Pros and cons of using formal methods

✓ Nothing better than a mathematical proof

➡ A code "proven safe" is safe

◉ Development is time and effort (and so money) consuming

➡ Should be motivated by the risk analysis

◉ Do not prevent from specification bugs

➡ Example of network protocols

Build Better Operating Systems