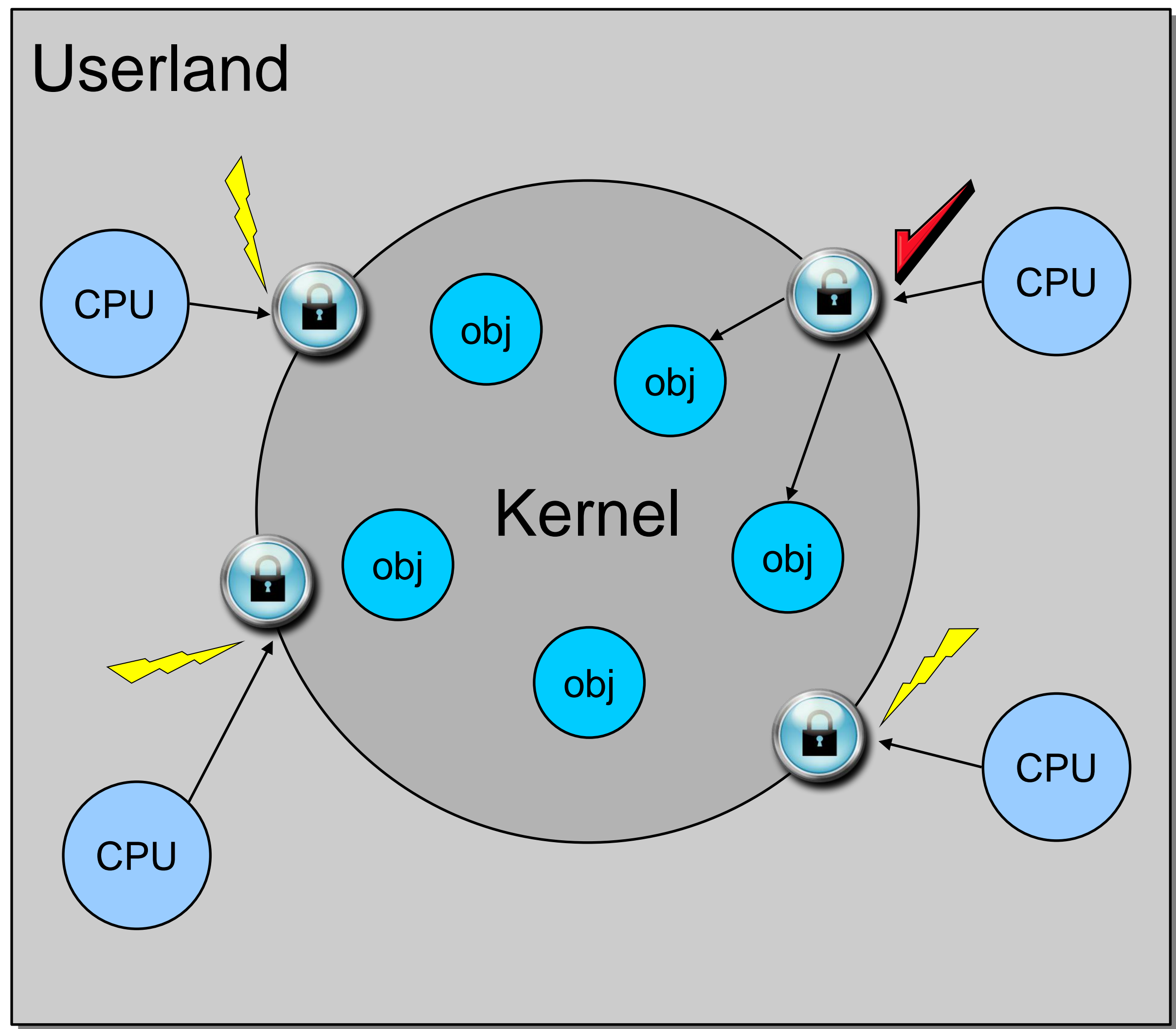
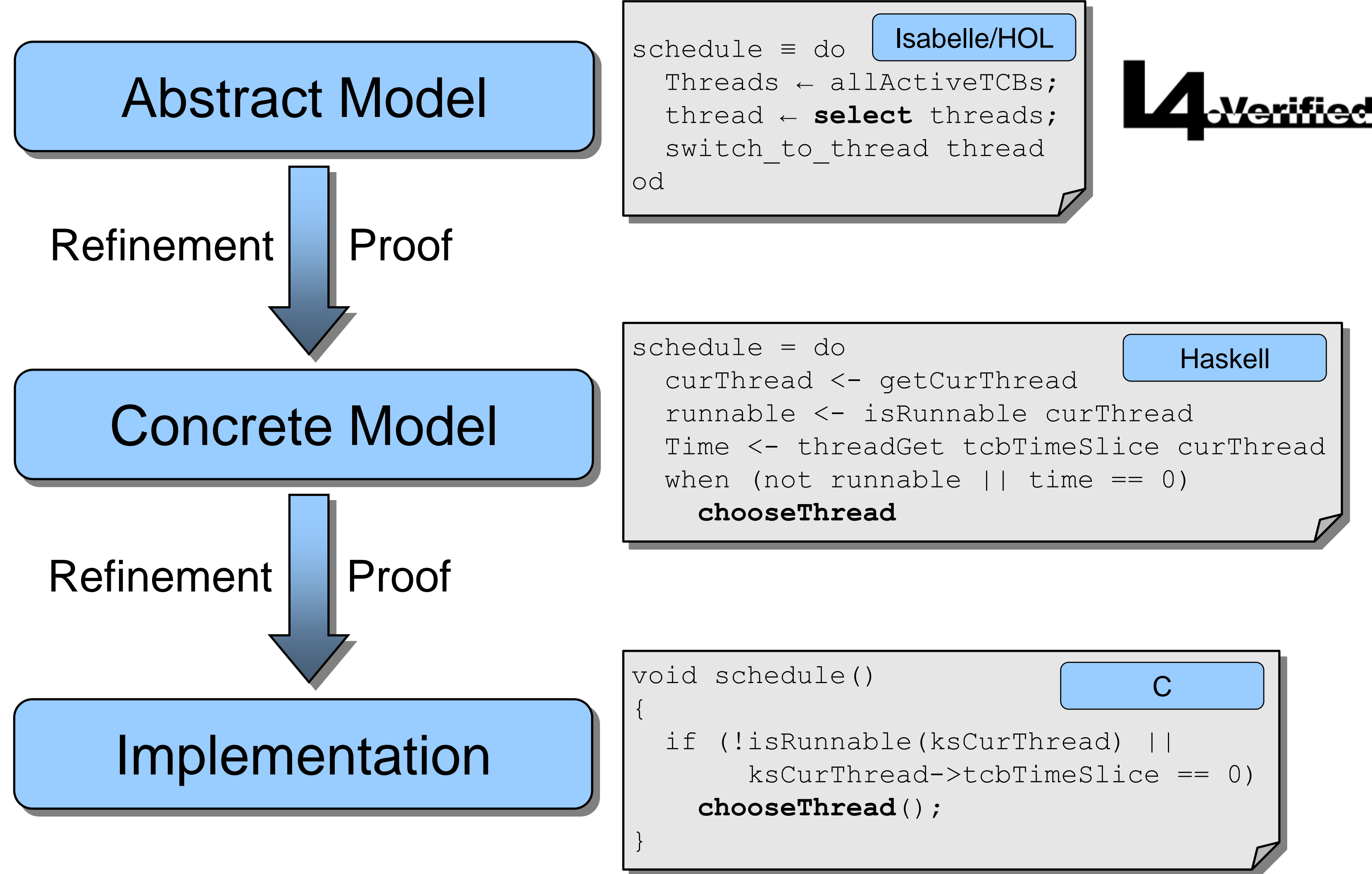


Towards a Formally Verifiable Multiprocessor Microkernel

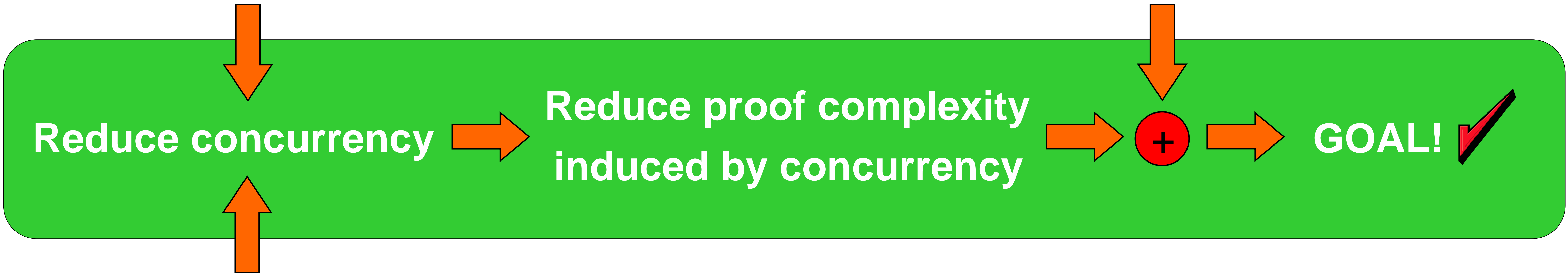
Michael von Tessin (NICTA and UNSW)



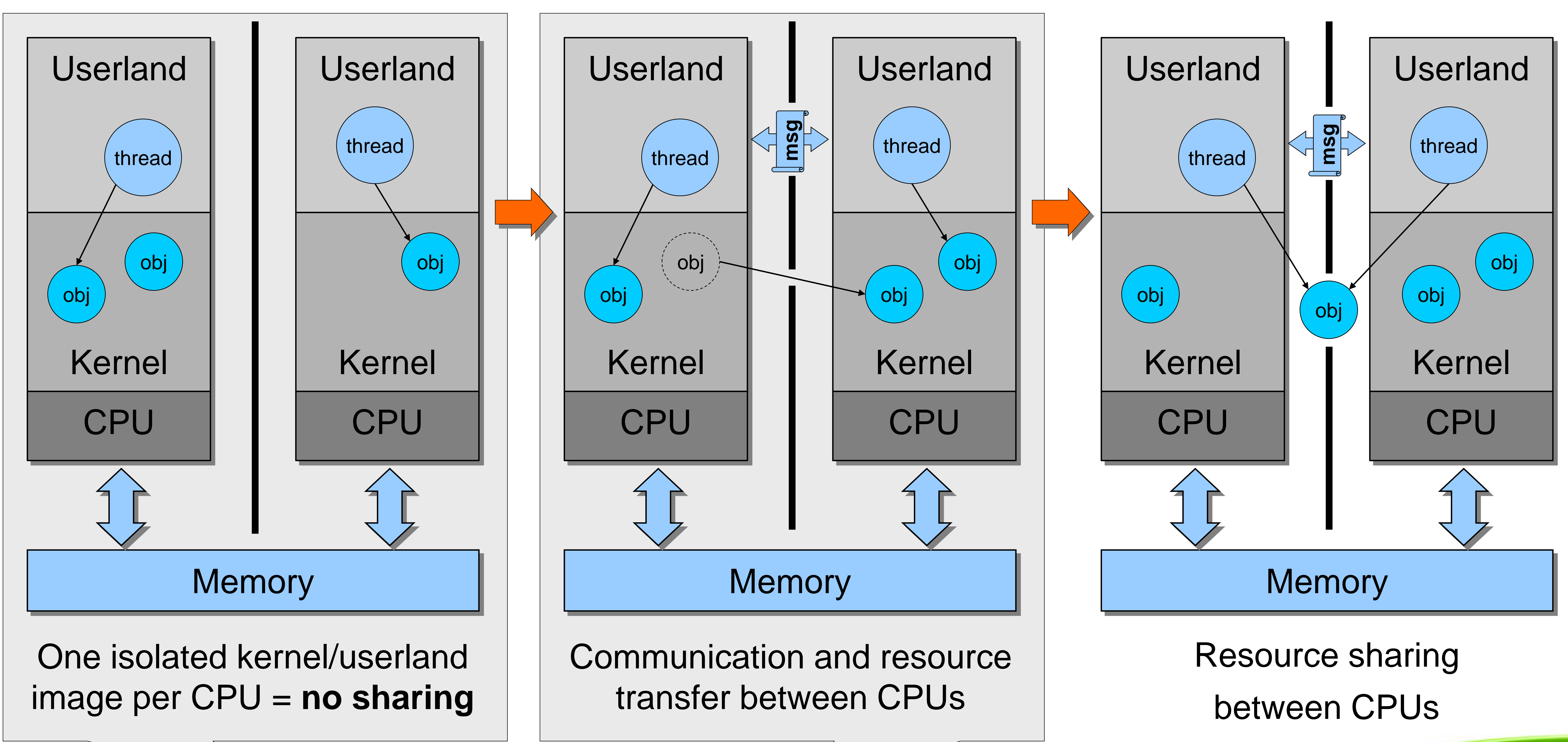
Reduce parallelism by having a **big lock** around the whole kernel



Formal verification approach of the **uniprocessor** version



Reduce sharing with a **multikernel** approach like in *Corey* or *Barrelfish*



Progress: implemented in C and semi-formally proved

low-level design