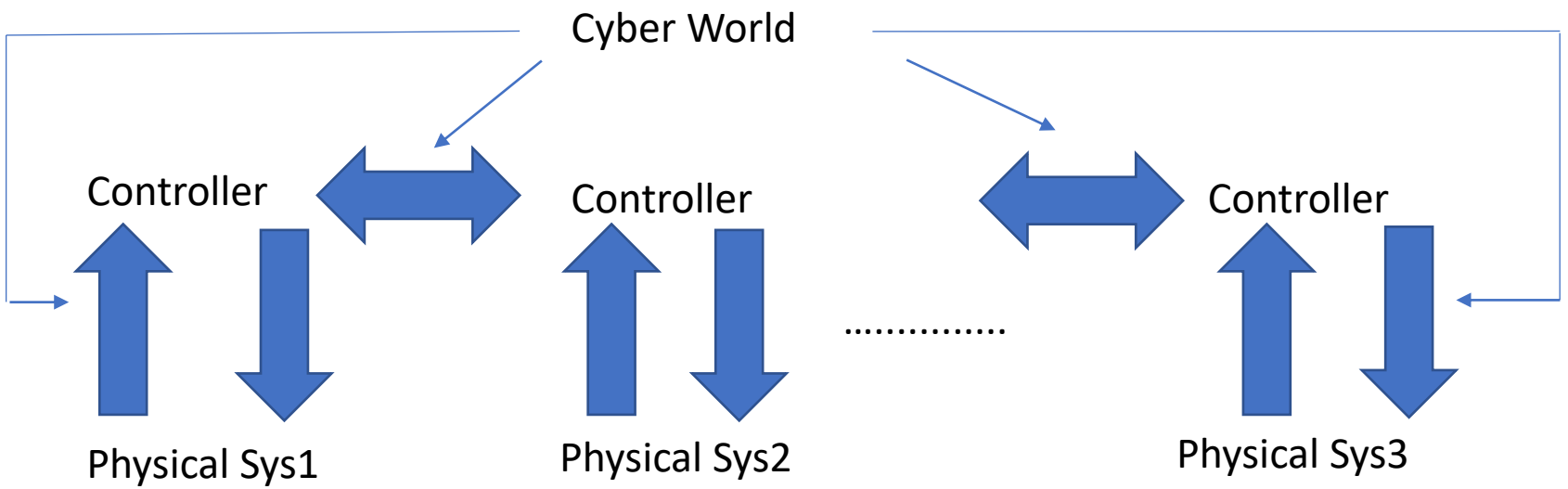
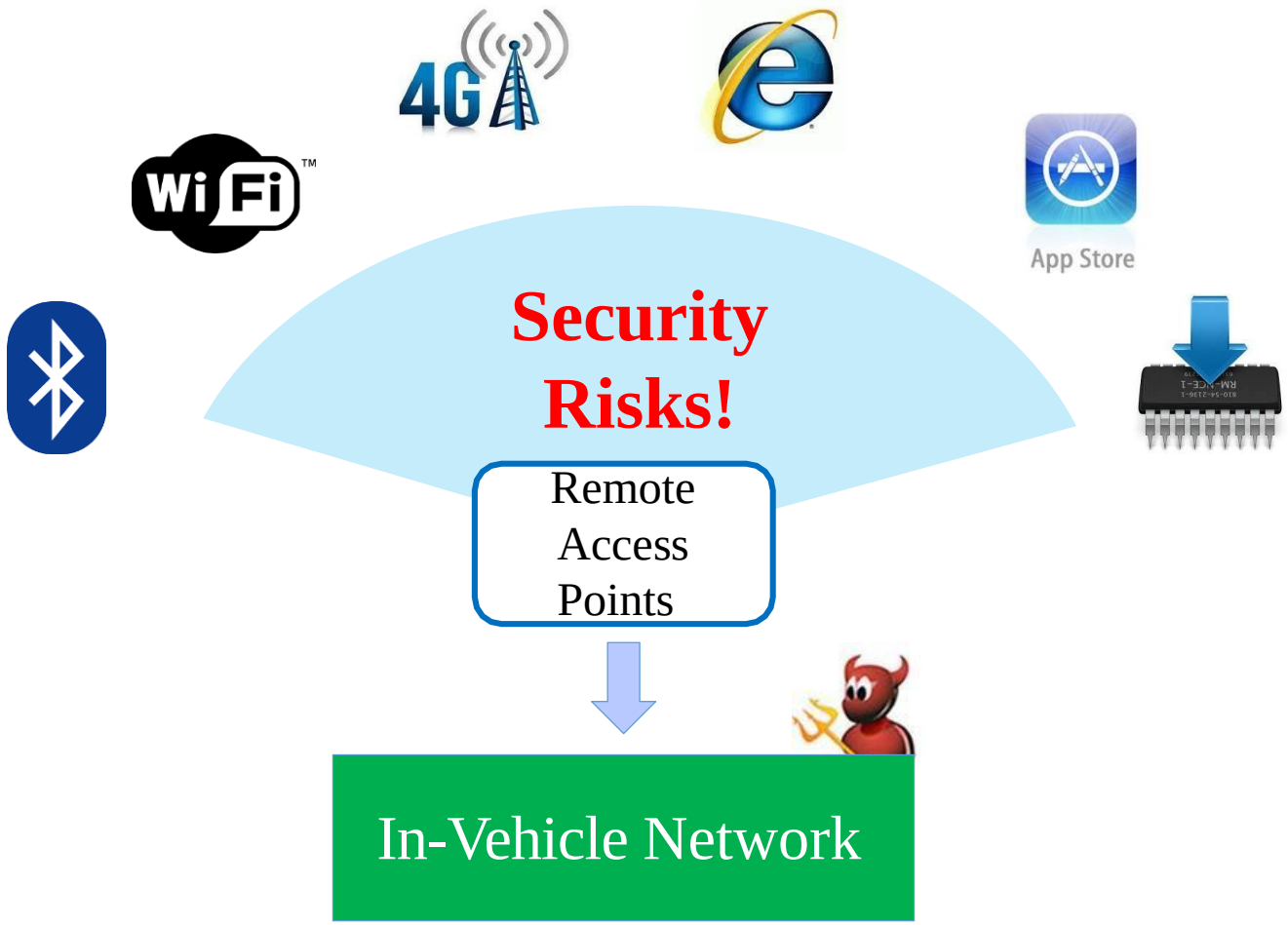
Computational Foundations of Cyber Physical Systems (CS61063)



- Soumyajit Dey
- CSE, IIT Kharagpur

Vehicle Cyber Attacks



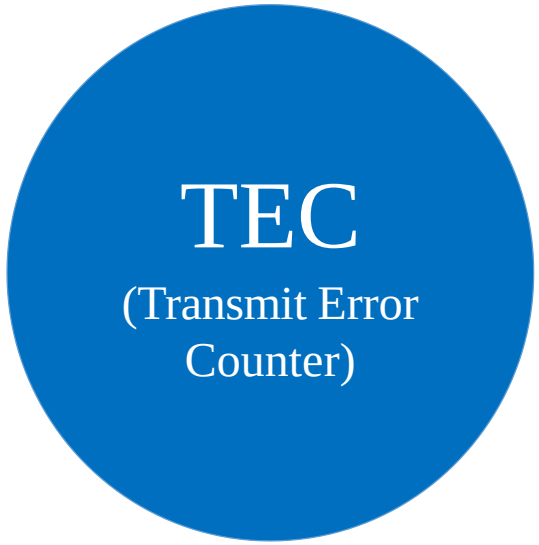
CAN: In-Vehicle Network

- CAN is the most popular protocol among in-vehicle control networks
- Vulnerability of this protocol to security threats has been pointed out: *falsification of meter readings*, *disablement of brake function*, *unauthorized control by a spoofed message injected into the network*
- It is difficult for CAN to directly use the security measures because:
  - maximum data transfer rate of CAN is 1 Mbps
  - maximum payload of a message is 8 bytes

In-built Error Handling in CAN

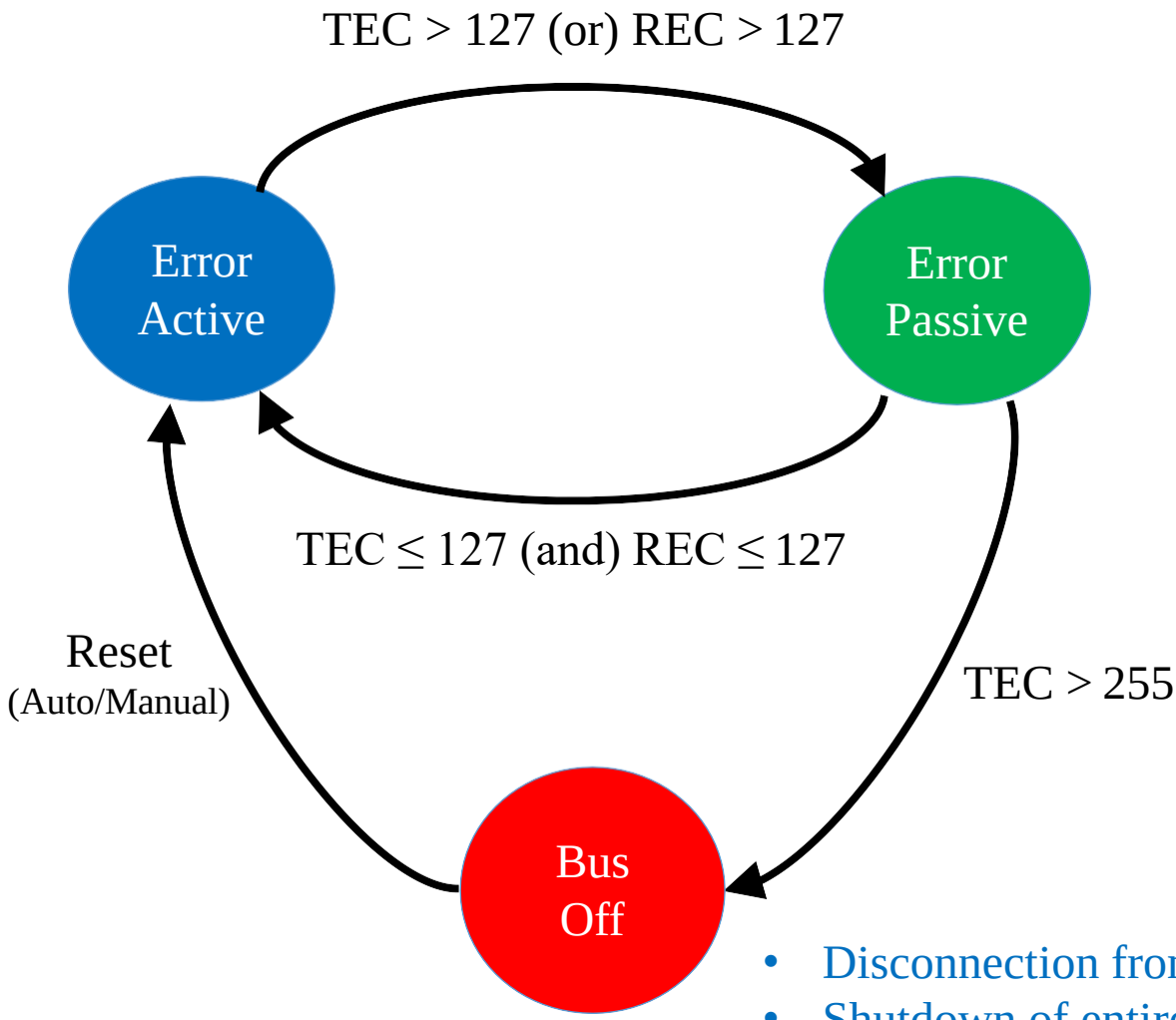
1. **Bit Error:** Every transmitter compares its transmitted bit with the output bit on the CAN bus. If the two are different, a *bit error* has occurred, except during arbitration.
2. **Stuff Error:** After every five consecutive bits of the same polarity, an opposite polarity bit is stuffed for maintaining soft synchronization. Violation of this incurs a stuff error.
3. **CRC Error:** If the calculated CRC is different from the received CRC, a CRC error is raised.
4. **Form Error:** If the fixed-form bit fields (e.g., CRC delimiter, ACK delimiter, EOF, IFS) contain at least one illegal bit, a form error has incurred.
5. **ACK Error:** When a node transmits a message, any node that has received it issues a dominant bit in the ACK slot. If none replies, an ACK error is raised.

Error Count



During	Transmission	Reception
Error	+8	+1
Error-free	-1	-1

Fault Confinement



- Disconnection from bus
- Shutdown of entire system

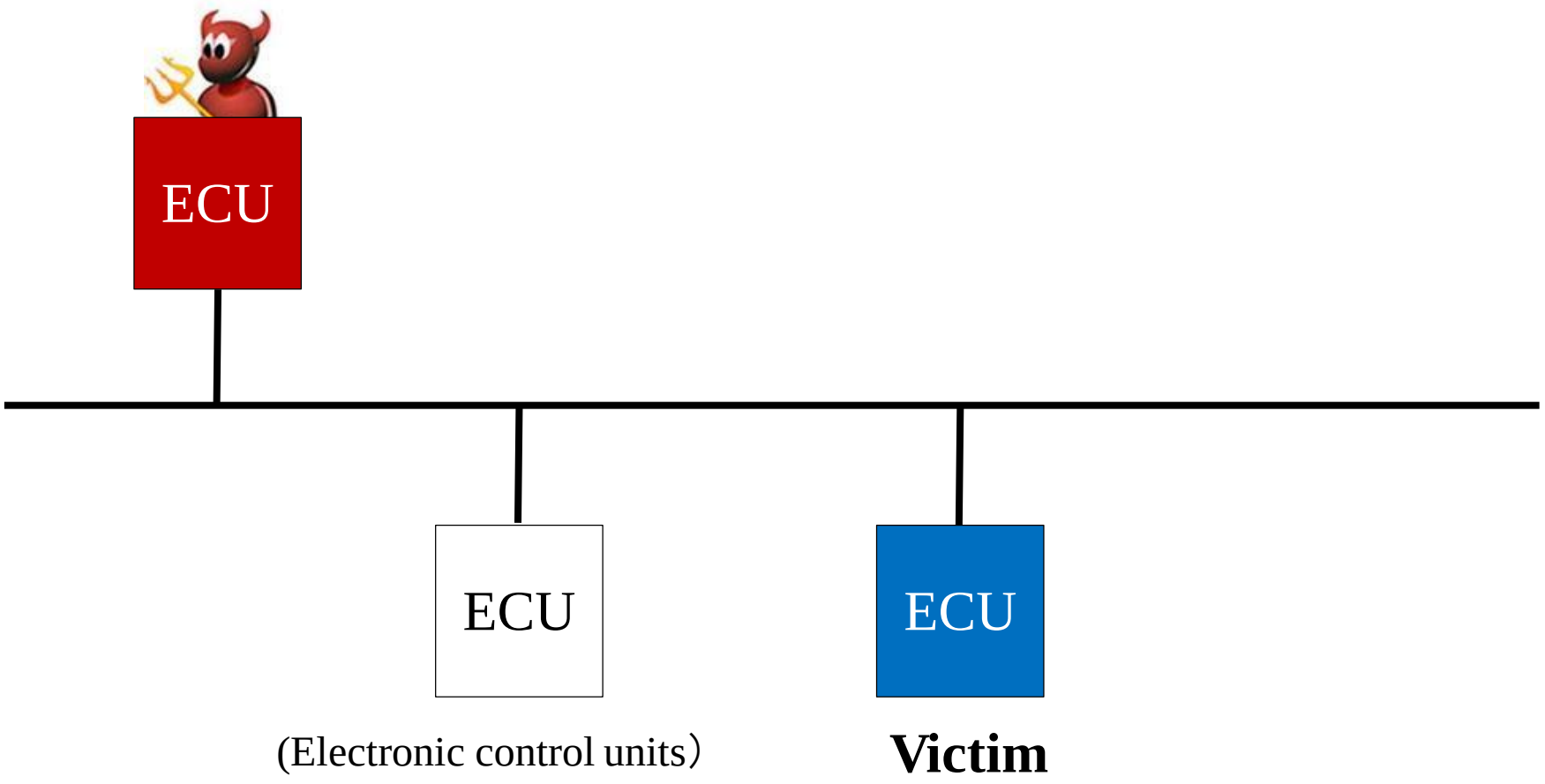
Bus-off Attack: Bypassing Error Handling

Shut down uncompromised (healthy)

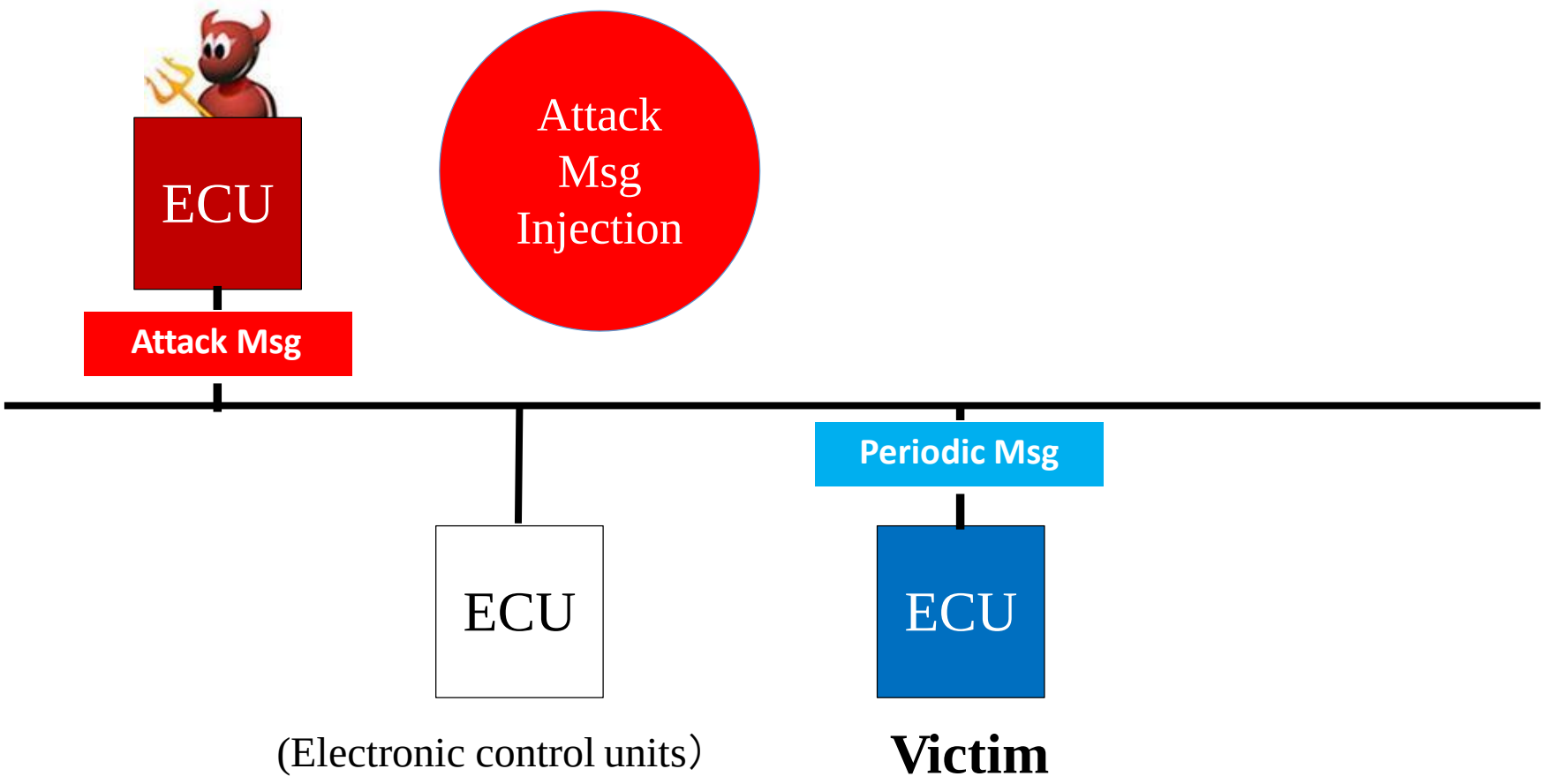
in-vehicle ECUs

with minimal number of injections

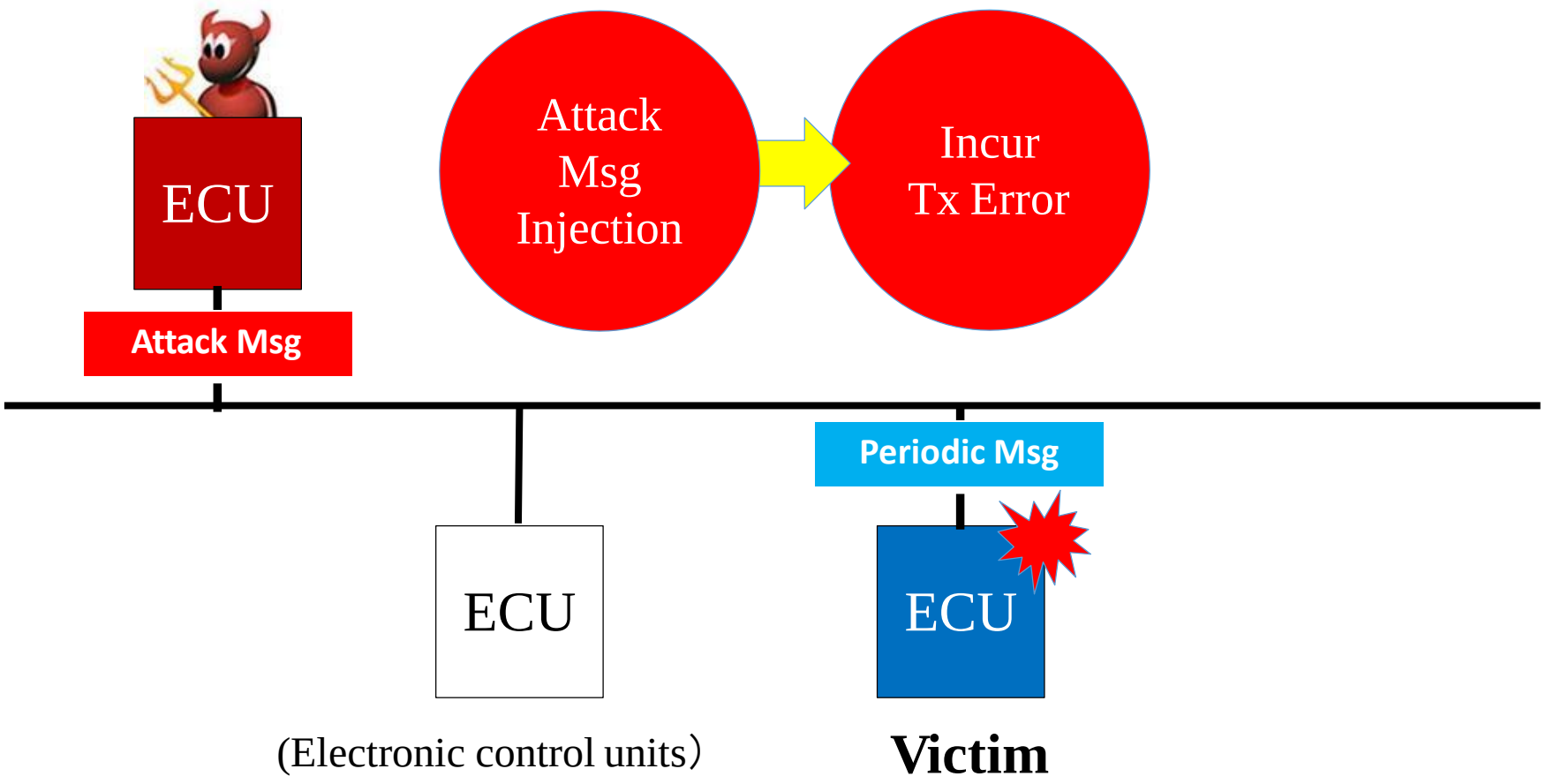
Bus-off Attack



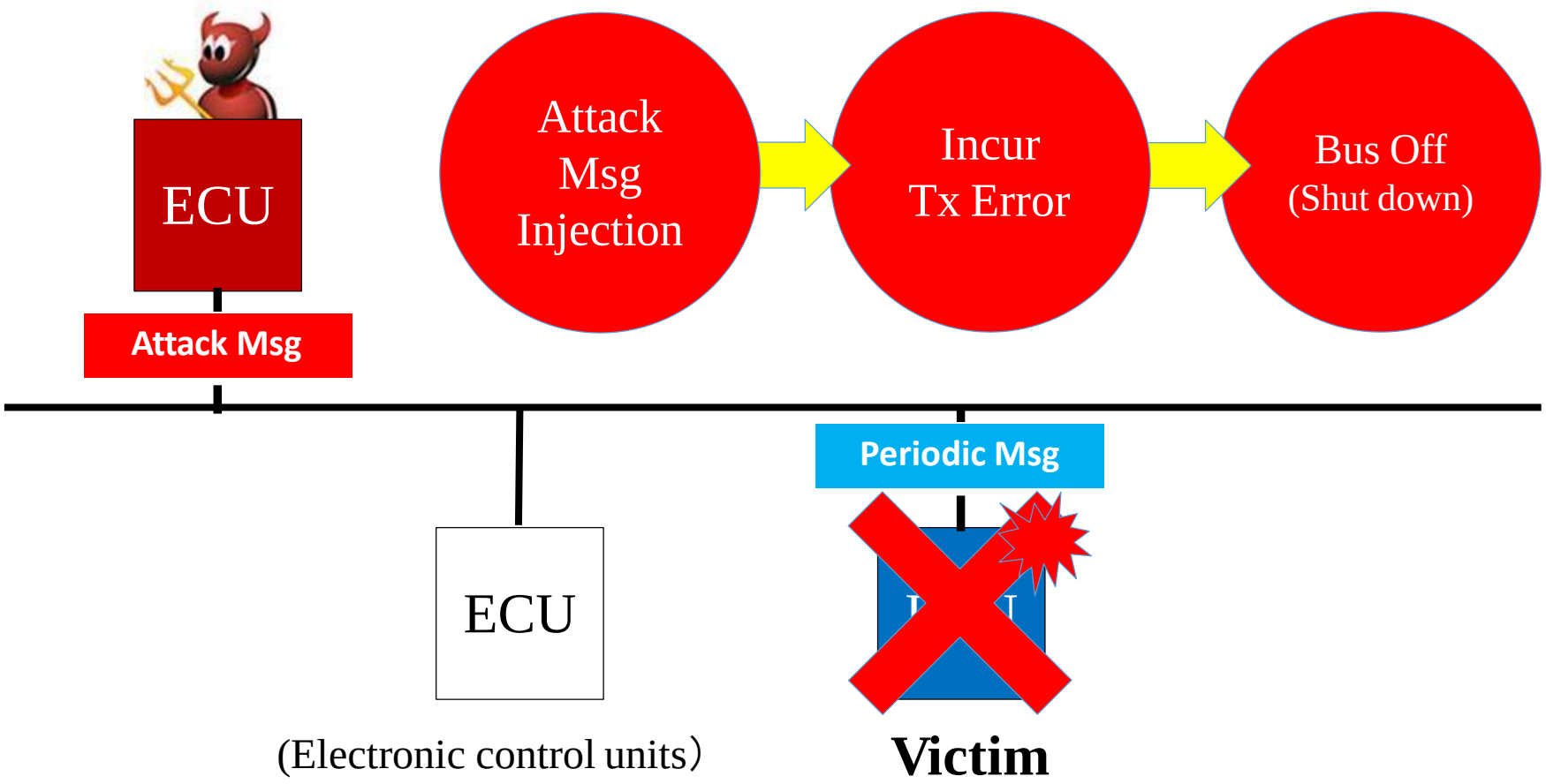
Bus-off Attack



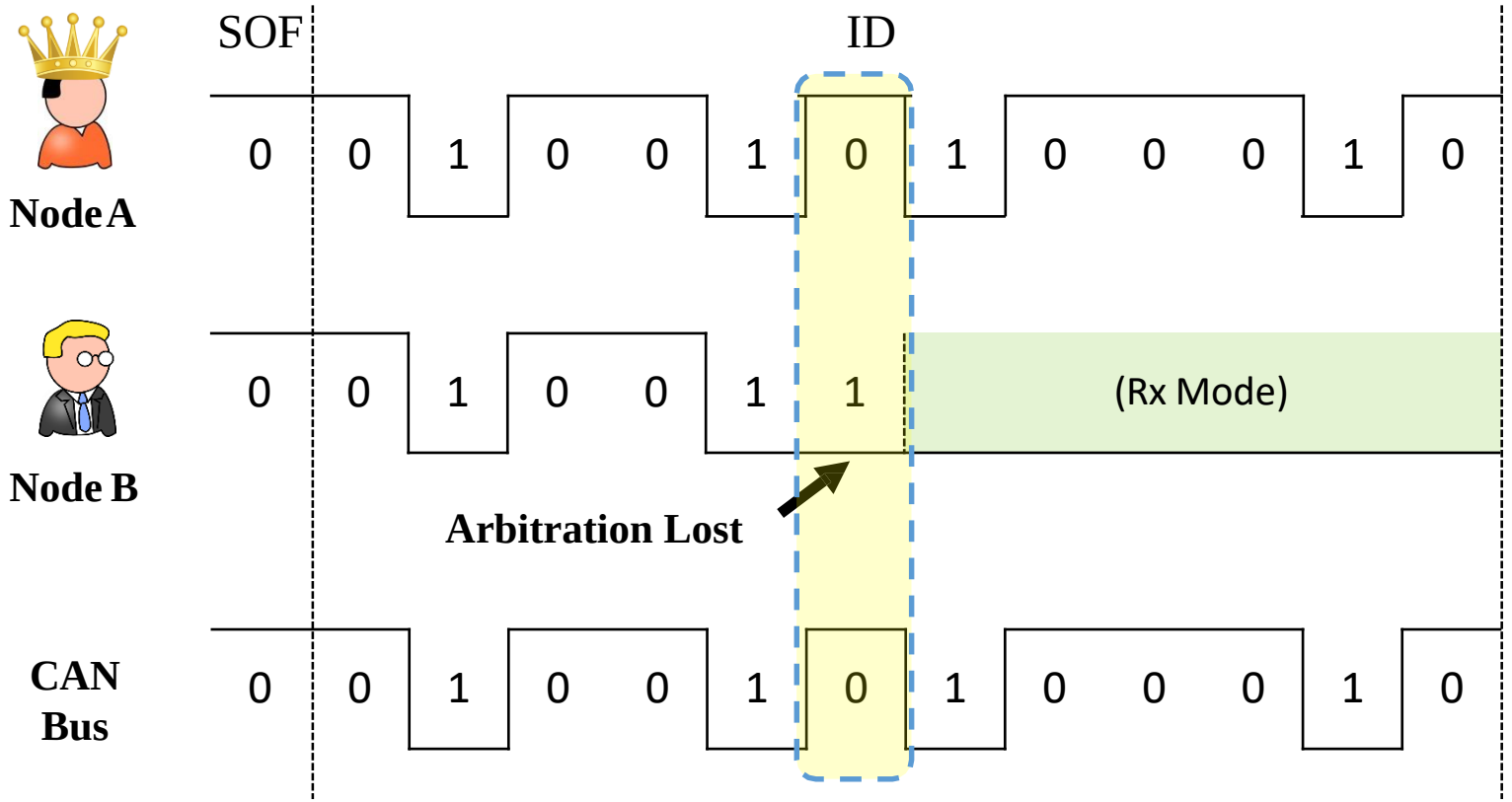
Bus-off Attack



Bus-off Attack

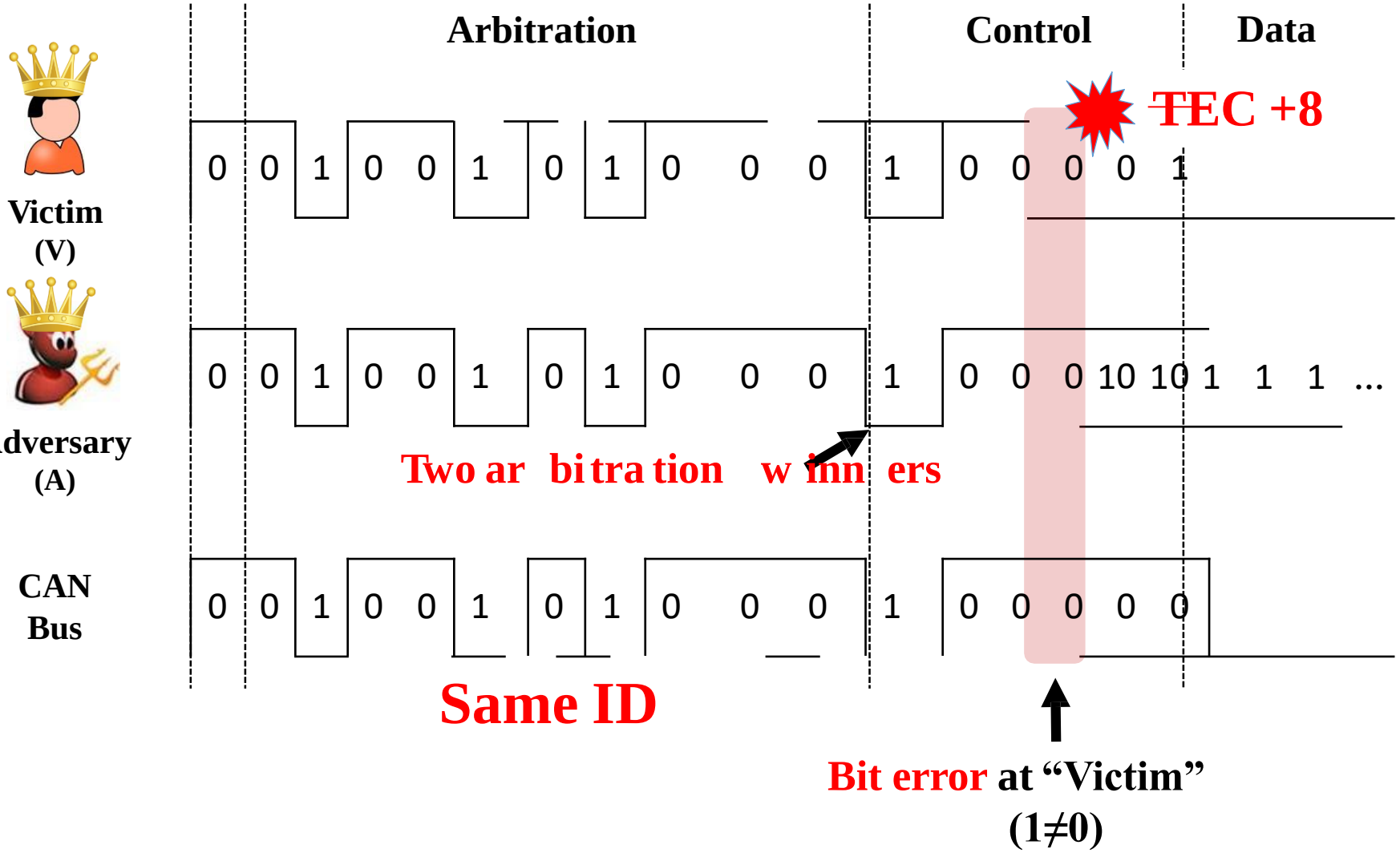


Arbitration in CAN Protocol

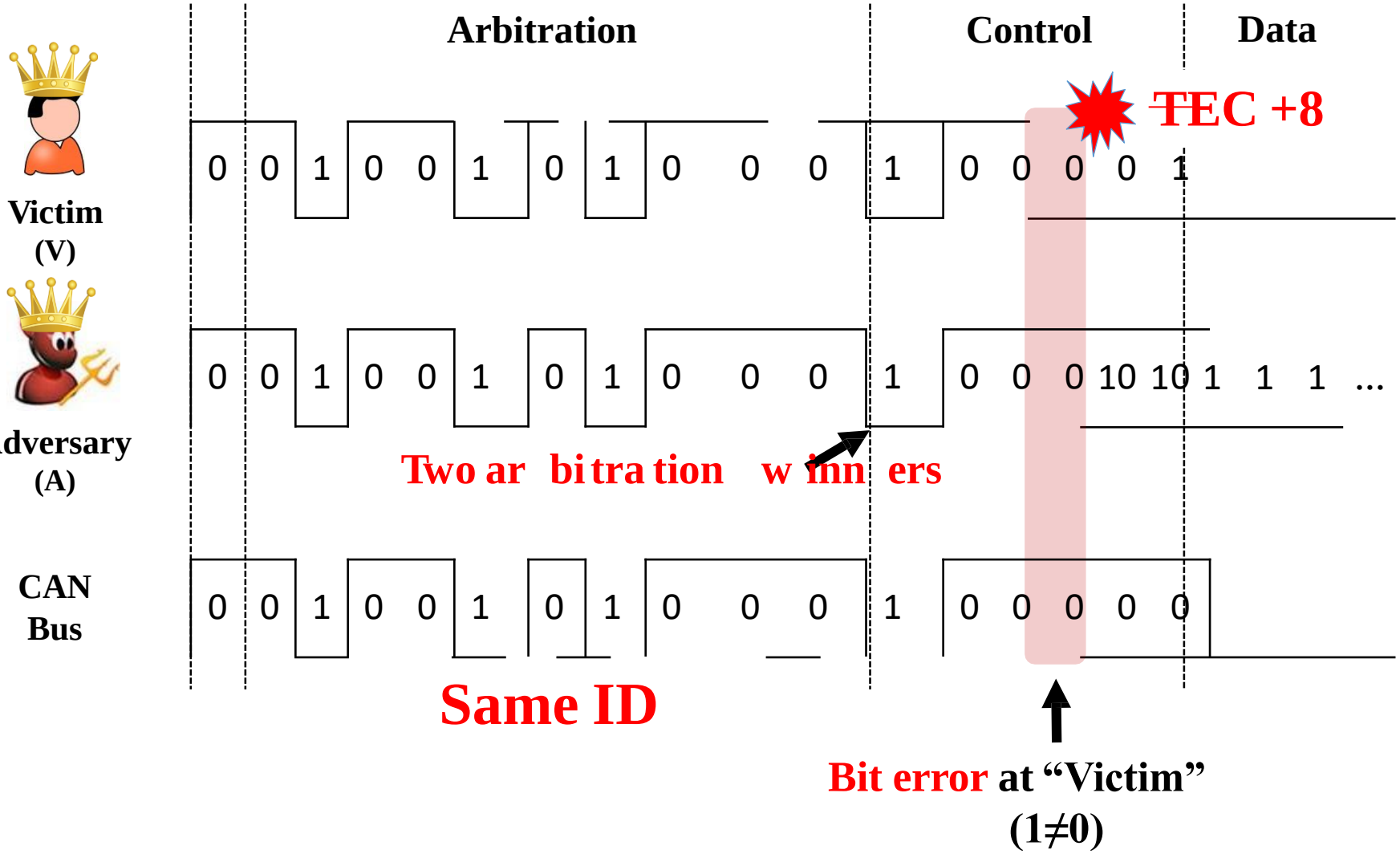


Only ONE arbitration winner !

Arbitration in Bus-off Attack



Arbitration in Bus-off Attack



Iteratively deceive the victim into thinking it is "erroneous"!

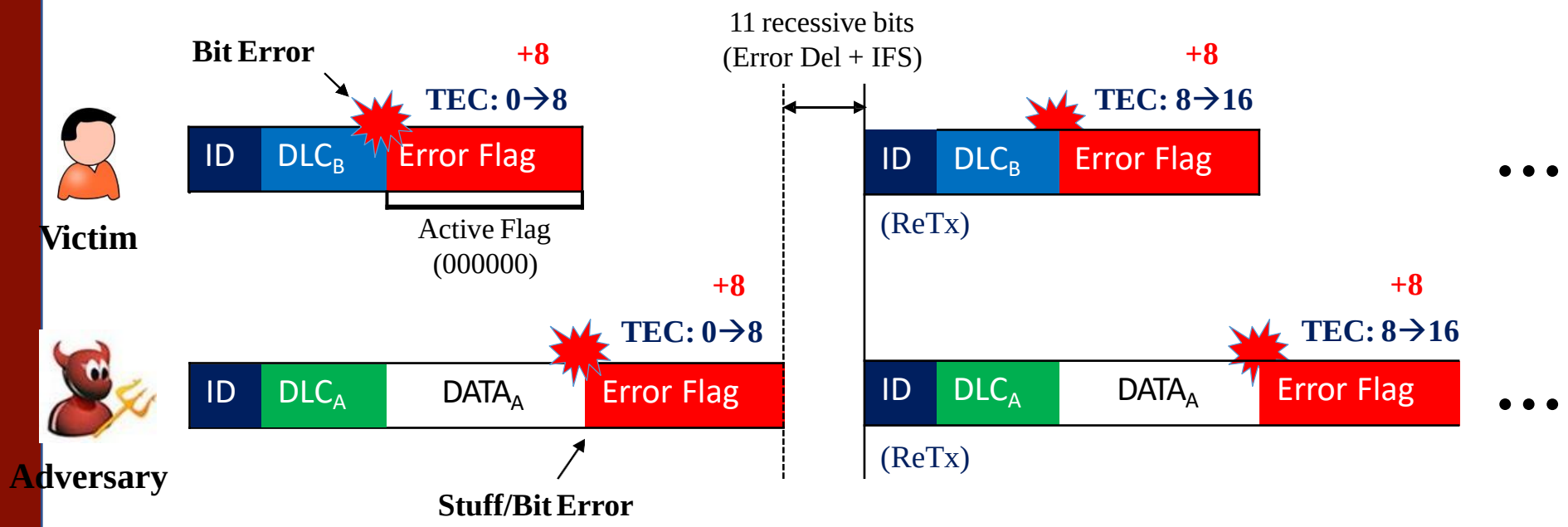
Bus Off
(Shut down)

Feasibility of Bus-off Attack

1. **Same ID:** the attack message to have the same ID as the target
2. **Content:** Having at least one bit position in which it is dominant (0), whereas it is recessive (1) in victim's message
3. **Timing:** Adversary should synchronize its transmission time with that of victim's. This can be done by monitoring preceding messages

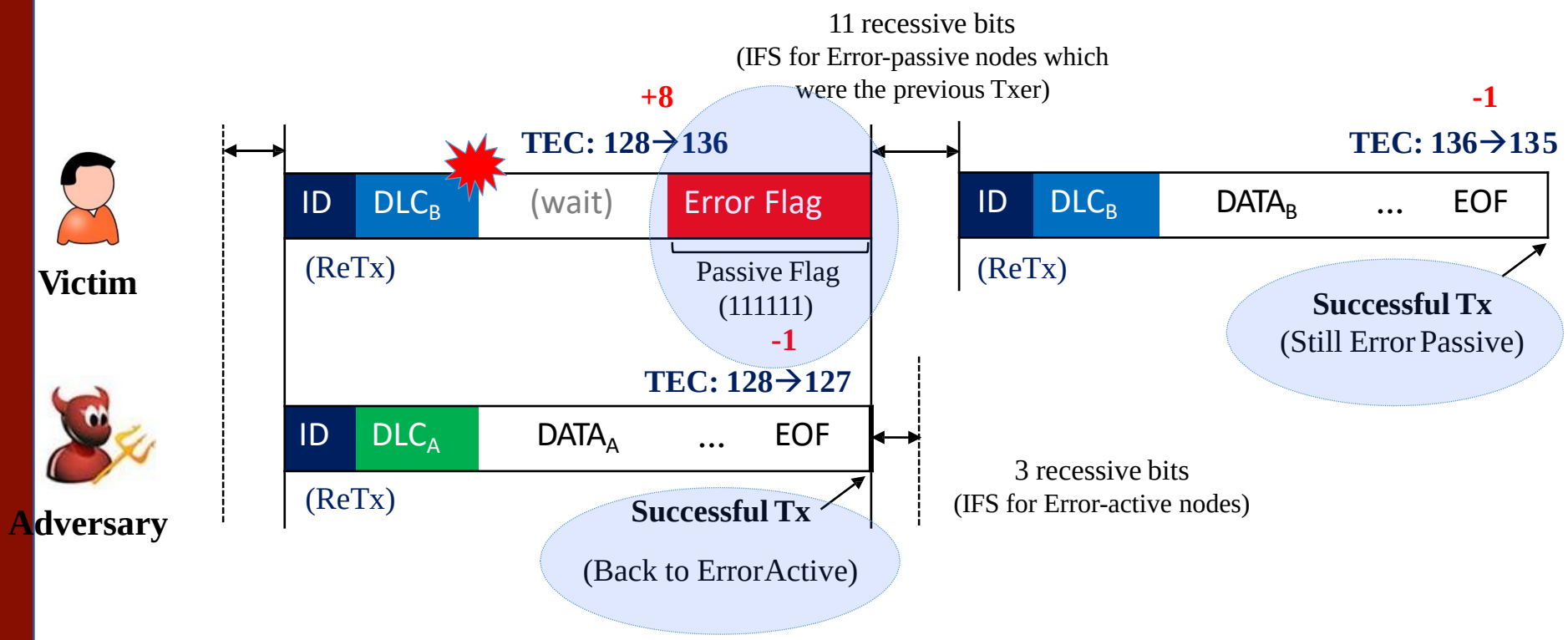
Bus-off Attack: Phase 1

Victim in Error Active mode



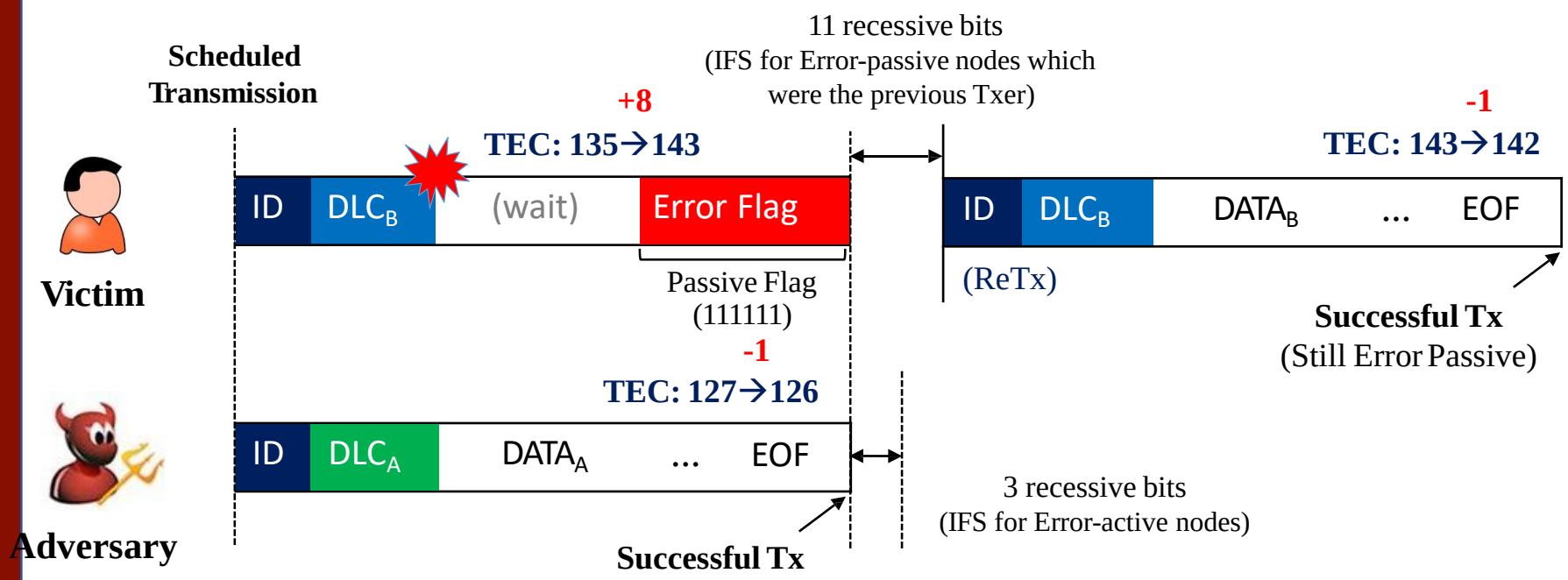
Bus-off Attack: Phase 1 to Phase 2

Both nodes concurrently enter Error Passive mode.



Bus-off Attack: Phase 2

Victim in Error Passive mode



Countermeasures

F1: Indication

In phase 1, due to CAN's automatic retransmission, at least two consecutive errors occur during the Tx of frames. Thus, we watch for consecutive error frames with an active error flag.

F2: Fact

In phase 2, due to the difference in error modes, at the time when the (error-passive) victim's TEC increases, a message with the same ID will be successfully transmitted by some ECU on the bus.

Defense Mechanism:

An ECU or its error counters are reset whenever F2 is observed after N consecutive error frames.