Standardizing Open Source License Compliance With OpenChain

Shane Coughlan, Linux Foundation

This article explores the intersection between open source and standards. The OpenChain Project submitted a specification to the ISO/IEC JTC1 PAS Transposition Process in early 2020 for review. The methodology applied and the lessons learned are explained along with observations of the implications for projects moving forward.

Digital Object Identifier 10.1109/MC.2020.3016107
Date of current version: 21 October 2020

Open source has become a prominent, if not the most prominent, method of developing software. This is especially true when dealing with technology like operating systems that provide the foundation for building products but do not provide a competitive advantage per se, as that advantage lies in the layers of code that execute over the foundation. The increased prominence of open source in all aspects of product and service deployment has pushed increased standardization throughout the field. The first phase focused on de facto standardization where successful approaches to frameworks quickly became industry norms. The second phase is now underway where de facto standards become more traditional, formal international standards. This development reflects the increased emphasis on making open source available and adoptable by the widest audience possible and acknowledging

0018-9162/20©2020IEEE

EDITOR DIRK RIEHLE
Friedrich Alexander-University of Erlangen Nürnberg;
dirk.riehle@fau.de

FROM THE EDITOR

In the eyes of many, collaboration is an important part of open source, more so than the licenses. Hence, why not solve the problems created by open source license compliance through open collaboration among the involved parties? In this column, for instance, Shane Coughlan, of the Linux Foundation, explains how companies have come together to define the OpenChain set of standards and practices to get a handle on open source license compliance. Interested parties can use OpenChain as a guide to ensure that their own handling of open source and that of their supply chain is safe and effective. Learn more in this article! — *Dirk Riehle*

that the framework solutions developed in open source are likely to impact each technology area for years to come.

THE OPENCHAIN PROJECT

The OpenChain Project develops a specification and associated reference material that describes and provides examples of quality open source license compliance programs. It demystifies the methodology of managing the legal side of open source and, as such, assumes a natural position of the first international standard fostered by the Linux Foundation in 14 years. It is also the first international standard submitted to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 Publicly Available Specification (PAS) transposition process via the Joint Development Foundation (JDF), an organization that supports the practical process of converting de facto standards into formal ones in the years to come. This article will explore how and why this came to be and explain what it means for the software industry at large. The focus is on processes used, lessons learned, and how this is applicable to a wide range of software development, specification creation, and interoperability projects. The OpenChain standard targets open source licensing and compliance, but the experience of drafting, deploying, and then maturing to formal standardization contains lessons for all types of project. As with the OpenChain standard for open source compliance itself, the emphasis is entirely on real-world challenges and solutions.

Open source has its origins in the 1980s and gained significant corporate investment in the late 1990s, with open source compliance in the commercial sphere underpinning growing adoption. From the open source definition to the documentation published by the Free Software Foundation, there is a wealth of material to guide potential and current users of open source through the terms they must follow. However, the available material skewed toward individual organizations rather than multiple entity solutions, and there was no single path to compliance suitable for businesses of differing sizes and in differing markets. The OpenChain Project addresses this gap in the market by describing the key components of a generic but quantitative open source compliance program. It does this by outlining the inflection points where learned experience shows processes should exist. Distilled to its essence, implementing processes at these inflection points reduces errors and makes remediation simpler.

THE OPENCHAIN SPECIFICATION

The OpenChain Specification has seen exceptional engagement and adoption since its launch three years ago. Pent-up demand to simplify supply chain process management underpins this alongside its inherently uncontroversial structure. Its focus on practicality without undue prescription solicits a positive reaction rather than skepticism, a key aspect of bringing different, often competing, entities together in any field. The lack of a significant number of companies capable of achieving individual excellence in matters of compliance and, without the available companies coming together to distill that learned experience, it would be hard to offer a market standard with the requisite gravitas.

OpenChain's strategic goals extend beyond individual company applicability and adoption. Although the OpenChain Specification defines the process inflection points for the inbound, internal, and deployment management of open source licensing on a company basis, the targeted goal is to create chains of conformant companies and gradually facilitate entire supply chains that provide greater clarity, confidence, and remediation potential when it comes to open source compliance. The reasoning behind this approach is purely pragmatic. There is no single company large enough to effectively mandate and enforce a singular approach to open source compliance across a large supply chain, and likewise there is no singular method of cooperative application for an approach that can obtain immediate results. The effective solution was to put in place the mechanisms necessary to improve the situation for all stakeholders in a pragmatic manner that retains a clear vision for the desired destination.

There are two questions that immediately arise when the existence of the OpenChain Specification is made known: how do we know this can work, and how can companies adopt it in practice? The very existence and sustainability of the OpenChain Project proves the former. Since its public launch in October 2016, and in the two formative years prior, the project has been led exclusively by user companies pooling their knowledge around open source compliance. Whether discussing successes or the challenges faced, more than 100 contributors to the final specification sought to distill what works into the smallest standard possible. In subsequent years, a great deal of additional feedback has been received and incorporated from entities around the world, leading to a series of updates of the initial standard to improve clarity and translatability.

The second question is more nuanced. Companies differ dramatically in their knowledge and applied experience to questions related to open source management processes. Partly this is due to market dynamics, with different sectors requiring different approaches, but largely it is due to varying maturity by entities or even segments with respect to the practical adoption, development, and deployment of open source code. The OpenChain Project addresses this through reference material. There are currently more than 400 reference documents available to companies seeking to adopt the OpenChain Specification, and this materially is equally useful for more singular activities related to compliance. Two examples are the Reference Training Slides, which encompass core concepts from "what is intellectual property" through to examining tooling options, and the policy template, which helps guide companies through a series of action items to determine appropriate policy approaches.

The existence of the OpenChain Project and the OpenChain Specification marks a significant step forward in open source compliance. In the three years that it has been in market, we have seen the emergence of local and global communities coalescing around a single approach to manage openly licensed code in their workflows. Today, there are local work groups in China, Japan, Korea, Taiwan, India, Germany and, as of 23 July 2020, the United Kingdom, most of which meet quarterly. There are global work groups focused on reference tooling and the automotive space, with the former meeting biweekly and the latter on a quarterly cadence, matching the local activities. There are biweekly global webinars, biweekly specification meetings, and active mailing lists, Slack channels, and a GitHub presence. OpenChain as a standard for compliance has fostered a hive of activity.

The adoption of the standard has spanned all industry sectors, from silicon to consumer electronics to automotive, and support of the standard has ranged for the formal application of personnel and fiscal resources through Platinum Membership—Bavarian Motor Works CarIT being the latest of 20—to the informal application of similar resources through the participation and support of community activities. A steady stream of conformance announcements has helped solidify the usefulness of the standard across sectors—the latest being Cisco and Fujitsu—and the emergence of a vendor ecosystem has illustrated the emergence of sustainable economics that will serve to ensure the standard has a place in product portfolios for many years to come.

The practical creation of an industry standard constitutes five distinct phases: formulation, initial drafting, community building, fostering adoption, and scaling.

However, there is a difference between an industry standard that appeals to and is adopted by an entrenched segment of a technology community and an international standard with immediate understandability and applicability to all companies potentially affected by a sphere of technology, whether it be hardware, software, or data. This nuance is the different between de facto and formal standards, and naturally, it is vitally important to address whether a nascent standard is to scale from hundreds to thousands of companies. The methodology of doing so is well established, constituting a submission to an international standardization body and the subsequent publication of the standard under their auspices. This may occur via a regional body such as ECMA or via a global body such as ISO. The OpenChain Project, as an international standard, has elected for the latter.

The OpenChain Specification entered the ISO/IEC JTC1 PAS transposition process, a method of converting de facto industry standards into formal international standards in a relatively short timescale. It focuses on existing standards rather than the creation of new ones and is managed by a range of PAS submitter organizations around the world. In the case of the OpenChain Project, the PAS submitter in question is the JDF, a sister activity under the auspices of the Linux Foundation. This allows a close relationship and a degree of understanding that benefits expediency with a strong foundation of knowledge. The OpenChain Specification Draft International Standard (DIS) ballot was scheduled to conclude on 23 September 2020, and unless voting and comments require an additional Final Draft International Standard ballot, publication as an ISO/IEC international standard commences within six weeks. Meanwhile, the OpenChain Specification is in the ISO database as DIS 5230.

The targeted result is that by late third quarter or early fourth quarter of 2020, the OpenChain Specification will obtain an ISO/IEC standard number that fits into existing processes used by sales, procurement, and related business departments. The nuance here is important. Bespoke approaches to managing intellectual property solve individual organization challenges, but it is less understood what common approaches are equally useful, especially if they potential require adjustments to existing processes. Although many companies have Open Source Program offices, they are rarely able to talk to sales and procurement on an even footing and rely on the sophistication and willingness of key individuals managing copyright and patents in legal departments to act as a bridge. An oft-cited albeit informal goal of the OpenChain Project is to "reduce 12 pages of bespoke open source sales or procurement requirements down to saying, 'use this standard'," but to realize such as aspiration is far easier through a respected standards body than via a de facto industry standard, regardless of how well received and adopted it may be.

It is tempting to frame the OpenChain Project and OpenChain Specification as pre-ISO/IEC and post-ISO/IEC, with the former around the emergence of the standard and the latter constituting the scaling of the standard globally. However, such a framing would give unfair relevance to other critical aspects in the development and deployment of the standard, not least because the OpenChain Project operates in a similar manner to an open source project, with all the advantages and challenges that entails. The practical creation of an industry standard constitutes five distinct phases: formulation, initial drafting, community building, fostering adoption, and scaling. The post-ISO/IEC situation for the OpenChain Specification is all about scaling, something supported by becoming an international standard, but depends on actual adoption. Indeed, the success of all standards truly belongs in the stages of community building and fostering adoption, both of which involve a mix of marketing and inclusiveness, with the latter often involving the inclusion of new ideas and potentially even new directions for an emerging standard.

The OpenChain Project set out to clarify this situation from its inception, by providing mailing lists, telephone conferences, and online spaces for existing and new participants to both obtain and contribute knowledge. At certain key points this proved crucial for the emergence of the standard, especially when entities from new market sectors provided feedback on assumptions that did not scale to their area and when entities operating in languages other than English highlighted phrasing that provided too little clarity to ensure fidelity in their geography. Such steps go far beyond accommodation and instead reflect an understanding that the initial people in the room are not always the smartest or most informed in the field, an understanding that is arguably not always at the forefront of young standardization initiatives. Clarity of vision infused with humbleness is the key to any successful community.

The concept behind successful collaborative projects has been well served by the Linux Foundation for many years, which has an internal motto of being helpful, humble, and hopeful. This simple mantra, when internalized, has led to more than 1,400 companies collaborating across roughly 200 projects, ranging from code (the Linux Kernel) to specifications (the OpenChain Project). Company decisions about which project to support reflect practical market dynamics and the reality that no project has universal applicability. What is notable is that the methodology of collaboration fostered a methodology that scales. This, perhaps more than anything else, is at the heart of what makes open source work. It is not really about code, and it is not really about licenses. Open source is about providing a framework that allows people (and companies) to collaborate on an equal basis on projects of shared interest. From this perspective, open source enables one of the key tenants of successful economics, whereby parties who do not inherently trust each other may have a shared frame of referencing for pricing or access and conduct themselves appropriately.

Open source is about providing a framework that allows people (and companies) to collaborate on an equal basis on projects of shared interest.

There is a certain irony in stating that open source is not about licenses and then immediately returning to the topic of licensing, but that is what we must do when considering the governance of the systematic approach offered. With all parties being equal, open source provides a mechanism for resource scaling that would be unheard of otherwise, with wide ranges of parties contributing 3, or 2, or 1% of the total corpus of knowledge under consideration—whether code or otherwise—and obtaining 100% of the result. Free riders, obtaining 100% of the result while contributing 0% of the effort, are an inevitable side effect, although their lack of contribution eventually erodes their specific benefit from the corpus of material. However, parties who sidestep the licensing of the system provide a systemic risk. If any significant number of parties do not obey the terms of the licensing that provide the underlying governance structure of equal access, all parties will have eroded self-interest in continued engagement and contribution. Licensing is the check and balance to ensure that this does not happen, and open source compliance is the mechanism to accomplish this task.

The OpenChain Project is an example case of measured but determined consensus building with a clear strategic direction. The tactics chosen to support this strategy have avoided distraction and dilution. When adjacent but noncore concepts like the inclusion of security or export control come up, the discussions move to post-ISO review. If there is one key takeaway from the OpenChain journey it is that diffusion is the enemy of deployment. A project seeking to evolve from de facto to formal standardization needs to identify its unique core to succeed. The broader the range of activities the more difficult it will be to distill the clear borders and content of an international standard.

Seeking to standardize processes or code is a daunting prospect for a project without experience in that domain. However, the JDF is creating a pipeline of future standards, with a Software Bill of Materials specification called *SPDX* scheduled for after OpenChain, and software-related standards to follow in the coming year. JDF support services are available to any project with a de facto industry standard, including the early stages of assessing whether the proposed standard is mature enough to become an application. The OpenChain Project and its collaboration with JDF has shown the potential of aligning open source and standards, an activity that is key to sustainable collaborative frameworks, and it opens the door to other projects in their own lifecycle of adoption and growth. The task remaining is to encourage more projects to discuss the creation of international standards that complement existing standards, a process that will benefit all market participants.

SHANE COUGHLAN is with the Linux Foundation. Contact him at scoughlan@linuxfoundation.org.

Digital Object Identifier 10.1109/MC.2020.3027331