Pacific Northwest
NATIONAL LABORATORY

PNNL- 36365

Solar Industry Manufacturer Experience with The SD2-C2M2 Assessment Tool

August 2024

Scott R Mix

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

Acknowledgment:

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Solar Energy Technologies Office Award Number 38451.

1.0 Introduction

1.1 Approach

The Pacific Northwest National Laboratory (PNNL) offered facilitated cybersecurity maturity self-assessments of several manufacturers or vendors of solar-related products as part of the U.S. Department of Energy's (DOE) Solar Energy Technology Office (SETO) Securing Solar to the Grid (S2G) project. The assessments were conducted using PNNL's Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) tool. SD2-C2M2 is part of the maturity model framework developed by PNNL[1], and uses the same underlying tool infrastructure as is used by other maturity model assessment tools.

The SD2-C2M2 tool is web browser based, running on computers managed by the manufacturer, with no data being shared with PNNL except when explicitly shared by the manufacturer. Non-disclosure agreements (NDA) were put in place to protect the information discussed by the manufacturer during the assessment[2], along with any follow-on discussions regarding interpretation of the results of the assessment.

The intent of the assessments is to determine the maturity level of the manufacturer's cybersecurity policies and practices, compare the maturity levels with expected maturity levels as identified by the manufacturer's management, and using the SD2-C2M2 tool's reporting and analysis component, produce a gap analysis indicating which practices had not met management's expectations. At this point, the manufacturer can develop a plan to remedy the gaps and re-perform the assessment after the remediations are put into place and can optionally modify the expected maturity levels.

The tool is intended to be periodically re-run (e.g., annually) so that results can be assessed and progress to increasing maturity levels can be compared.

1.2 Process

PNNL, working with the National Renewable Energy Laboratory (NREL), initially identified a total of 25 potential manufacturers and vendors of equipment used in the solar industry for the assessment. Initial outreach resulted in responses from 10 manufacturers. In many cases, the manufacturers were not interested in participating for a number of reasons, chief among them not having the time or resources to be able to complete the assessment. In two cases, access to the tool was provided to the manufacturer to allow them to review the tool for applicability, but no follow-on interest was expressed. In the end, three manufacturers expressed interest and completed some aspects of an assessment.

Each assessment began with a 2-hour presentation from PNNL. This presentation provided a brief history of the SD2-C2M2 tool development, an overview of maturity models, and an introduction to the tool itself. The presentation also provided information on the structure of the domains, objectives, and objective areas in the tool, as well as a mapping of the practices in

[1] See https://www.pnnl.gov/pnnl-maturity-models (accessed 06/10/2024)

[2] Note – NDAs for early assessments also covered the intellectual property of the SD2-C2M2 practice statements themselves, but during the task, PNNL determined that the tool would be made publicly available, so later assessment NDAs did not contain this language.

standard IEC/ISA 62443-4-1[1] to the practice statements in the tool. The manufacturers were then provided a password which gave them access to the SD2-C2M2 tool, and time permitting, PNNL assisted the manufacturer to walk though initial responses to the management selection criteria and the practice statements contained in the tool's core assessment. In some cases, PNNL continued to facilitate the assessment, but in many cases, the manufacturer continued the self-assessment without any further facilitation. PNNL remained available to address any questions that the manufacturer raised concerning the meaning of any practice statements.

Once the assessment was completed, PNNL was available to help the manufacturer review the results of the assessment, using both the dynamic results in the web-based tool, as well as the static results from the PDF report that the tool can automatically generate.

In parallel with the assessment conducted for the S2G project, a user's guide and additional documentation is being developed to allow non-facilitated assessment to be more readily performed. A significant component is a detailed explanation of each practice statement, along with examples and implementation guidance for many practices to assist with understanding each practice statement without the need for a trained facilitator. When complete, these documents will address several issues raised by participants and assist future participants.

2.0 Use Cases and experiences

The following sections of the report provide a brief overview of the lessons learned and experiences from the three participants that participated in the assessment and provided specific feedback. The attributed material presented here is being included with the permission of the participants.

2.1 Operant

The first assessment of a manufacturer in the Solar DER space using the Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2) tool was completed in July 2022. The participant, Operant Networks (https://operantnetworks.com/), is an early-stage startup developing secure communication solutions for distributed energy sites. An NDA was in place to protect discussions regarding Operant’s design and development practices, as well as any intellectual property contained in the assessment tool.

The analysis was completed in approximately eight to ten hours of facilitated interactions, including a PowerPoint introduction to the tool, management desired maturity level selection, and performing the core assessment that involved responding to the practice statements. Operant’s team spent additional time outside the facilitated assessment reviewing responses and “working ahead” responding to practice statements. Once the core assessment was completed, an additional three facilitated hours was used review and discuss the results from the assessment using the tool-generated report.

[1] While not heavily used in the U.S., the IEC/ISA 62443 standard is expected or required in many European and Asian markets, and multi-national manufacturers have shown interest in how the SD2-C2M2 practice statements map to the practices in IEC/ISA 62443. It is comprised of many individual standards; IEC/ISA 62443-4-1 *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements* is the specific standard that deals with design and development processes, and is the only standard from the IEC/ISA 62443 standard family that has been mapped to the SD2-C2M2 practice statements.

In general, Operant was pleased with the assessment and found the process valuable.

> "The SD2-CM2 tool is flexible, comprehensive, and painless. It accounts for senior management's business priorities and allows focus to be put on areas of the most importance and relevance. The output of our evaluation was accurate and actionable. We are already using the results to further improve engineering and quality standards. We plan to reassess periodically, measure our progress, and make adjustments as necessary. Kudos go to the PNNL team for making this tool available to the industry." – Andrew Bartels, Operant VP of Engineering

The results accurately captured strengths in areas that Operant had developed and documented procedures providing a clear baseline that Operant can use to assess improvement, and identified gaps in areas where Operant had not developed any procedures and acknowledged there were deficiencies. Using the management selection process, Operant was able to focus on gaps that were seen as critical, while simultaneously identifying where existing capabilities are. Operant also noted that the tool can assist in identifying practice areas that address organizational misalignment between developers or departments in the organization.

Operant also provided feedback and suggestions on tool improvements which have been added to the PNNL development backlog for future development activities.

Operant was also very open about their experiences with the SD2-C2M2 tool and assessment process, allowing PNNL to publicize their participation while attempting to recruit other participants, and provided a public discussion of their experiences at industry meetings related to the S2G project. Operant also gave presentations on their experience using the SD2-C2M2 tool at both the S2G Industrial Advisory Board meeting in Las Vegas, NV on September 14, 2023, as well as at the DOE Energy Transition Summit in Arlington, VA on February 7, 2024.

Operant is planning on conducting bi-annual assessments, with annual re-evaluation of management expectations.

2.2 Lumian Foundation

The second manufacturer assessment performed under the S2G project was a review of the practices in the SD2-C2M2 tool performed in January 2024. The participant, the Lumian Foundation, is the governing body of Lumian (https://www.lumian.org/), a distributed computing platform optimized for security. Lumian’s mission is to secure and streamline the digital supply chain, starting with distributed energy. An NDA was in place to protect discussions regarding Lumian's design and development practices, as well as any intellectual property contained in the assessment tool.

Lumian was not ready to perform a full assessment within the timeframe of the S2G project. However, they were able to review the practice statements and provide a set of comments, questions, and concerns to PNNL for several practice statements. PNNL provided a written response to the Lumian's comments. Following this interaction, Lumian created a cybersecurity policy based on the content of some of the practice statements. As expected, their cybersecurity policy is much more detailed and prescriptive than the practice statements but covers many of the same topics.

Since Lumian did not complete the assessment using the SD2-2M2 tool, no follow-on discussions pertaining to understanding the tool results were held.

As part of their comments, Lumian expressed several concerns with the content of the practice statements and how they relate to current software development methodologies such as the Agile software development methodology[1], and concerns about using open source. Some of this was due to the lack of understanding by Lumian staff and an explanation of the individual practices by PNNL staff, using extracts from the under-development documentation for the assessment, addressed the issue somewhat. However, other criticism may require a re-evaluation of some of the practice statement assumptions, particularly for different development methodologies, and how these methodologies can or should be applied to development processes for critical infrastructure components or systems. Further research into this area is warranted.

2.3 Lastwall

The third and final manufacturer assessment performed under the S2G project was completed in April 2024. The participant, Lastwall (https://www.Lastwall.com/), is an early-to-mid stage startup delivering a range of highly secure, identity-centric, and quantum resilient cybersecurity software solutions designed for compliance driven and threat intensive environments in defense, government, and critical infrastructure sectors. Lastwall's mission is to protect democratic institutions by strengthening the cybersecurity posture of government, defense, and critical infrastructure partners. Its solution is deployed with the U.S. Deptartment of Defense (DoD), Defense Innovation Unit, and as such is subject to the stringent DoD cybersecurity requirements and audits. An NDA was in place to protect any potential discussions or SD2-C2M2 responses regarding Lastwall's design and development practices; however, by the time the NDA was put into place for Lastwall, PNNL no longer included protecting the intellectual property of the practice statements in the tool.

Lastwall completed the full self-assessment in approximately eight to ten hours. At the time of the assessment, Lastwall had already completed a significant number of control-related documentation related to US Dept. of Defense Impact Level 4 and FedRAMP Moderate authorizations – the controls of which had medium to significant overlap with the SD2-C2M2 assessment. Given the Lastwall team's recent familiarity with its procedures, and its company and product focus on security and compliance, much of the information included in the SD2-C2M2 assessment was readily available. Once the core assessment was completed, an hour was used to review and discuss the results from the assessment using the tool-generated report. They were able to complete the assessment without any facilitation support from PNNL.

The Lastwall team was grateful to have had the opportunity to complete the self-assessment, and some valuable learnings were developed in the process. Specifically, documentation gaps were identified to which the team can more effectively develop evidence of control-based compliance.

> "The [SD2-]C2M2 tool was efficient and effective in helping our company identify gaps in our compliance and documentation framework. We were able to rapidly complete the assessment, learn from the results, and improve. As we expand our product offering and customer base in the broader energy sector, this tool brings with it greater evidence and

[1] See https://www.atlassian.com/agile (accessed 06/10/2024)

> validation related to our focus on security and compliance” – Shawn Moorhead, Vice President of Market and Business Development.

Lastwall is hoping to use the SD2-C2M2 results as sales and marketing collateral to demonstrate the security orientation of their product and company as they expand beyond the Dept. of Defense into working with groups in the energy sector.

No follow-on discussions took place, as Lastwall did not pose any questions concerning the SD2-C2M2 tool results.

2.4 Others

Several other manufacturer organizations expressed initial interest in the SD2-C2M2 tool and were provided access in order to evaluate it. However, limited or no additional feedback was provided to PNNL. Attributions are not provided for these manufacturers.

One potential participant noted that they "see great value in the tool and wish PNNL would extend the support provided to new users." However, the assessment timeframe and other pressing issues did not allow them to perform an assessment during the project timeframe, but they are likely to perform a self-assessment in the future.

Another potential participant expressed concerns over the "guided assessment" process that was proposed, citing issues with release of intellectual property that they were unsure that an NDA would address. The additional documentation being developed as part of another project can greatly reduce the need for a guided assessment by providing the content of the "guidance" (i.e., the PNNL-provided explanation of the practice statements and their context) as a standalone document that can be provided to participants to significantly reduce the need for a facilitated or guided assessment.

Another potential participant expressed interest in performing the assessment but was unable to allocate or schedule resource to participate due to other commitments.

Yet another potential participant was nearly ready to perform an assessment when they had a significant personnel turnover, the champion for performing the SD2-C2M2 assessment at the company left, and the remaining staff were focused on recovering from the personnel loss rather than performing an assessment. An NDA was put in place in anticipation of the assessment, but no assessment was performed.

Several other manufacturers (approximately 14) were contacted about participation, and while one or two responded to request emails and declined to participate, most were unresponsive.

These manufacturers may revisit performing an unfacilitated assessment once the user's guide and additional documentation is completed.

3.0 Conclusion

The participants in the assessment generally found the tool useful and were able to either identify or validate gaps in their cybersecurity practices or validate that their cybersecurity practices were generally complete. Operant, as the first organization to perform an assessment. has been able to perform several iterations of the assessment process to assess whether their maturity level has improved over time and plans to continue performing biannual technical assessments with an annual reassessment of management priorities. Lumian did not provide comments on their future uses of the SD2-C2M2 tool. Lastwall intends on publicizing their use of the tool in marketing material.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov