CONTROL SCHEME STRATEGIES FOR SEU-INDUCED PROTECTION RELAY FAILURES

Paper No. PCIC Europe 26_05

Andrea Santarpia
SBM Offshore
11, Av. Albert II, 98000
Monaco
Andrea.Santarpia@sbmoffshore.com

Abstract – Over a 24-month period, more than fifteen incidents occurred on SBM Offshore FPSO units due to protection relays rebooting after Single Event Upsets (SEUs). These transient faults – caused by high-energy particle interactions with microprocessor-based electronics – resulted in unintended breaker or contactor operations, production losses, and operational disruption. This paper outlines the physical mechanisms behind SEUs, their impact on protection devices in offshore environments, and mitigation measures implemented within control schemes to enhance resilience and maintain process continuity.

Index Terms — Protection Relays, Single Event Upset (SEU), Flip-Bit, Electrical Control Schemes.

NOMENCLATURE

FPSO	Floating Production Storage and Offloading
MV	Medium Voltage
LV	Low Voltage
IED	Intelligent Electronic Device (Protection Relay)
IC	Integrated Circuit
SEU	Single Event Upset
SRAM	Static RAM (Random Access Memory)
DRAM	Dynamic RAM (Random Access Memory)
FPGA	Field Programmable Gate Array
VCB	Vacuum Circuit Breaker
VSC	Vacuum Switch Contactor

I. INTRODUCTION

Soft memory errors caused by high-energy particles have been documented for decades, particularly in aviation and aerospace applications [1][2]. These “random, nonrecurring, single-bit” soft errors affect only stored data, cause no physical damage, and are cleared by the next write cycle. Their effects range from correctable malfunctions to conditions requiring device reboot.

A Single Event Upset (SEU) is a soft error caused by the interaction of a single energetic particle with a memory cell. This paper reviews SEU mechanisms and mitigation strategies, with emphasis on incidents from offshore floating facilities and control-scheme adaptations used to reduce operational impacts.

II. SEU DEFINITION, CAUSES AND EFFECTS

An SEU is a bit flip in a writable memory cell resulting from a single energetic particle strike. Two main particle sources dominate:

- Cosmic-ray-induced particles, generated in atmospheric cascades. Some reach sea level and can interact with sensitive electronics (Figure 1).
- Radioactive traces in packaging materials, which can emit alpha particles capable of disturbing semiconductor structures (Table 1).

A. Cosmic particle radiation

Primary cosmic rays produce cascades of secondary particles in the atmosphere; a fraction reaches ground level and can upset electronic devices. Particle flux varies with altitude and geomagnetic latitude: higher elevations and polar regions experience higher exposure, increasing SEU likelihood. Figure 1 illustrates this process.

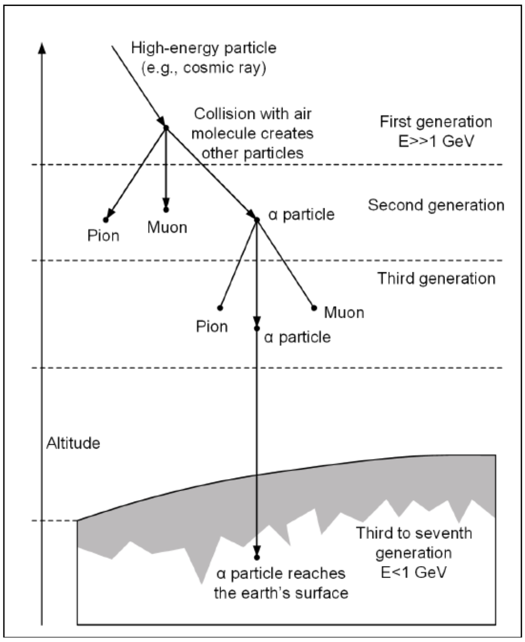

Figure1: Particle collisions in the atmosphere [7]

B. Nuclear traces in semiconductor packaging material

Radioactive contaminants in IC packaging were first identified as a soft-error source in the late 1970s [2]. Encapsulants and metals emit varying levels of alpha radiation (Table 1), and emitted particles may reach sensitive device regions.

C. Bit Flip Process

Energetic particles generate electron–hole pairs along their track. If the collected charge exceeds a circuit’s critical charge, the node voltage is disturbed (Figure 2). In bistable structures (Figure 3), this disturbance may cause the cell to switch states, producing a bit flip. As devices scale down and supply voltages drop, susceptibility increases

TABLE I
TYPICAL ALPHA FLUX FROM PACKAGING MATERIALS (APPROX. VALUES)

Material category	***Material component***	***Alpha Flux $(\alpha/cm^2 * h)$***
Hermetic	*Hermetic Sealing Glass*	*10 – 100*
Ceramic	*Alumina Ceramics (Standard)*	*0.1 – 1*
Ceramic	*Low Alpha Alumina Ceramics*	*≈0.01*
Metal/Solder	*Solder (Sn-Pb, Conventional)*	*~1.0*
Metal/Solder	*Low Alpha Lead/Solder*	*< 0.01*
Metal/Solder	*Ultra-Low Alpha (ULA) Solder*	*< 0.002*
Metal/Solder	*Super ULA Solder*	*< 0.001*
Silicon	*Silicon Die (Surface)*	*< 0.1*
Packaging	*Gold Plating/Metal Lids*	*< 0.1*
Polymer	*Molding Compounds/Epoxies*	*Variable (trace U/Th)*

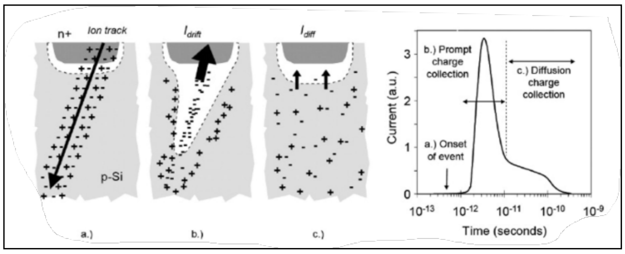

Figure 2: Illustration of the Bit-Flip process [7]

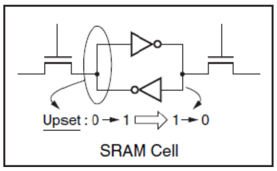

Figure 3: SRAM cell representation

D. Impacts on Protection Relays

Because protection relays depend on memory, logic, and processors for measurement and control, bit flips may affect communication, logic evaluation, or trigger unintended operations. Some devices automatically reboot on error detection, which can open breakers or contactors. At sea level, soft-error MTBF values of roughly 50–250 years are typical [7][8][9], but susceptibility rises in harsher radiation environments.

E. Mitigation methods

Mitigation approaches include low-alpha packaging materials, protective coatings, improved circuit tolerance, and system-level logic to reduce the operational impact of SEUs.

The following sections analyze the incidents within the SBM Offshore fleet and the control-scheme strategies used to prevent recurrence.

III. INCIDENTS IN SBM OFFSHORE FLEET

Although the manufacturer specifies an MTBF of 114 years, operational data from the past 24 months indicates significantly higher SEU occurrence. Across 490 relays of identical type (manufactured in 2019–2023), more than fifteen confirmed SEU-related events were recorded on SBM Offshore FPSOs. Both HV and LV relays were affected, leading to disturbances ranging from accommodation blackouts to full production upsets and loss of several thousand barrels of oil.

Events occur without warning and leave no trace in the relay's event recorder. Evidence is found only in internal logs, obtainable through a dedicated extraction process.

In all cases, an SEU-induced bit flip forced an automatic reboot of either the FPGA or communication card. During reboot, all digital outputs revert to their neutral state (open if N.O., closed if N.C.), directly influencing controls and breakers or contactor circuits.

Figure 4 illustrates the VCB/VSC opening command scheme applied onboard the FPSOs.

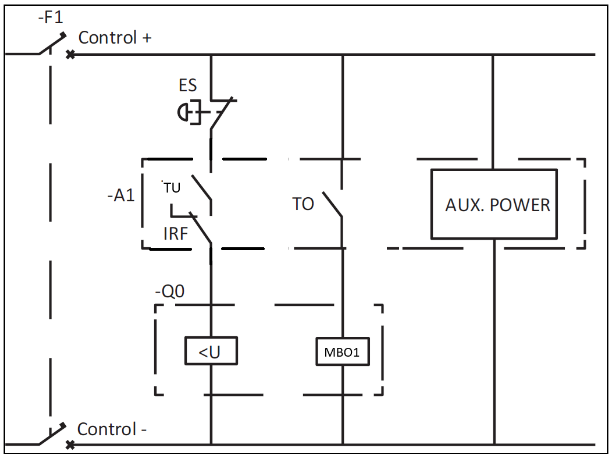

Figure 4: VCB and VSC opening commands scheme:

A1	*Protection relay*
ES	*Local Emergency Stop*
TU	*Trip Undervoltage (N.O. relay configurable D.O.)*
IRF	*Internal Relay Fault (N.O. relay dedicated D.O.)*
TO	*Trip Opening Coil (N.O. relay configurable D.O.)*
Q0	*VCB / VSC*
U<	*Undervoltage Coil (fail-safe)*
MBO1	*Opening Coil (energize to trip)*

When the relay reverts to its neutral state, the undervoltage coil, normally energized for fail-safe operation, de-energizes. This triggers the undervoltage release and causes the breaker or contactor to open.

IV. CONTROL SCHEME STRATEGIES

The undervoltage-coil command in Figure 4 follows a fail-safe philosophy: loss of the energizing signal opens the breaker. While beneficial for protection integrity, this design makes the circuit vulnerable to unintended opening during a relay reboot caused by an SEU.

Mitigation depends on required availability and the system's tolerance for temporary loss of control and protection. Relay reboot times range from a few seconds to around twenty seconds; the scheme must therefore accommodate this temporary unavailability.

When uninterrupted control and protection is required, redundant relays schemes may be implemented, as illustrated in Figure 5. In this setup, protection continuity is maintained even if one relay undergoes a reboot. Although this solution ensures continuity of control and protection – and the probability of both relays rebooting simultaneously is extremely low – the added hardware, possible larger footprint, and increased maintenance requirements, make it suitable only for applications where any loss of control and protection lead to significant operational and/or safety consequences.

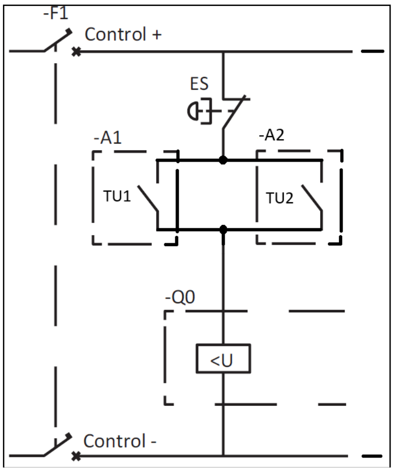

Figure 5: redundant scheme

A1	*Protection relay 1*
A2	*Protection relay 2*
ES	*Local Emergency Stop*
TU1	*Trip UV1 (N.O. relay configurable D.O.)*
TU2	*Trip UV2 (N.O. relay configurable D.O.)*
Q0	*VCB / VSC*
U<	*Undervoltage Coil (fail-safe)*

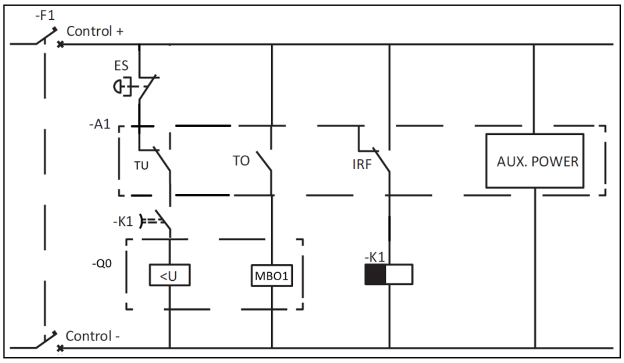

Figure 6: opening command scheme

A1	*Protection relay*
ES	*Local Emergency Stop*
TU	*Trip Undervoltage (N.C. relay configurable D.O.)*
IRF	*Internal Relay Fault (N.O. relay dedicated D.O.)*
TO	*Trip Opening Coil (N.O. relay configurable D.O.)*
K1	*Time-off relay*
Q0	*VCB / VSC*
U<	*Undervoltage Coil (fail-safe)*
MBO1	*Opening Coil (energize to trip)*

Where brief protection loss is acceptable – such as when robust upstream and downstream protections are in place – the undervoltage command can be wired through a normally closed (N.C.) digital output, as shown in Figure 6. In this arrangement, the relay's neutral state does not deenergize the undervoltage coil, preventing unintended trips during reboot. A supervised time-off relay is added to ensure tripping capability in case of permanent relay failure. Compared to the redundant solution, this approach reduces both cost and maintenance effort. However, during the relay reboot, protection temporarily shifts to backup protections, which may affect plant operations. The operational risk remains limited to the rare scenario where a relay reboot coincides with an equipment failure.

An additional key factor when selecting between these schemes – beyond protection continuity – is the plant's switching and control requirements, particularly in systems that experience a high rate of switching operations

While the redundant scheme ensures near-complete immunity of control functions during relay reboot, the single-relay configuration may temporarily impair operation (e.g., missed open/close commands to the VSC). For this reason, the designer should adopt either the redundant scheme, or the single-relay scheme with hardwired control circuits, acknowledging the corresponding impacts on capital and operative costs.

V. CONCLUSIONS

Analysis of SEU-driven relay failures shows that control scheme design, rather than relay hardware, is the primary factor in limiting operational impact. Because SEUs can trigger unexpected reboots, schemes relying on normally energized fail-safe signals (e.g., undervoltage releases) are particularly vulnerable to spurious openings.

To avoid production losses, control logic must tolerate short relay interruptions. Redundant architectures are preferred where continuous protection and control is mandatory, while N.C. undervoltage command schemes, coupled with a supervised time-off relay, are suitable where brief protection gaps are acceptable.

Selecting the appropriate mitigation strategy improves overall system resilience and significantly reduces the operational impact of SEU-induced relay reboots.

VI. REFERENCES

[1] E. Normand, J. L. Wert, H. Quinn, T. D. Fairbanks, S. Michalak, G. Grider, P. Iwanchuk, J. Morrison, S. Wender, and S. Johnson, "First Record of Single-Event Upset on Ground, Cray-1 Computer at Los Alamos in 1976," IEEE Transactions on Nuclear Science, Vol. 57, Issue 6, December 2010, pp. 3114–3120.

[2] T. C. May and M. H. Woods, "Alpha-Particle Induced Soft Errors in Dynamic Memory," *IEEE* Transactions *on Electron Devices*, Vol. 26, Issue 1, January 1979, pp. 2–9.

[3] J. F. Ziegler and W. A. Lanford, "Effect of Cosmic Rays on Computer Memories," Science, Vol. 206, Issue 4420, November 1979, pp. 776–788.

[4] A. Taber and E. Normand, "Single Event Upset in Avionics," *IEEE Transactions on Nuclear Science*, Vol. 40, Issue 2, April 1993, pp. 120–126.

[5] J. L. Wert, E. Normand, D. L. Oberg, D. C. Underwood, M. Vallejo, C. Kouba, T. E. Page, and W. M. Perry, "Single Event Effects Test and Analysis Results from the Boeing Radiation Effects Laboratory (BREL)," proceedings of the IEEE Radiation Effects Data Workshop, Seattle, WA, July 2005.

[6] Single-Event Effect Activities at CIAE - The 6th INFN National School on Detectors and Electronics. GUO Gang March 2015, Padova, Italy
[7] D. Haas and K. Zimmerman, “Single Event Upsets in SEL Relays” – March 2018.
[8] K. Zimmerman and D. Haas, “Impacts of single event upsets on protective relays”, 72nd Annual Conference for Protective Relay Engineers, College Station, TX, USA, 25–28 March 2019.
[9] White paper “Single Event Upset”, Published by Siemens Smart Infrastructure Digital Grid, June 2021.

II. VITA

Andrea Santarpia serves as the Electrical Global Operations Technical Authority at SBM Offshore. He earned a master’s degree with honors in electrical engineering from the University of Rome “La Sapienza” in 2010. His professional experience includes roles as Electrical Lead Engineer at Technip Italy, Electrical Project Lead at Kinetics Technology (Maire Tecnimont Group), and Asset Integrity Electrical Engineer at SBM Offshore, where he later assumed responsibilities as EC&I Group Lead and Digital Solution Lead.
He is an individual member of the IEEE Industry Applications Society (IAS).
andrea.santarpia@sbmoffshore.com