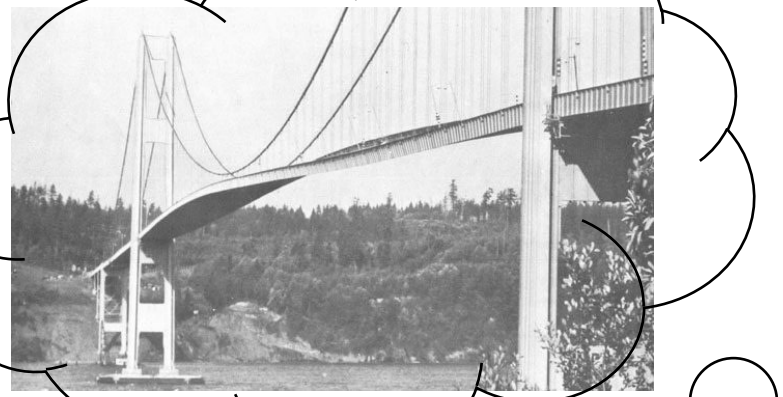


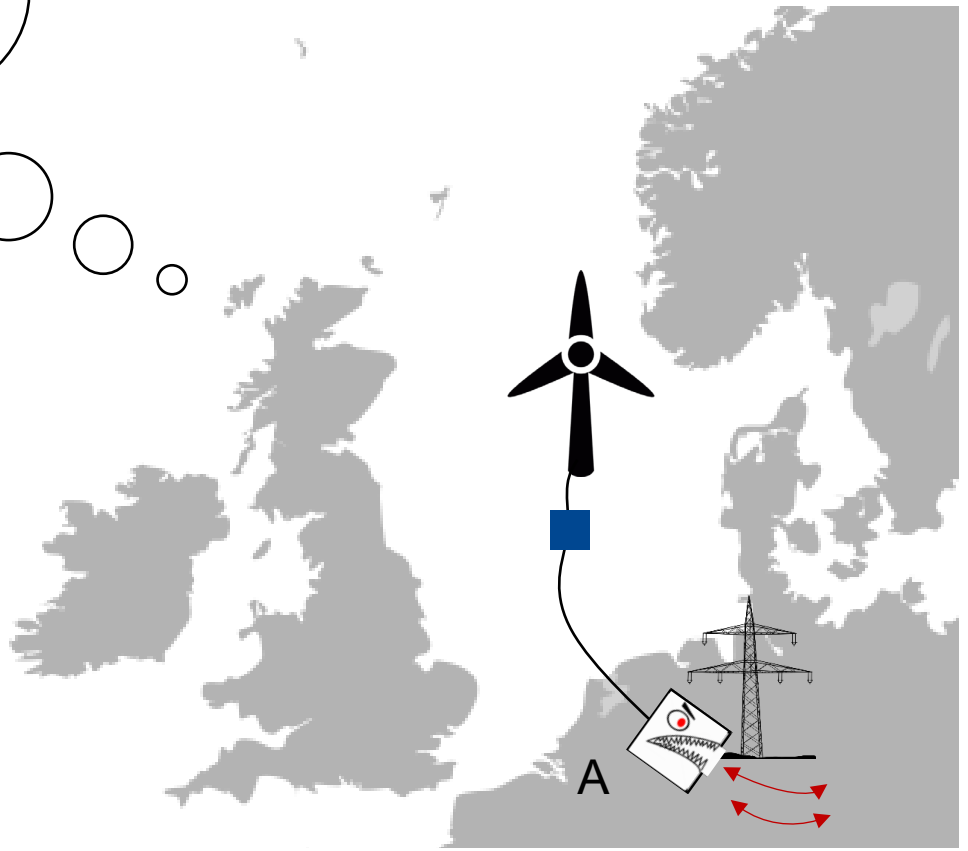
Do we need partially open software for big power converters?

Ilka Jahn – KTH Royal Institute of Technology

STandUPAcademy 2026 | Session 2: Electricity Grid

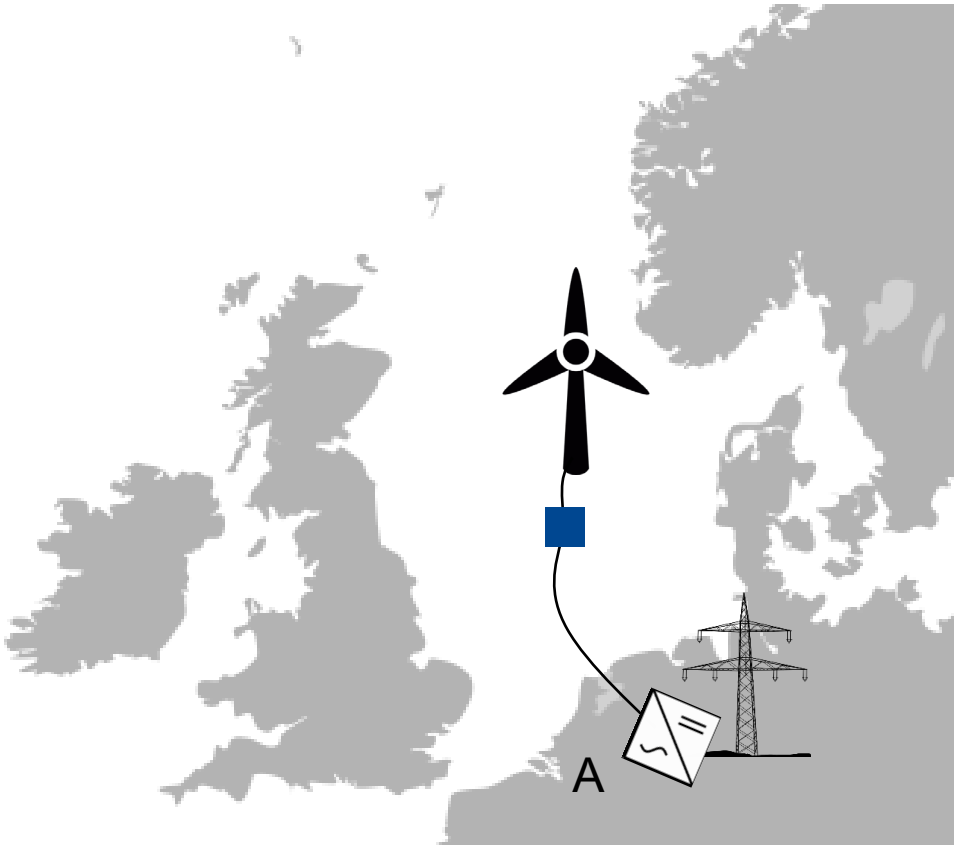
Control interaction - illustration



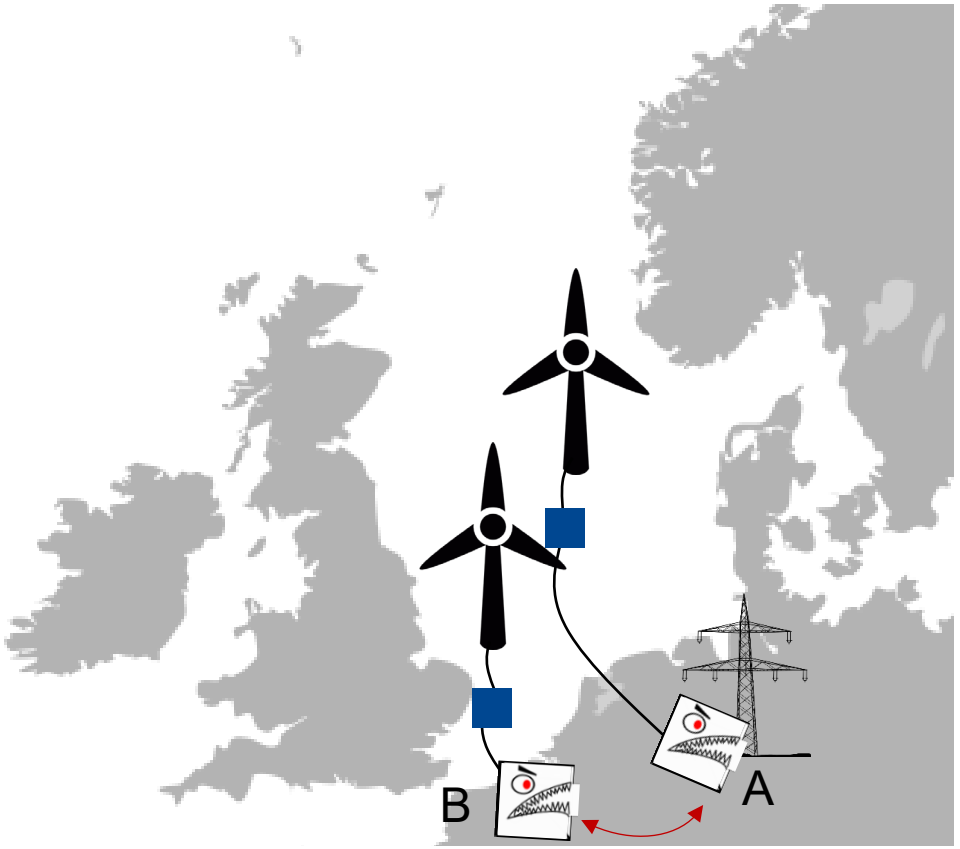


Control interaction - illustration

Software upgrade
single-vendor A



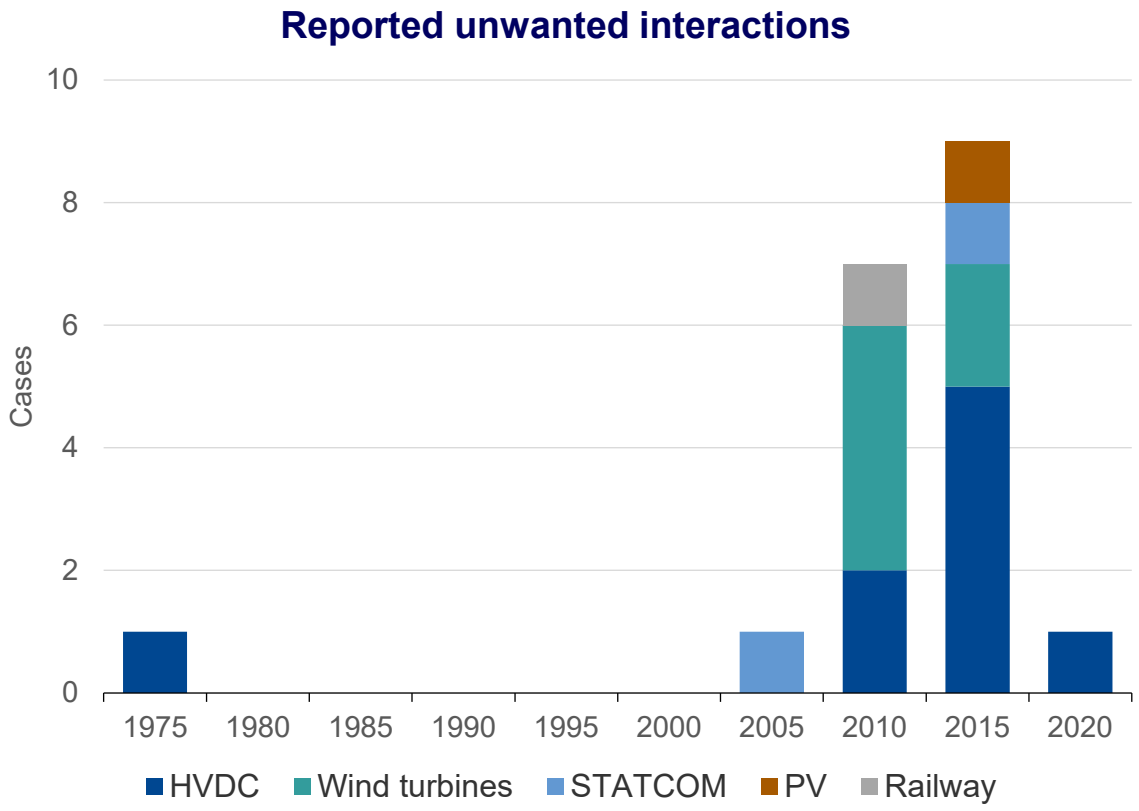
Control interaction - illustration



BLACK-BOXED software

What now?

More and more software -related interactions …



Germany 2017
Offshore HVDC link resonates at 1.5–1.8 kHz after switching in the onshore AC grid
Fix: vendor software upgrade

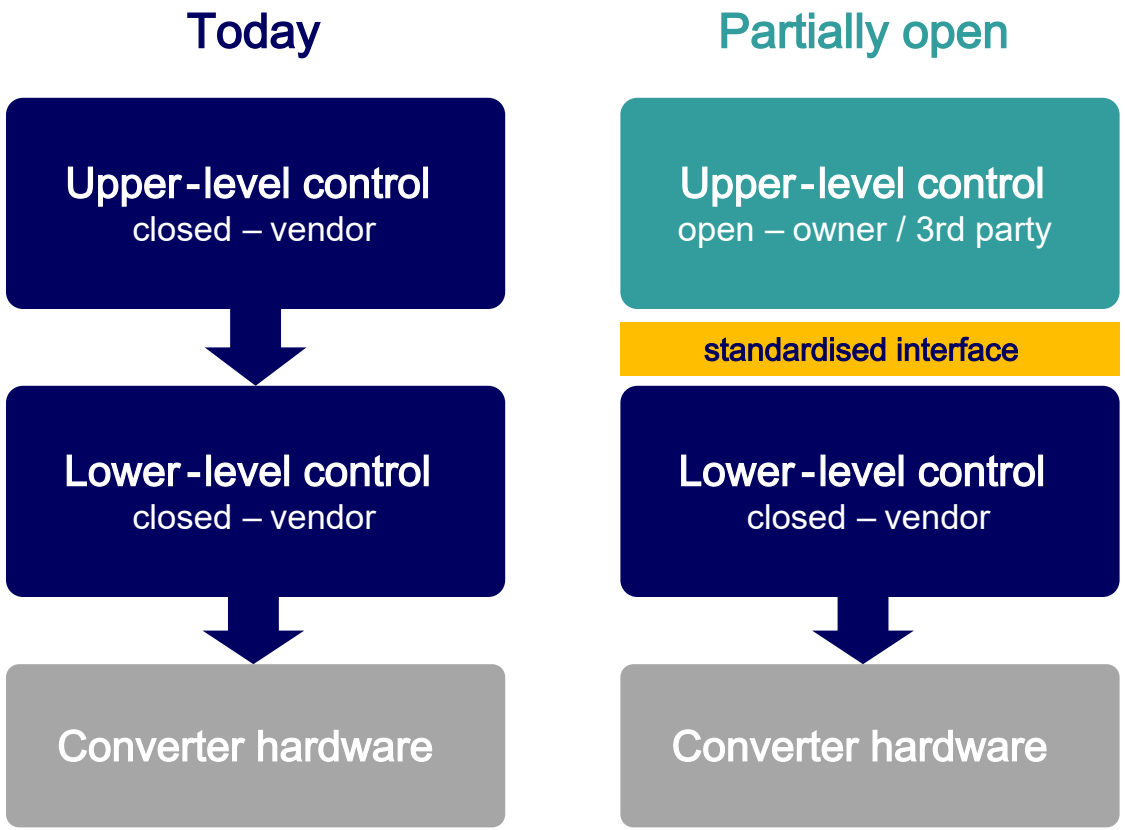
Johan Sverdrup 2020
Two HVDC links from different vendors in parallel
Fix: third party integrates both, with C&P replicas and adapted vendor software

North China 2015
Sub- and supersynchronous events with 7 turbine and 10 converter vendors
Fix: one vendor re -tuned controls in 2000 turbines

Software caused it, software fixed it – and the fix depended on the vendor.

Source: I. Jahn et al., "Moving beyond open-source modelling", OSMSES 2022 (literature survey; chart shows reported cases per 5 -year period)

Partially open controls



System-behavior
DC voltage / active power, AC voltage / reactive power, AC current, PLL, external protection,…

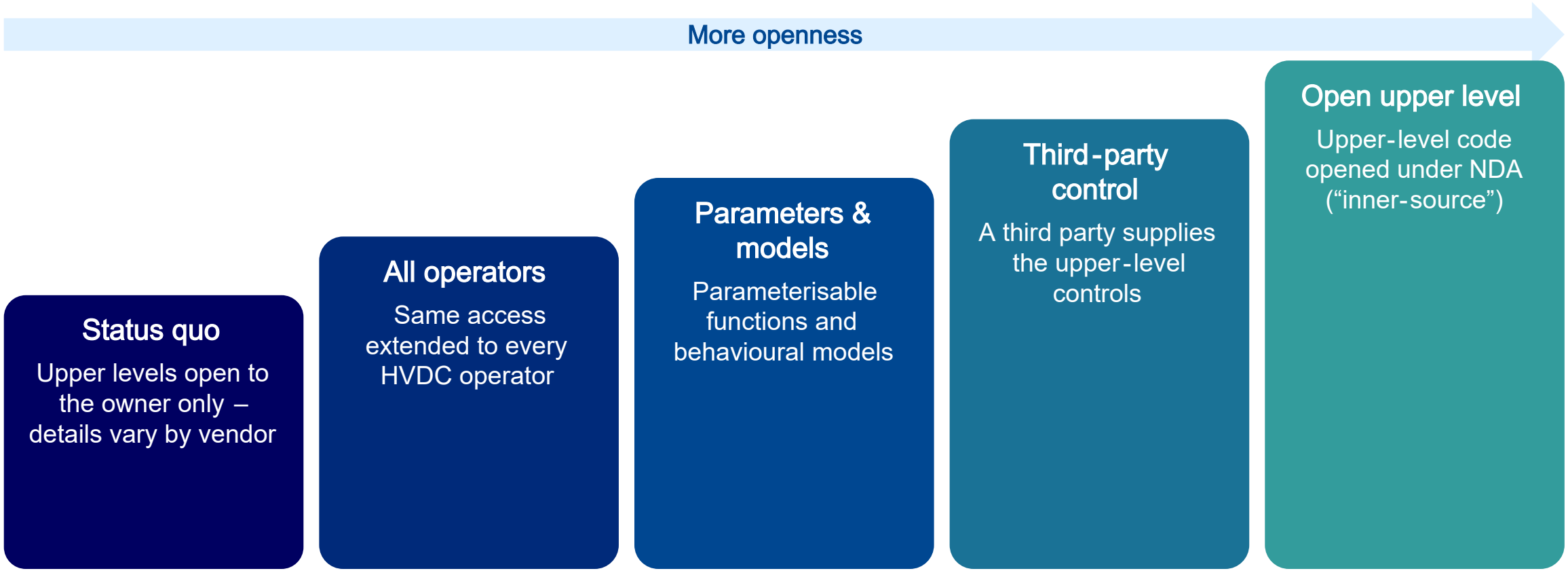
Converter -internal behavior
Circulating current, arm energies, modulation, capacitor balancing, internal protection ,…

Physical equipment
Valve controllers, MMC cells, sensors,…

Grid behaviour becomes accessible – vendor IP stays with the vendor.

Based on CIGRE WG B4.85 "Interoperability in HVDC systems based on partially open -source software"

“Open” is a spectrum, not a switch



Open ≠ public: access limited to owners, operators and trusted parties.

Levels of openness as discussed in CIGRE WG B4.85

What does it mean for AI, data and cybersecurity

Data & AI

Open interfaces let owners use their own operational data on the real control code – for digital twins, AI-assisted monitoring and re-tuning.

Cybersecurity

Openness and security are not opposites: obscurity is a weak defence, and reviewed code with controlled access can be stronger. But every extra party widens the attack surface.

Responsibility

Who is liable when shared code misbehaves? This needs contracts, verification and testing – and enough skilled engineers.

From “can we open it?” to “who may access it – and who is responsible?”

My answer: yes – partially open software

1. **As a fall-back / for flexibility**
   When the grid changes, owners must be able to adapt converter behaviour – not only the original vendor.

2. **Partially**
   Open the upper level; vendor IP and hardware protection stay closed.

3. **Already under way**
   CIGRE WG B4.85, Linux Foundation Energy, and the InterOPEn doctoral network (engineering + law).

For the panel

Who carries the liability?

Do we have enough engineers?

Can standards keep pace with the technology?