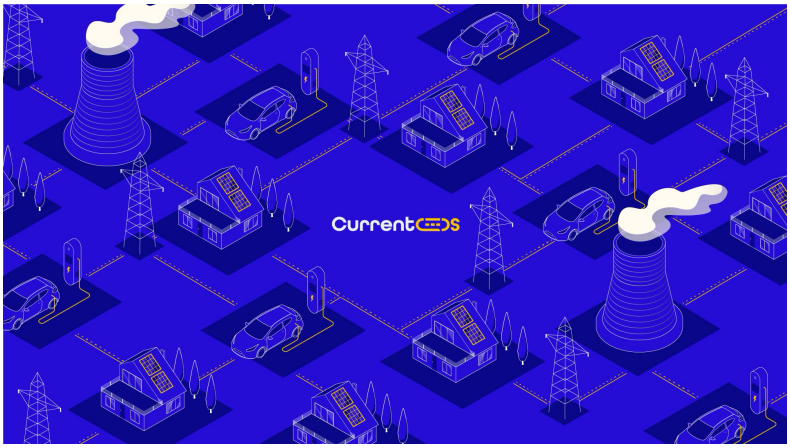
Press release Current/OS
Aalsmeer, the Netherlands, August 26, 2025

Direct Current (DC) Microgrids: A Bulwark Against Cyberattacks

With the rapid electrification and digitalisation of our energy infrastructure, cybersecurity is fast establishing itself as a major concern with respect to our power networks. Current/OS, an independent, non-profit organisation promoting the deployment and adoption of direct current (DC) microgrids, brought together key industry stakeholders at a recent webinar to examine the growing threats facing cloud-managed electrical systems, and to showcase the potential of DC microgrids in reinforcing energy resilience.



The Increasing Vulnerability of Power Grids

Traditional power networks left no entry points for cyberattacks, by virtue of being fully decoupled from digital networks. This has slowly changed, moving towards the use of interconnected digital systems to facilitate energy management. These remotely operable systems bring significant improvements to how resources are used, but also put the entire network at risk of hacking, ransomware attacks or unauthorized manipulation of consumption.

Yannick Neyret, President of Current/OS, clarifies: *"With life now being near-impossible without electricity, it is even more important to think about the security of our distribution network. It is far too essential to depend on communication networks. As a result, each device operates autonomously in Current/OS-compliant electrical systems, altering its response based on the electricity available in the system at any given time. Hence, a failure in the main grid does not impact local electricity distribution, since the interface converter isolates threats or issues arising in the main network."*

In response, the Current/OS Foundation advocates for the deployment of autonomous DC microgrids, connected to the main grid through an Interlink Converter to enable decentralized energy management. Within such systems, each device adjusts its behavior based on the voltage available, without requiring centralised control or cloud-based management. Thus, the microgrid operates in a so-called 'island', connected to the main grid, yet operating independently from it.

Such independence of operation ensures continuity of service during outages. Effectively, the Interlink Converter acts as a technical safeguard, separating microgrid operations from disruptions or cyberattacks affecting the main grid. This secure architecture brings several advantages, notably protection against grid interruptions, local prioritization, and the absence of typical vulnerabilities associated with smart devices.

Putting Energy Sovereignty at the Heart of Our Approach

Current/OS supports a number of projects deploying DC microgrids across Europe, and calls for a serious rethink on the design of local power networks to make them more independent and secure. The centralised approach to energy distribution is no longer viable as cyber threats continue to escalate. In such a context, the shift towards local and decentralised distribution is not only possible, but also essential.

About Current/OS

The Current/OS Foundation brings together an ecosystem of over 95 partners from 25 countries, including electricity stakeholders, construction firms, certification companies, trade groups, universities, and more to promote a unified standard for DC installations, by providing rules for the manufacture and installation of compatible equipment that can operate safely in localised DC power distribution networks. With UL Solution as a founding partner, as well as ABB, Eaton, Mersen, Schneider Electric, Tridonic on its board, the partnership includes industry leaders such as Siemens, Kone, Vinci Energies, Daikin, Hisense, as well as niche expert and innovative startups. https://currentos.org/

Press Contacts Current/OS:
Jean-François Kitten jf@licencek.com +33 (0)6 11 29 30 28
Jérémy Cariddi j.cariddi@licencek.com +33 (0)7 66 39 75 99
Avtansh Behal a.behal@licencek.com +33 (0)7 69 53 08 25