

Definitions

Thierry Sans

Safety (a.k.a correctness) vs Security

Safety

Satisfy specifications

“for reasonable inputs,
get reasonable outputs”

Security

Resist attacks

“for **un**reasonable inputs,
get reasonable outputs”