Open Data **Standards** for Open Source Software Risk Management **Routines**: An Examination of SPDX

Georg Link

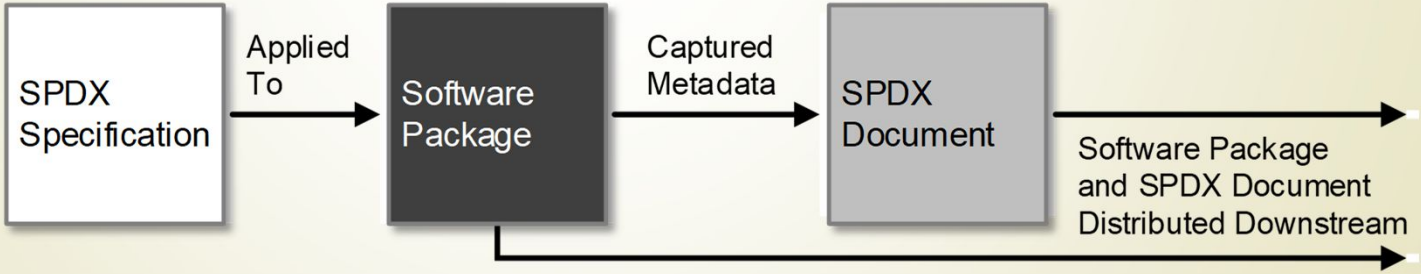
Coauthors: **Robin Gandhi** and **Matt Germonprez**

GROUP 2018, Sanibel Island, Florida, USA

Paper https://doi.org/10.1145/3148330.3148333

The SPDX Specification

- "The Software Package Data Exchange® (SPDX®) specification is a **standard format** for communicating the components, licenses and copyrights associated with software packages." - www.spdx.org



This repository Search Pull requests Issues Marketplace Explore

torvalds / linux

Watch 6,031

Code Pull requests 192 Projects 0 Insights

Branch: master linux / COPYING

torvalds/linux is licensed under the
GNU General Public License v2.0

The GNU GPL is the most widely used free software license and has a strong copyleft requirement. When distributing derived works, the source code of the work must be made available under the same license. There are multiple variants of the GNU GPL, each with different requirements.

Permissions	Limitations
✓ Commercial use	✗ Liability
✓ Modification	✗ Warranty
✓ Distribution	
✓ Private use	

This is not legal advice. Learn more about repository licenses.

License File

Pekka J Enberg [PATCH]

0 contributors

357 lines (292 sloc) | 18.3 KB

```

  NOTE! This copyright does *not* cover user programs that use kernel
 services by normal system calls - this is merely considered normal use
 of the kernel, and does *not* fall under the heading of "derived work".
 Also note that the GPL below is copyrighted by the Free Software
 Foundation, but the instance of code that it refers to (the Linux
 kernel) is copyrighted by me and others who actually wrote it.

 Also note that the only valid version of the GPL as far as the kernel
 is concerned is _this_ particular version of the license (ie v2, not
 v2.2 or v3.x or whatever), unless explicitly otherwise stated.

                        Linus Torvalds

----------------------------------------

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991
```

This repository Search Pull requests Issues Marketplace Explore

torvalds / linux

Watch 6,031

Code Pull

Branch: master

torvalds/linux is li

GNU General

The GNU GPL is the most
requirement. When distri
made available under the
each with different requi

This is not legal advice. L

Pekka J Enberg [PA

0 contributors

357 lines (292 sloc)

```
1
2    NOTE! Thi
3   services by
4   of the kern
5   Also note t
6   Foundation,
7   kernel) is
8
9   Also note t
10  is concerne
11  v2.2 or v3.
12
13
14
15 ----------------------------------------
16
17                    GNU GENERAL PUBLIC LICENSE
18                       Version 2, June 1991
19
```

This repository Search Pull requests Issues Marketplace Explore

torvalds / linux

Watch 6,031

Code Pull requests 192 Projects 0 Insights

Tree: bafb0762cb linux / drivers / staging / rtlwifi / phydm / phydm.c

Ping-Ke Shih staging: r8822be: Add phydm mini driver

0 contributors

1987 lines (1672 sl

Short License Header

```
1                                                  ******************************************
2
3                    007 - 2016  Realtek Corporation.
4   *
5   * This program is free software; you can redistribute it and/or modify it
6   * under the terms of version 2 of the GNU General Public License as
7   * published by the Free Software Foundation.
8   *
9   * This program is distributed in the hope that it will be useful, but WITHOUT
10  * ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or
11  * FITNESS FOR A PARTICULAR PURPOSE.  See the GNU General Public License for
12  * more details.
13  *
14  * The full GNU General Public License is included in this distribution in the
15  * file called LICENSE.
16  *
17  * Contact Information:
```

This repository Search Pull requests Issues Marketplace Explore

torvalds / linux

Watch 6,031

Code Pull requests 192 Projects 0 Insights

Branch: master linux / drivers / gpu / vga / vgaarb.c

bjorn-helgaas vgaarb: Factor out EFI and fallback def

15 contributors

1513 lines (130

MIT License, not GPL

```
/*
 * vgaarb.  plements the VGA arbitration. For details refer to
 * Documentation/vgaarbiter.txt
 *
 *
 * (C) Copyright 2005 Benjamin Herrenschmidt <benh@kernel.crashing.org>
 * (C) Copyright 2007 Paulo R. Zanoni <przanoni@gmail.com>
 * (C) Copyright 2007, 2009 Tiago Vignatti <vignatti@freedesktop.org>
 *
 * Permission is hereby granted, free of charge, to any person obtaining a
 * copy of this software and associated documentation files (the "Software"),
 * to deal in the Software without restriction, including without limitation
 * the rights to use, copy, modify, merge, publish, distribute, sublicense,
 * and/or sell copies of the Software, and to permit persons to whom the
 * Software is furnished to do so, subject to the following conditions:
 *
 * The above copyright notice and this permission notice (including the next
 * paragraph) shall be included in all copies or substantial portions of the
 * Software.
 *
 * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
 * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.  IN NO EVENT SHALL
 * THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
 * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
 * FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
 * DEALINGS
 * IN THE SOFTWARE.
```

This repository Search

torvalds / linux

Code Pull requests

Tree: bafb0762cb linux / dr

Ping-Ke Shih staging: r8822b

0 contributors

1987 lines (1672 sloc) 50.7

```
/*******************
 *
 * Copyright(c) 2007
 *
 * This program is fr
 * under the terms of
 * published by the F
 *
 * This program is di
 * ANY WARRANTY; with
 * FITNESS FOR A PART
 * more details.
 *
 * The full GNU Gener
 * file called LICENS
 *
 * Contact Informatio
```

This repository Search

torvalds / linux

Code Pull requests

Branch: master lin

torvalds/linux is li

GNU General

The GNU GPL is the most
requirement. When distri
made available under the
each with different requi

This is not legal advice. L

Pekka J Enberg [P

0 contributors

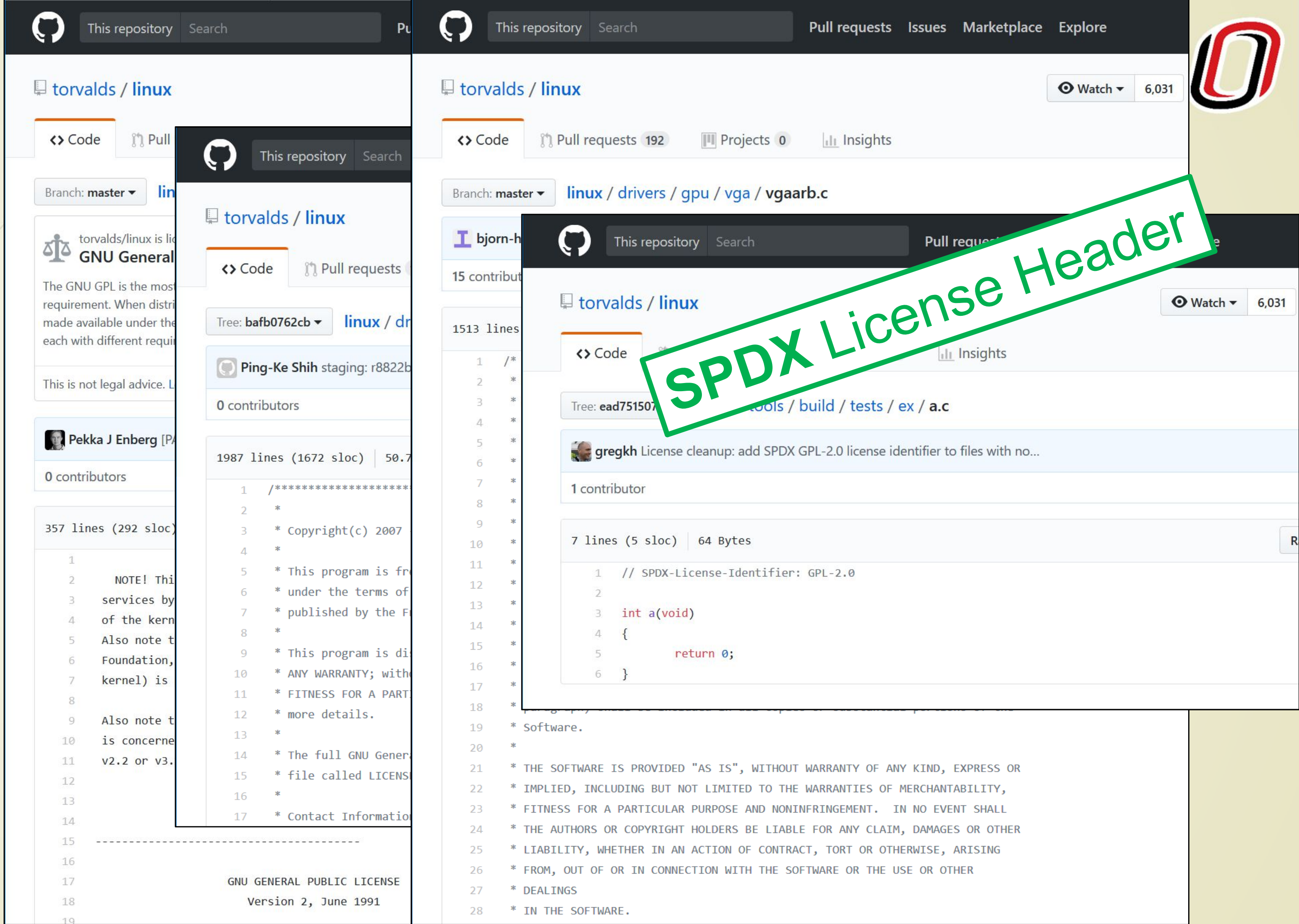
357 lines (292 sloc)

```
  NOTE! Thi
services by
of the kern
Also note t
Foundation,
kernel) is

Also note t
is concerne
v2.2 or v3.


--------------------------------------

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991
```



SPDX License Header

torvalds/linux is li

GNU General

The GNU GPL is the most
requirement. When distri
made available under the
each with different requi

This is not legal advice. L

Pekka J Enberg [PA

0 contributors

357 lines (292 sloc)

```

  NOTE! Thi
services by
of the kern
Also note t
Foundation,
kernel) is

Also note t
is concerne
v2.2 or v3.




 ------------------------------------------

                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991
```

Ping-Ke Shih staging: r8822b

0 contributors

1987 lines (1672 sloc) | 50.7

```
/********************
 *
 * Copyright(c) 2007
 *
 * This program is fr
 * under the terms of
 * published by the F
 *
 * This program is di
 * ANY WARRANTY; with
 * FITNESS FOR A PART
 * more details.
 *
 * The full GNU Gener
 * file called LICENS
 *
 * Contact Informatio
```

linux / drivers / gpu / vga / vgaarb.c

bjorn-h

15 contribut

1513 lines

```
/*
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *
 *

 * Software.
 *
 * THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 * IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
 * FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.  IN NO EVENT SHALL
 * THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
 * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
 * FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
 * DEALINGS
 * IN THE SOFTWARE.
```

ools / build / tests / ex / a.c

gregkh License cleanup: add SPDX GPL-2.0 license identifier to files with no...

1 contributor

7 lines (5 sloc) | 64 Bytes

```
// SPDX-License-Identifier: GPL-2.0

int a(void)
{
        return 0;
}
```

SPDX Community

- SPDX® (Software Package Data Exchange®)
- The vision of SPDX is to achieve license compliance with minimal cost across the supply chain
- SPDX community produces
  - License List
  - SPDX specification
  - Tools

OSS Risk Management Routines

Research Questions

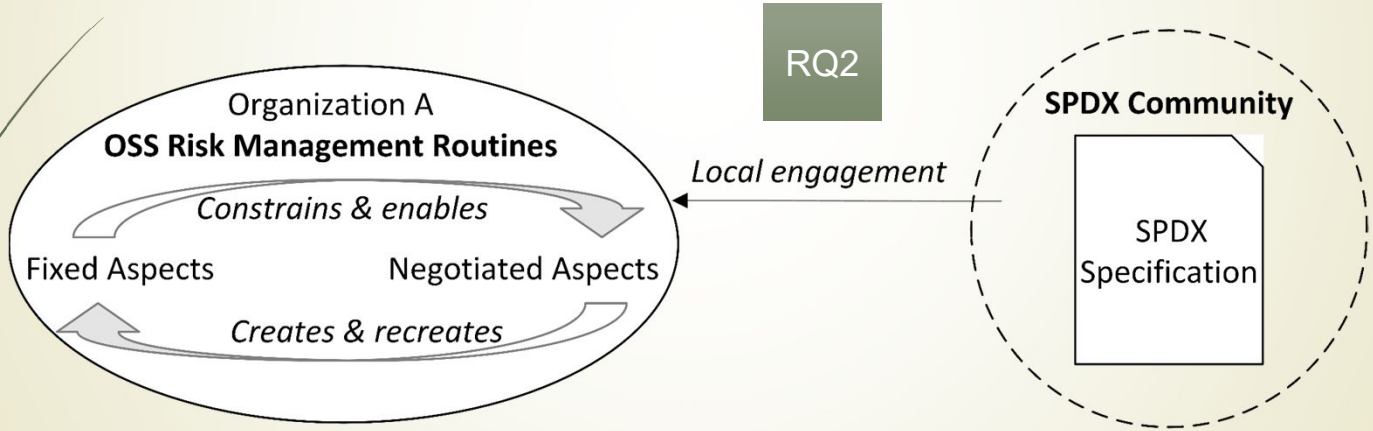
- RQ1: *How do organizations participating in the SPDX community describe their* **local interpretations** *of communally structured OSS risk management routines?*

Shared OSS Risk Management Routines In the Shared SPDX Standard Development

Research Questions

- RQ1: *How do organizations participating in the SPDX community describe their* **local interpretations** *of communally structured OSS risk management routines?*
- RQ2: *How do these local interpretations influence the extent of their SPDX* **adoption***?*

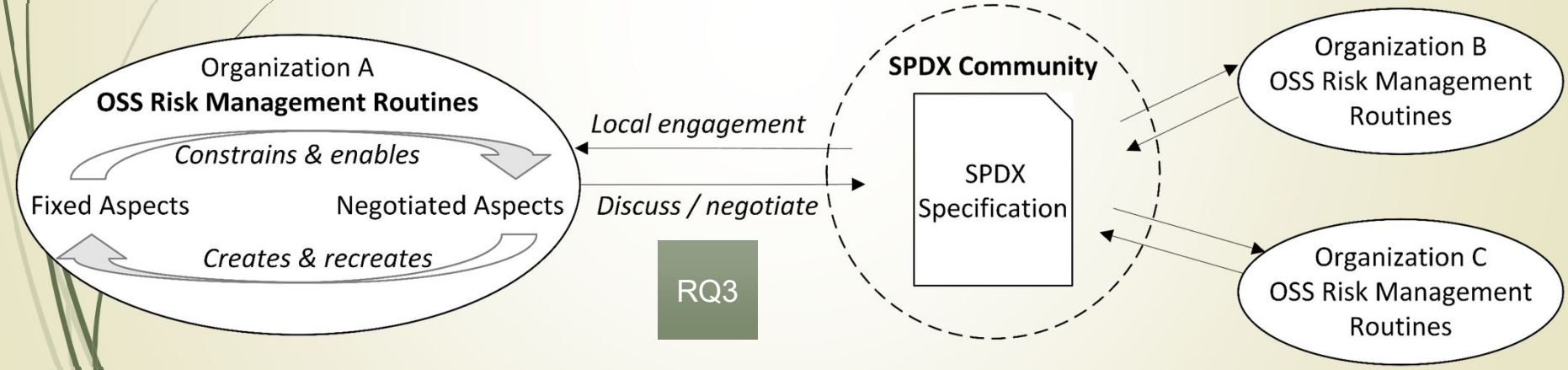
Shared OSS Risk Management Routines In the Shared SPDX Standard Development



Research Questions

- RQ1: *How do organizations participating in the SPDX community describe their* **local interpretations** *of communally structured OSS risk management routines?*
- RQ2: *How do these local interpretations influence the extent of their SPDX* **adoption***?*
- RQ3: *How do these member organizations seek to guide the* **advancement** *of the shared SPDX specification?*

Shared OSS Risk Management Routines In the Shared SPDX Standard Development



RQ3

Data Collection and Validation

- Assurance Case Method

- 16 Interviews
- 15 Organizations
- 10 hours of recording
- Field notes

Validation

- Focus Group with 15 SPDX members at Open Source Leadership Summit 2017

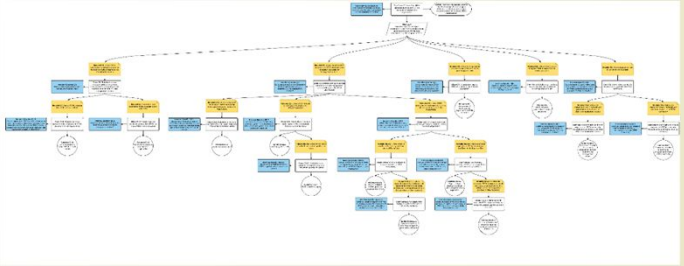
Interview Protocol

SPDX Case Study
IRB Approved: #473-19-EX

Main Interview Question:
In the context of software exchange, could you describe your organization's OSS risk management routines?

Follow-up questions:

Sense Making	**Q1**: How did your organization become familiar with or adopt SPDX?
Adoption Strategies	**Q1.1**: Can you speak about SPDX adoption strategies in your organization and how those strategies have been informed (i.e., through the SPDX website, discussions in the SPDX community, upstream and downstream vendors, or elsewhere)?
SPDX Use Cases	**Q1.2**: Could you describe SPDX-related use cases for your existing OSS risk management routines?
Compatibility	**Q2**: Could you comment on the compatibility of SPDX specification with your **existing** OSS risk management routines?
Usefulness	**Q2.1**: Approximately what percentage of SPDX fields are you currently using or plan to use? Could you comment on the use of these fields or the non-use of others?
Integration Points	**Q2.2**: Are SPDX fields used for enforcing automatic "gates" in the development build and release cycles? If yes, where would such "gates" be?
Tooling Feasibility	**Q2.2.1**: Are you using or custom developing SPDX compatible tools to support such "gates"?



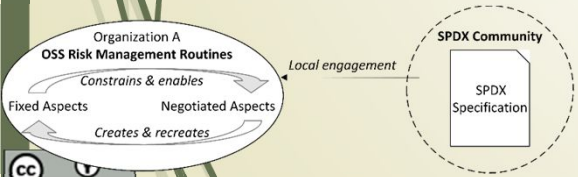
https://github.com/SPDX-CaseStudy/files

Answering the Research Question 1

- RQ1: *How do organizations participating in the SPDX community describe their* **local interpretations** *of communally structured OSS risk management routines?*
  - **Very differently, ranging from using full standard to learning from early adopters.**
    - *"When I hear my guys having modeling discussions, I often say, 'look at SPDX, if it's a coin flip what to call this field, let's go with the standard.'"*

Answering the Research Question 2

- RQ2: *How do these local interpretations influence the extent of their SPDX* **adoption***?*
  - ***Local interpretation is the adoption of SPDX for local needs.***
    - *"The cost of distributing license information was our business driver for adopting SPDX."*



Answering the Research Question 3

- RQ3: *How do these member organizations seek to guide the* **advancement** *of the shared SPDX specification?*
  - ***Local interpretations are source of innovation for communal practices.***
    - *"[In the SPDX group] we talked about the merits of different fields, how to characterize them, and how to serialize formats."*

Implications for Research and Practice

- **Parallels to risk practices**
  - Many organizations attempt to address risk close to delivery
  - Federating risk practices throughout product development can be successful
- **Built-in gradation for adoption**
  - Partial and successive implementation enables maturing local practices

Implications for Research and Practice

- **Stabilizing highly dynamic practices**
  - SPDX specification improves guidance by declaring potential risks in OSS
  - SPDX stabilizes the complexities in software design
  - SPDX is itself entails responsive design within the duality of routines
- **Strategic and brokered communities**
  - Brokers, such as the Linux Foundation, shape the ecosystem
  - SPDX is one example of a community that enables new interactions
  - Brokered engagements can include internal communal needs and external needs from brokering foundations

Contributions to

- **Routines:** Uncover complexities involved in the development of communal risk related open data standards.
- **Open source:** Report how the SPDX project is changing the open source ecosystem by developing shared routines and encoding fixed elements in the SPDX specification
- **Standard setting:** Demonstrate how shared practices shape standards
- **Methodology:** Demonstrate the use of the assurance case driven case study design.

Thank you!

- **Robin Gandhi**
  rgandhi@unomaha.edu
- **Matt Germonprez**
  mgermonprez@unomaha.edu
- **Georg Link**
  glink@unomaha.edu


Robin


Matt


Georg

Assurance case and interview protocol:
https://github.com/SPDX-CaseStudy/files

Full Paper:
https://doi.org/10.1145/3148330.3148333

BRIDGE LAB

University of Nebraska Omaha

Backup Slides

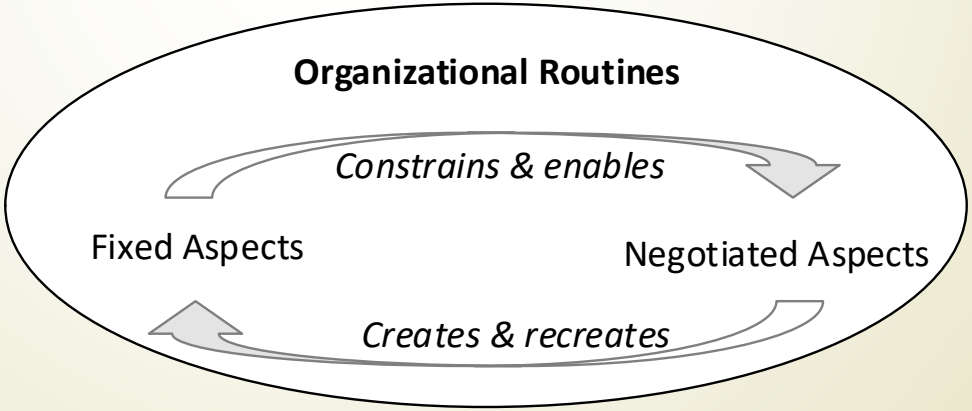
Key Findings

Rebuttal	Elimination Summary
Rebuttal R1: Unless the SPDX specification is deemed complex for operational needs of local OSS risk management routines.	**Rebuttal R1** is not eliminated for organizations just starting with SPDX. Organizations engaged in the SPDX community for a long time easily address the rebuttal.
Rebuttal R2: Unless the information recorded in an SPDX document does not support local OSS risk management routines.	**Rebuttal R2** is eliminated in most organizations by mapping parts of SPDX to local OSS risk management routines.
Rebuttal R3: Unless the organization does not require SPDX documents upon supply or intake.	**Rebuttal R3** is not eliminated in most organizations as SPDX adoption in OSS supply chains is not widespread. Few organization are starting to use and ship SPDX to customers.
Rebuttal R4: Unless SPDX does not integrate well in to organizational training programs.	**Rebuttal R4** is partially eliminated by the inclusion of License List in developer training and best practices. However, there is only mention of SPDX in formal training.
Rebuttal R5: Unless engagement with SPDX community is difficult.	**Rebuttal R5** is eliminated in organizations that directly participate, observe, or engage through proxy representation in the SPDX community. SPDX community is perceived as open and inviting.

Table 1. Rebuttals and summary of findings.

Exchanging Organizational Routines

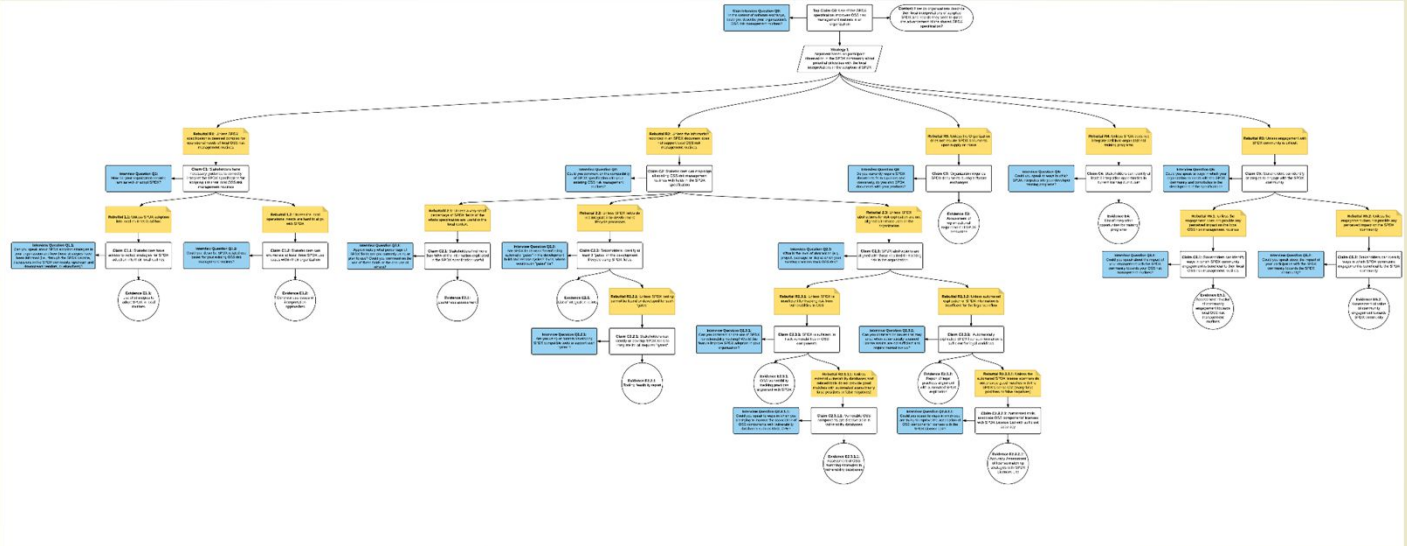
- Routine = Set of actions executed repeatedly with reliable outcomes
- Fixed vs. negotiated aspects
  - Fixed: artifacts, workflows, forms, tools, standards, …
  - Negotiated: actual use, workarounds, shortcuts, …
- Knowledge boundary complicates exchange of routines



Creating Shared Routines through Shared Standards

- Shared standards embody the fixed aspects of shared routines
- Achieve compatability and foster exchange
- Requires building shared understanding
  - Adoption is local interpretation
  - Unexpected implementations result from deviant interpretations
  - Audits and certifications assure uniform implementations
- Standardization process benefits participant organizations
  - Align standard with local interpretation
  - Align organization with emerging standard
  - Information advantage

Method: Assurance Case

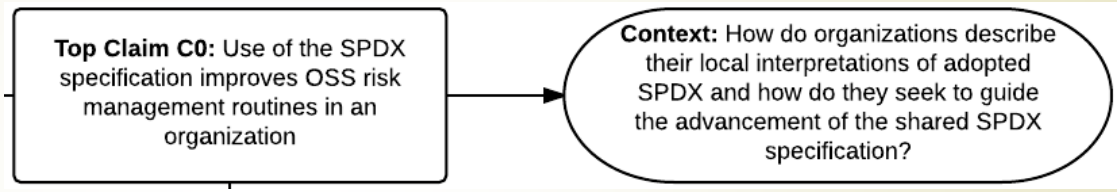


https://github.com/SPDX-CaseStudy/files

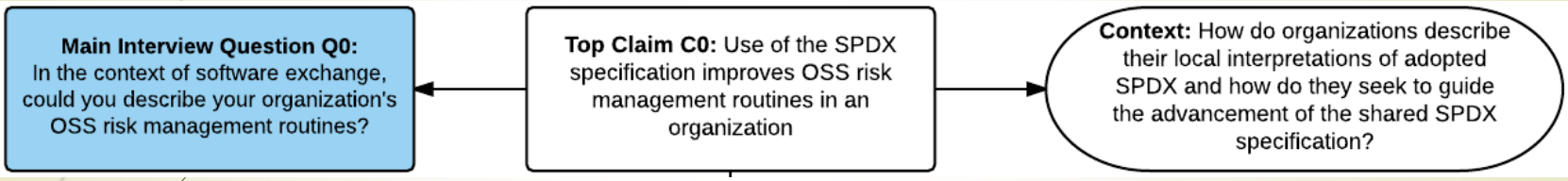
Assurance Case: Top Claim C0

Top Claim C0: Use of the SPDX specification improves OSS risk management routines in an organization

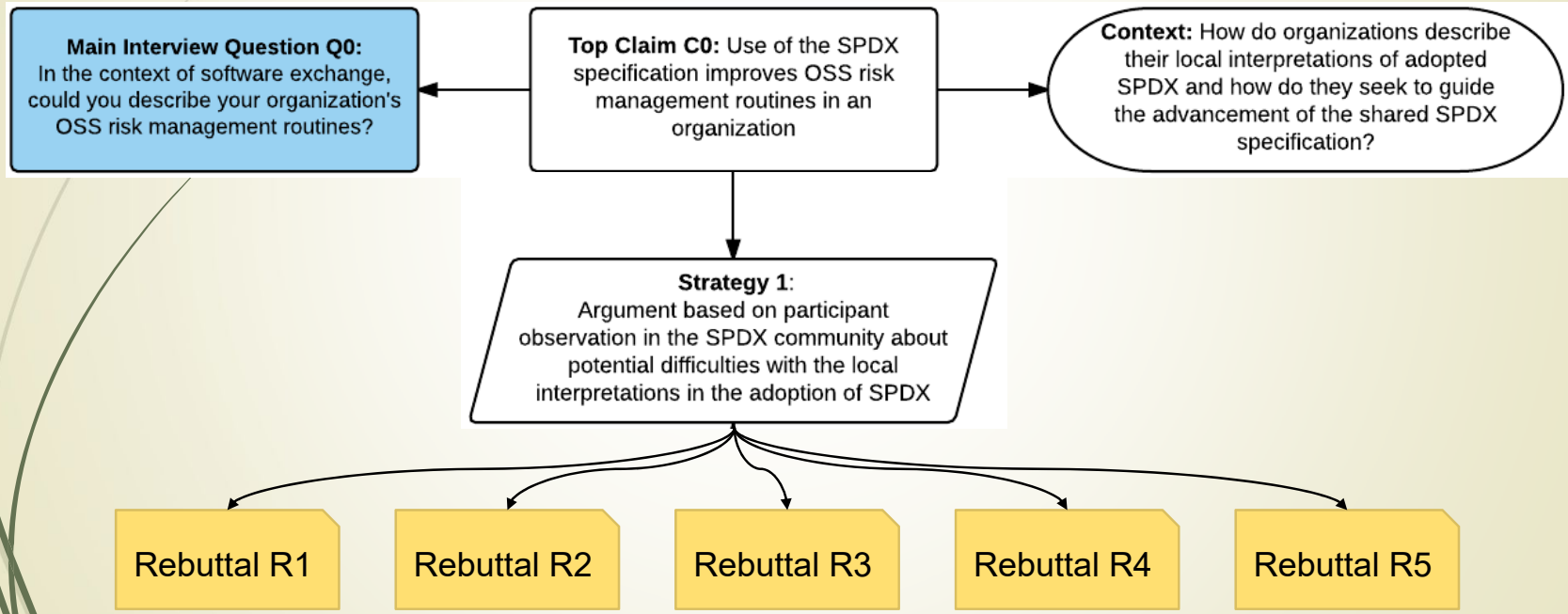
Assurance Case: Top Claim C0



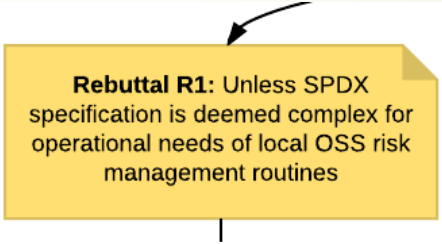
Assurance Case: Top Claim C0



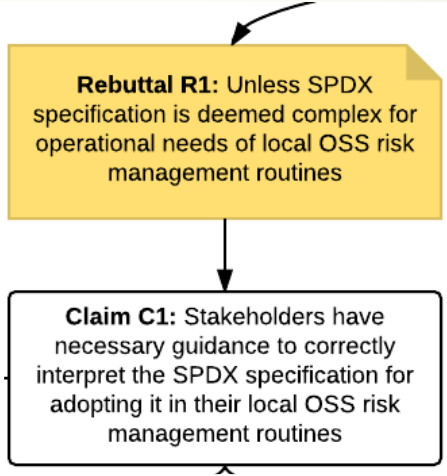
Assurance Case: Top Claim C0



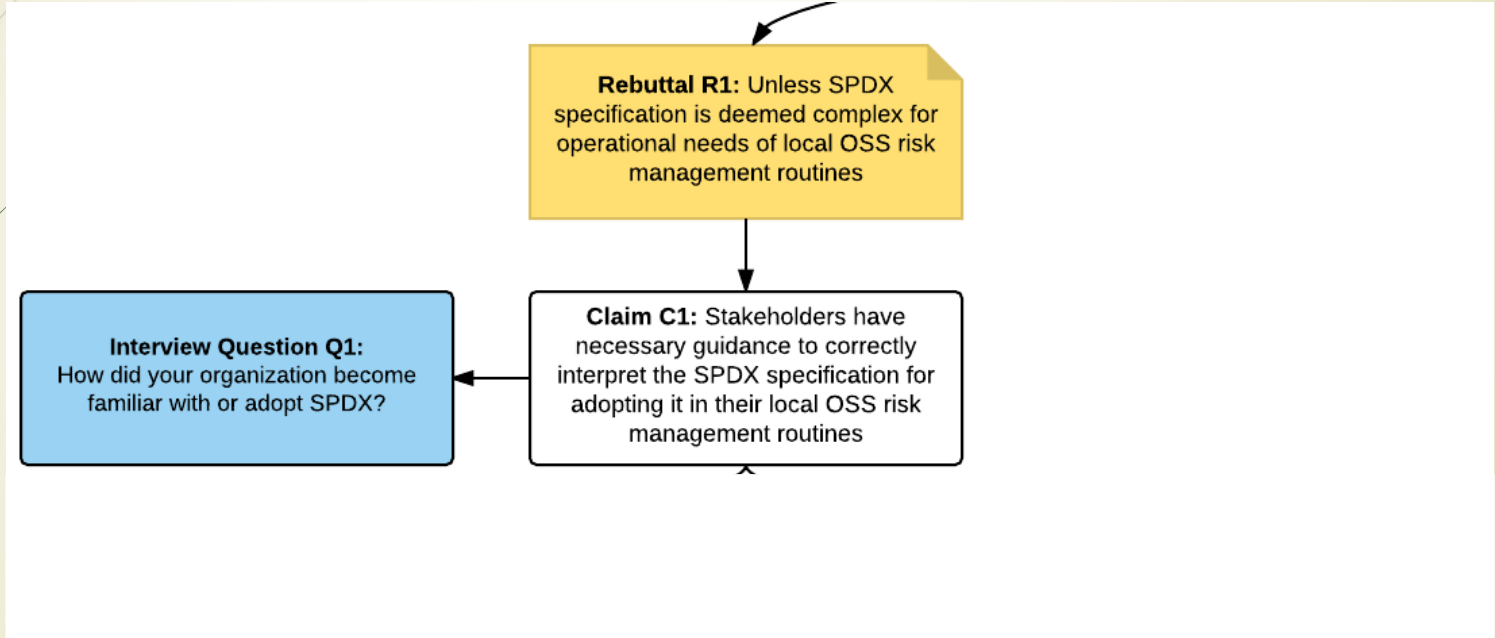
Assurance Case: Rebuttal R1



Assurance Case: Rebuttal R1



Assurance Case: Rebuttal R1



Assurance Case: Rebuttal R1