**Cyber Innovation Hub: Open-Source Data Diode**

*Together we increase the Cyber resilience of the Netherlands*

**Content**

1. Cyber Innovation Hub
2. Data diode vs. Open-Source Data Diode
3. OSDD: Basic concepts
4. OSDD-community
5. Use cases
6. How can you contribute as a developer?
7. License

**1. Cyber Innovation Hub**

The Cyber Innovation Hub, established in 2019 from the Ministry of Defence, ensures that departments, research institutions and companies work together on joint security issues in the field of cyber (security). The aim is to strengthen cyber knowledge and skills in the Netherlands, facilitate innovations and experiments and build an ecosystem of cyber experts, innovators and other partners to reduce cyber threats. The Cyber Innovation Hub is included in the Dutch Cyber Security Agenda (NCSA) (2020) and in the vision of Defence.

**2. Data diode vs. Open-Source Data Diode**

The Cyber Innovation Hub has launched the **Open-Source Data Diode (OSDD)** innovation program with the aim of increasing cyber security in the Netherlands for public and private parties in the Netherlands.

**What is a data diode?**

A data diode is a network appliance in the form of a hardware device, which, based on its physical components, enables data traffic between two separate networks in only one secure direction. In short, data can be sent from A to B, but not from B to A. Because the security is not software-based, it cannot create vulnerabilities in the form of software bugs and cannot be attacked by online hacks. For example, a data diode could provide remote access to the data of an IoT device, without the risk of a third-party tampering with this device. Thus, the distributed data can be trusted. It therefore offers one of the most effective ways to protect networks and systems against external cyber threats.

***Example 1: Operations Center***

*Defence has an operations centre where important information about missions comes together. People from outside sometimes try to get into that system. For fear of a hack, the information in this centre is no longer sent digitally to, for example, other departments. A courier will literally pick up the information. Thanks to the diode, this is no longer necessary.*

**Data diode vs. Air gap**

A common solution to protect sensitive or classified information against cyber-attacks is to completely disconnect it from other networks (**air gapping**). Air gapping works well to prevent remote cyber-attacks, but in itself lacks a way to easily communicate with the outside world. There are situations where information needs to be transferred to or from the secure network. Data diodes solve that problem and are the ideal solution for maintaining air-gapped security against outside attacks while enabling remote communication.

**Data diode vs. firewall**

A **firewall** is probably most commonly used to regulate the flow of information. Unlike a data diode, a firewall is a software solution. Humans have programmed the software and therefore bugs are not completely avoidable. In addition, a firewall can be complex to manage and configure. This leads to errors, such as opening wrong ports, which hackers can use. A data diode, on the other hand, is a relatively easy product to implement, configure and maintain. Physically setting up the data diode does not cost more than connecting two network cables and the power cable and setting up the proxy servers.

**3. Open-Source Data Diode**

The invention of a data diode is not new. But the fact that the Open-Source Data Diode is offered **low-end, low-cost**, and as the name suggests, open source is something new. The currently available data diodes are mainly used for highly classified domains, where a high degree of information security applies. The high demands in highly classified domains make them relatively complex and expensive. However, the OSDD is based on a simple but reliable design and use at low costs, which makes the product more accessible and affordable for a multitude of companies, (semi) governments and individuals. In addition, the basic principle is that the OSDD can be used flexibly.

Low-end, low-cost data diodes, are intended for use in the lower classified domain. Think of:

* Medical sector (operating rooms, privacy)
* Smart City and semi-vital infrastructure (Internet of things, connected devices)
* Linking legacy systems (logistics, admin)
* Robotic Industry, Industrial Control Systems
* Data streams to and from the internet

Anyone can use the OSDD because it is made available open source. The design and source code may therefore be used freely. The aim of the OSDD is to improve the cyber resilience of the Netherlands by lowering the threshold for the larger-scale application of data diodes. To make this possible, the price of data diodes must be significantly reduced, the devices must be miniaturized and responsible use must be made easy. The OSDD can thus make an important contribution to strengthening sectors and domains in which few digital security barriers are currently applied.

|  |  |
| --- | --- |
| **Open Source Data Diode** | **Bestaande Data Diodes** |
| Low price | High price |
| High volume | Low volume |
| Guaranteed quality | Certified |
| Departmental Confidential | NBV certification to secret |
| Dutch manufacture | Origin both Dutch and abroad |
| Enabler for broad knowledge development | Unilateral knowledge development |

**4. OSDD-community**

The Open-Source Data Diode is being further developed open source in the **OSDD-community** in the security domain. The hardware and software are accessible through the [OSDD-Github](https://github.com/CyberInnovationHub-NLD/OpenSourceDataDiode-OSDD-). The Cyber Innovation Hub brings together various development parties, management parties and launching customers via a community. The goal of the community is:

1. Enabling rapid interaction with and between parties;
2. Gain speed in technology and product development in a safe environment;
3. Bringing (complimentary) parties together who can share knowledge and skills;
4. Increasing the support of the OSDD;
5. Shorten the time to market of the OSDD

Various internal and external parties have now been approached from the Cyber Innovation Hub and there is the necessary interest in active participation.

The community is interesting for launching customers, because specific applications in terms of hardware and software can be submitted to the community. From the Cyber innovation Hub, we look at concrete use cases to make the OSDD useful applications for different situations. If you have a relevant use case in mind for your organization or work domain, please contact serina.vandekragt@ictu.nl

We use the Standard for Public Code as defined by the Foundation for Public Code We ask the participating parties to also subscribe to this standard. For more information: https://standard.publiccode.net/

**5. Use Cases**

The FRONT Innovation Center has developed a demonstrator with HSD and Technolution. Experiments were carried out within and outside the Ministry of Defence for its further development. This has led to an increase in demand. An example is the field test in an Enexis high-voltage substation. After that, the value was established and the demand increased. The CIH also held several presentations for CISOs and operators of critical infrastructure, which generated a lot of interest and demand. Through Proof of Concepts and successful testing, the demonstrator has been further developed into a **working demonstrator**. The proven demonstrator is applicable for IoT, SCADA-systems and PLCs.



**6. How can you contribute as a developer?**

The OSDD is currently tested and fully functional. However, to make the OSDD a useful device for a range of different usage scenarios requires further development of the software.

Current functional limitations are mainly found in the availability of supported network protocols and in the ability to securely update OSDD software remotely. A second area that needs improvement is ease of use. Reducing the technical know-how required to implement and use the OSDD would greatly improve its usability.

You can already contribute to the OSDD by applying the code and making useful additions via GitHub. It is also possible to collaborate structurally with the team, by joining the OSDD network as an organisation, user or developer. Knowing more? Please contact [serina.vandekragt@ictu.nl](mailto:serina.vandekragt@ictu.nl)

**7. License**

Currently the license is Apache 2. The code will be published under EUPL. Until formal publication, the original codebase is NOT intended for distribution and is only intended for use by the OSDD community members. Industries are free to distribute and publish at the discretion of the appropriate industry owner/moderator.