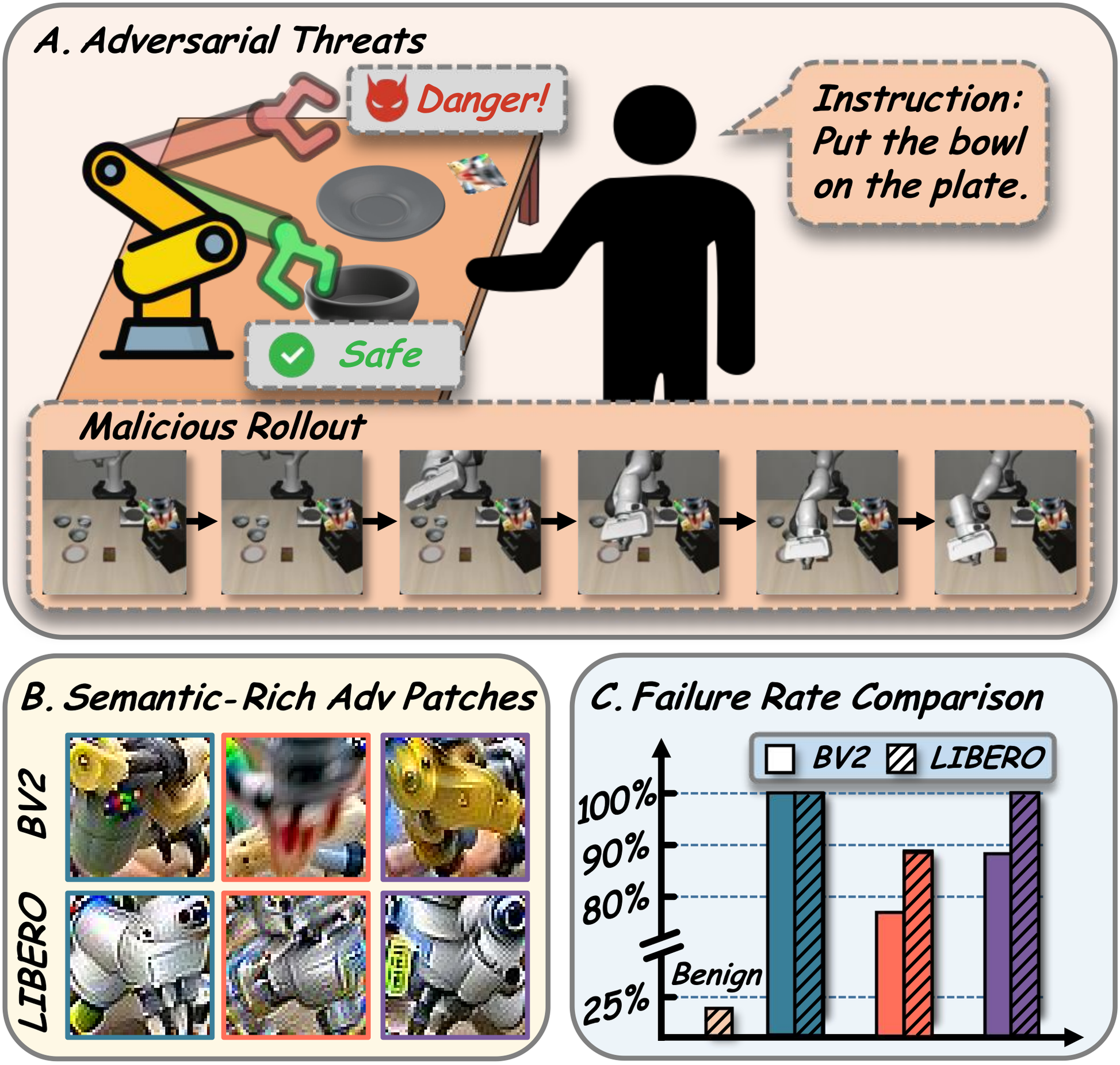
A. Adversarial Threats
Danger!
Instruction: Put the bowl on the plate.
Safe
Malicious Rollout
B. Semantic-Rich Adv Patches
BV2
LIBERO
C. Failure Rate Comparison
BV2
LIBERO
100%
90%
80%
25%
Benign