this is a safety–critical system so requires a lot of up–front analysis before implementation.