If you ignore who

the various multisig keyholders are, zkSync functionally can be instantly upgraded by m of n

keyholders. The scheme they have where there are two different groups, one who proposes and one who can speed up the proposal, doesn’t change the fact that if you can compromise m

keyholders across those two groups you can instantly upgrade the system and thereby steal all of the funds.

I think it is relevant to refer to the Ronin attack, where a state actor (allegedly) compromised a multisig to steal all of the funds of a platform. All of the other systems that have a yellow entry in the Upgradability column are protected against this attack vector to some degree, while zkSync is not protected against this attack vector.

IMO, a red yes in that column means there exists some set of keys that can upgrade the system instantly, while yellow means there exists some set of keys that can upgrade the system non-instantly and people can withdraw their funds during that intervening time.