirements

3.3 Reference documents

3.3.1 Documentation provided by Valmet Automation Oy

The ***exida*** repository used for this project contains snapshot documents from the Valmet Automation Oy that were reviewed as part of this assessment . The security case associates the documents with the requirements in the standard.Client supplied documentation used for this assessment are covered by Non-Disclosure Agreement and are not generally available for user inspection.

3.3.2 Documentation generated by *exida*

[R1]	(security case)	*exida* Security Development LifecycleAssessment Audit
[R2]	VAL2205333 SDLA 3.0.0 Assessment Report V1R1.docx, 2022-11-16	ISASecure Certification Report for Valmet Automation Oy (this report)

Documents [R1] through [R2] are covered by Non-Disclosure Agreement and are not generally available for user inspection.

4 Results of the Certification Assessment

4.1 Security Management (SM)

Pass

The Valmet 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 either up to date on training or scheduled for training in next 3 months.

ID	Requirement	Type of evaluation	Results
SM-1	Development Process	Full	Passed
SM-2	Identification of Responsibilities	Full	Passed
SM-3	Identification of applicability	Full	Passed
SM-4	Security expertise	Full	Passed
SM-5	Process scoping	Full	Passed
SM-6	File Integrity	Full	Passed
SM-7	Development environment security	Full	Passed
SM-8	Controls for private keys	Full	Passed
SM-9	Security requirements for externally provided components	Full	Passed
SM-10	Custom developed components from third-party suppliers	Full	Passed
SM-11	Assessing and Addressing security-related issues	Full	Passed
SM-12	Process verification	Full	Passed
SM-13	Continuous Improvement	Full	Passed

4.2 Specification of Security Requirements (SSR)

Pass

The secure product development lifecycle calls for security requirements to be documented as part of the overall product requirements. The Valmet's processes identifying system scope and boundaries were present. Product artifacts were examined and found to accurately document scope both physically and logically, and to clearly outline security requirements. In addition, threat modeling is required by the process. The process for threat modeling was reviewed and found to be compliant with the standard, and several example threat models were reviewed as well.

ID	Requirement	Type of evaluation	Results
SR-1	Product security context	Full	Passed
SR-2	Threat model	Full	Passed

ID	Requirement	Type of evaluation	Results
SR-3	Product security requirements	Full	Passed
SR-4	Product security requirements content	Full	Passed
SR-5	Security requirements review	Full	Passed

4.3 Secure by Design (SD)

Pass

The secure product development lifecycle includes the standards and guidelines needed for the creation of a modular design of products. Examples of design concepts included were:

- Secure Design Best Practices
- Design of Security functions
- External interface hardening
- Defense in Depth Design
- Attack surface reduction

ID	Requirement	Type of evaluation	Results
SD-1	Secure design principles	Full	Passed
SD-2	Defense in depth design	Full	Passed
SD-3	Security Design Review	Full	Passed
SD-4	Secure design best practices	Full	Passed

4.4 Secure Implementation (SI)

Pass

The Valmet secure product development lifecycle includes standards and guidance on the development of code which was reviewed for:

- Coding standards that discuss security concerns
- Banned code constructs and functions that pose a security risk
- Guidance for code reviews and static analysis
- Guidance for the use of code developed elsewhere (COTS)

Projects were audited to confirm that code review and static analysis were being performed as required.

ID	Requirement	Type of evaluation	Results
SI-1	Security implementation review	Full	Passed
SI-2	Secure coding standards	Full	Passed
SI-2G	Periodic update of security recommended processes	Full	Passed

ID	Requirement	Type of evaluation	Results
SI-3	Applicability to systems level code.	Full	Passed

4.5 Security Verification and Validation Testing (SVV)

Pass

In addition to product functional testing the Valmet secure product development lifecycle included validation planning focused on the security requirements. All procedures, test cases, and results were documented. In the audited products, all security requirements were validated by one or more tests. The assessment found processes were in place that outlined how Communication Robustness Testing (CRT) was performed involving automated test case generation and protocol fuzzing. This 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.

ID	Requirement	Type of evaluation	Results
SVV-1	Security requirements testing	Full	Passed
SVV-2	Threat Mitigation Testing	Full	Passed
SVV-3	Vulnerability testing	Full	Passed
SVV-4	Penetration Testing	Full	Passed
SVV-5	Independence of Testers	Full	Passed

4.6 Security Defect Management (DM)

Pass

Procedures are specified for handling security-related issues of a product. Procedures document the process to capture reported security issues and track them to closure in a compliant manner. Impact analysis of new security issues includes root cause analysis to identify potential threats. Newly identified issues are ranked and are required to be addressed in the design if they are determined to be of high enough criticality. Valmet Automation Oy has a public mechanism to report suspected vulnerabilities to its customers.

ID	Requirement	Type of evaluation	Results
DM-1	Receiving notifications of security-related issues	Full	Passed
DM-2	Reviewing security-related issues	Full	Passed
DM-3	Assessing security-related issues	Full	Passed
DM-4	Addressing security-related issues	Full	Passed
DM-5	Disclosing Security Related Issues	Full	Passed
DM-6	Periodic review of security defect management practice	Full	Passed

4.7 Security Update Management (SUM)

Pass

The Valmet secure product development lifecycle provided for a managed response to vulnerabilities reported from external sources. This was outlined in a detailed procedure posted on the client web site 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 updates. In addition, a process described a proactive approach for raising the awareness of new vulnerabilities and addressing them before they impacted field equipment.

ID	Requirement	Type of evaluation	Results
SUM-1	Security update qualification	Full	Passed
SUM-2	Security update documentation	Full	Passed
SUM-3	Dependent component or operating system security update documentation	Full	Passed
SUM-4	Security update delivery	Full	Passed
SUM-5	Timely delivery of security patches	Full	Passed

4.8 Security Guidelines (SG)

Pass

Security Guidelines are created based on a checklist that is part of the Security Plan template. The checklist is used to ensure that user documentation includes the required content including the defense in depth measures expected to be supplied in the environment where the product is installed. Security guideline documentation is reviewed to ensure that the required content has been included. The process also requires all user documentation to be reviewed by security experts to ensure that secure practices are described and that no insecure practices are recommended.

ID	Requirement	Type of evaluation	Results
SG-1	Product defense in depth	Full	Passed
SG-2	Defense in depth measures expected in the environment	Full	Passed
SG-3	Security hardening guidelines	Full	Passed
SG-4	Secure disposal guidelines	Full	Passed
SG-5	Secure operation guidelines	Full	Passed
SG-6	Account management guidelines	Full	Passed
SG-7	Documentation review	Full	Passed

5 Summary Results of Certification Assessment

This report summarizes the results of the security assessment of the Security Development Lifecycle according to ISASecure criteria.

The result of this ISASecure audit indicates the documented security development lifecycle generally complies with the IEC 62443-4-1 requirements as evaluated under the ISASecure SDLA certification program.

In addition, some or all 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 secure product development lifecycle being compliant. However, this does demonstrate that security is being considered as products are modified, and that Valmet Automation Oy has the capability to develop and maintain compliant products in the future.

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.

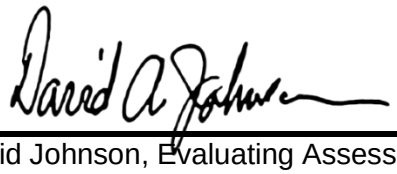
6.2 Revision History

Revision	Date	Author	Details
V0R1	9 Nov 2022	David Johnson	Initial draft
V1R1			Updated based on review.

6.3 Future Enhancements

At request of client.

6.4 Release Signatures



David Johnson, Evaluating Assessor

Bill Thomson, Certifying Assessor