Impacts of Single Event Upsets on Protective Relays

Karl Zimmerman and Derrick Haas, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—As early as the 1970s, the computing, aviation, and space exploration industries were aware of transient memory errors resulting from high-energy particles. These errors, which have been defined as "random, nonrecurring, single bit errors in memory devices," have become known as single event upsets (SEUs). SEUs do not damage the components themselves but can cause a memory bit to change state from a 0 to a 1, or vice versa. These changes, if they occur in memory applied in a protective relay, can produce a self-test error or even an undesired operation.**

This paper examines SEUs, their causes, mitigation methods, and most importantly, how engineers can make the protection system more resilient if or when SEUs occur. We quantify how often SEUs are likely to occur and suggest and compare some practical application and control design solutions.

I. Background

Reference [1] outlines the impact of single event upsets (SEUs) on microprocessor-based relays. The purpose of this paper is to summarize [1] and provide practical application and control design solutions to mitigate the impact of SEUs.

As early as 1979, the computing industry knew of transient memory failures (or soft memory errors) resulting from high-energy particles [2]. Later research and review of data from the Cray-1 mainframe computer in Los Alamos, New Mexico, revealed evidence that an SEU (a type of soft memory error) occurred on that machine in 1976 [3]. Another publication in 1979 documented an SEU that occurred in space in 1975 [4]. These references show that for decades, this phenomenon has been known and has been documented extensively in the computing, aviation, and space exploration industries.

Soft memory errors are defined as "random, nonrecurring, single bit errors in memory devices" [2]. A soft error is not permanent, and the memory device recovers completely by the following write cycle with statistically no greater chance of error recurrence at that location than at any other bit location in any other memory component in the device. Soft memory errors do not damage the components themselves. SEU is nearly synonymous with soft memory error, but an SEU is not specific to a memory component. Similar soft error phenomena can occur with other digital components that make up modern microprocessor-based relays. This paper refers to these errors as SEUs. The space industry [5] has added terminology as knowledge of SEUs and their causes has increased to more specifically categorize the impact of these events. Some of these terms include:

- Single event upset (SEU)—a change of state or transient induced by an energetic particle such as a cosmic ray or proton in a device. This may occur in digital, analog, and optical components or may have effects in surrounding interface circuitry (a subset known as single event transients [SETs]). These are "soft" errors in that a reset or rewriting of the device causes normal device behavior thereafter.
- Single hard error (SHE)—an SEU that causes a permanent change to the operation of a device. An example is a stuck bit in a memory device.
- Single event latchup (SEL)—a condition that causes the loss of device functionality due to a single event-induced, high-current state. An SEL may or may not cause permanent device damage, but it requires power strobing of the device to resume normal device operations.
- Single event burnout (SEB)—a condition that can cause device destruction due to a high current state in a power transistor.
- Single event gate rupture (SEGR)—a single ion-induced condition in power metal-oxide-semiconductor field-effect transistors (MOS FETs) that may result in the formation of a conducting path in the gate oxide.
- Single event effect (SEE)—any measurable effect to a circuit due to an ion strike. This includes (but is not limited to) SEUs, SHEs, SELs, SEBs, SEGRs, and single event dielectric ruptures (SEDRs).
- Multiple bit upset (MBU)—an event induced by a single energetic particle such as a cosmic ray or proton that causes multiple upsets or transients during its path through a device or system.
- Linear energy transfer (LET)—a measure of the energy deposited per unit length as an energetic particle travels through a material. The common LET unit is MeV • cm^2/mg of material (e.g., Si for MOS devices).
- Threshold LET (LETth)—the minimum LET to cause an effect at a particle fluence of 1E7 ions/cm^2. Typically, a particle fluence of 1E5 ions/cm^2 is used for SEB and SEGR testing.

A. Causes

SEUs are caused by high-energy particles, which come from two primary sources: cosmic rays radiating particles that interact with the earth's atmosphere and trace elements in semiconductor packaging material that emit particles. This section provides an overview of each source. As high-energy particles from cosmic rays collide with atoms in the earth's atmosphere, other particles are emitted as a result. These subsequent particles can then go on to collide with other atoms, and some particles may eventually reach the earth's surface. Fig. 1 illustrates the collision process.

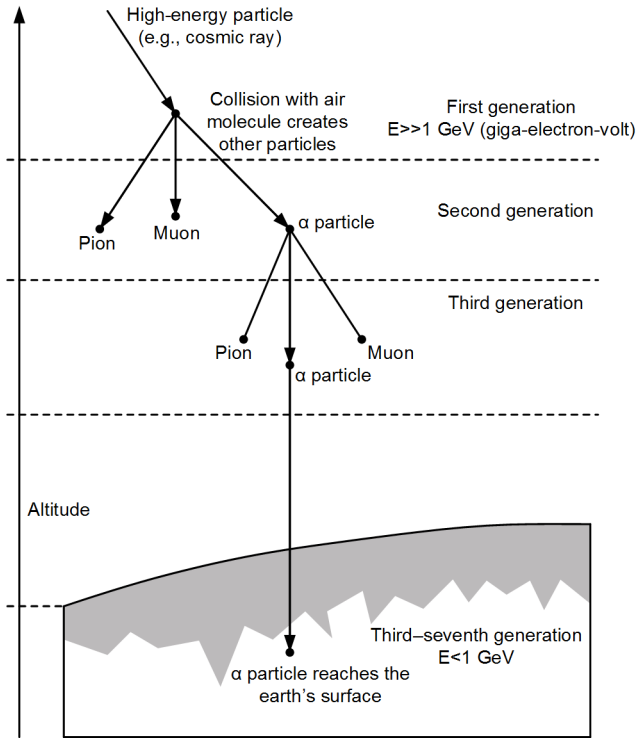

Fig. 1. Diagram of particle collisions in the earth's atmosphere

Of particular interest are collisions with nitrogen and oxygen molecules in the earth's atmosphere because these collisions often result in the creation of high-energy neutrons and of alpha (α) particles, which consist of two protons and two neutrons each. The collisions create other particles as well, such as pions and muons. However, it is the high-energy neutrons and the alpha particles in particular that can cause SEUs. Fig. 2 shows a rendering of a cosmic ray bombarding the earth's atmosphere and the numerous collisions and particles that a single cosmic ray can generate.

Of note is the amount of energy that a particle possesses, which is measured in electron-volts (eV). The energy attained by one electron after being accelerated through a potential difference of one volt is equivalent to 1 eV. A particle must have a sufficient energy level to cause an SEU, and certain particles will not interact with silicon to the same degree (beta and gamma particles have very low energy loss rates in silicon). Generally, SEU studies, testing, and literature only consider alpha particles and neutrons with energies of 1 MeV (million electron-volts) [6]. The amount of energy required for a particle to cause an SEU is dependent on the design of the digital component (e.g., processor or memory component), including aspects such as geometry and critical charge required for state change.

Fig. 2. Artwork of cosmic rays hitting Earth (credit: Mark Garlick/Science Photo Library)

The rate at which these particles pass through an area is called the particle flux. This is given as the number of particles passing through an area over an amount of time, with units of particles per cm^2 per hour. The particle flux gives us an idea of how many of these particles are present and can help evaluate the likelihood of a particle colliding with a digital component and causing an SEU. Because the earth's magnetic field and atmosphere impact many of these particles, the flux or frequency of the particles observed is higher at high altitudes and near the earth's magnetic poles. SEU occurrence rates are listed with the assumption that the component or equipment is at sea level at the latitude and longitude of New York City. Normalization factors can be used to convert SEU rates based on different latitudes, longitudes, and altitudes.

Fig. 3 shows the neutron flux levels at various altitudes. We can see that the neutron flux peaks at an altitude of approximately 60,000 ft above sea level and is several hundred times greater than the neutron flux at sea level. Similar data provide flux levels based on latitude [7]. Because of the higher levels of neutron flux at high altitudes, aeronautics and space exploration industries have an added interest in the impacts of high-energy particles on computing systems, including SEUs.

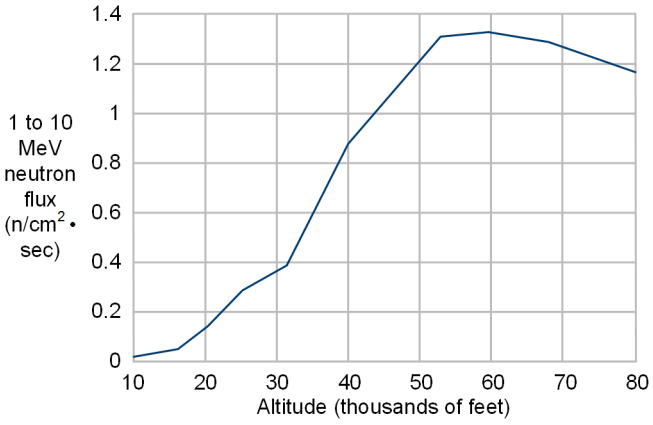

Fig. 3. Neutron flux versus altitude [6]

The second source of high-energy particles that can cause an SEU, digital component packaging material, was documented in 1979 [2]. Essentially every material has uranium, thorium, and other heavy radioactive elements present in small quantities. Digital component packaging material can therefore contain traces of these heavy elements. As the radioactive elements in the packing material decay, they often emit alpha particles. For clarity, the packaging or packing material in a microprocessor, memory chip, or an integrated circuit in general is the material (e.g., plastic) that encapsulates the semiconductor material that makes up the microprocessor. Fig. 4a shows a simplified diagram of a semiconductor device and its packaging material. Fig. 4b shows a microprocessor with a portion of the packaging material removed.

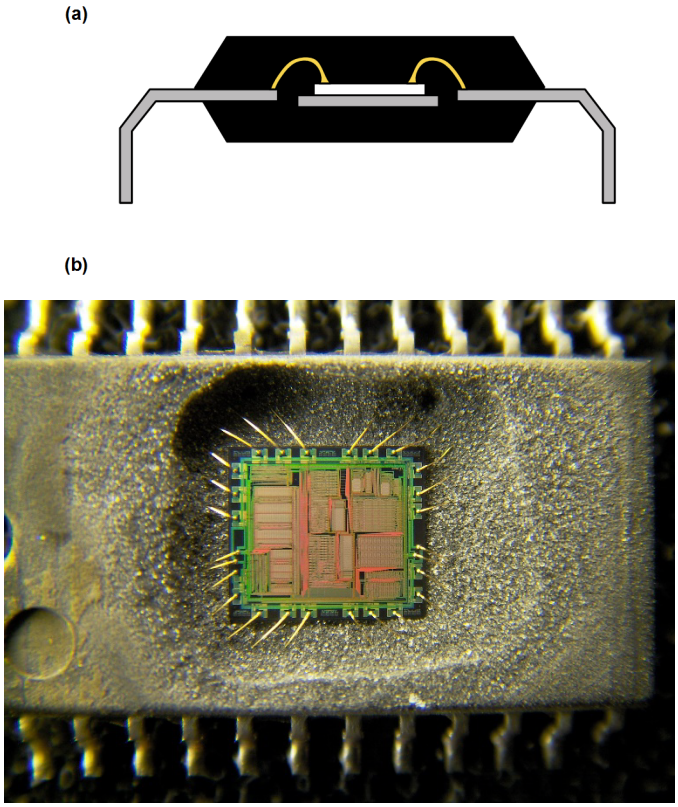

Fig. 4. Simplified diagram of semiconductor packaging material (a) and a microprocessor with some packaging material removed to expose the semiconductor device (b) [8]

Not much can be done to eliminate the SEU-causing sources like alpha particles and other high-energy particles coming from space. Fortunately, the earth's atmosphere does an excellent job of shielding us and our electronic devices from high-energy particles, making the statistical likelihood of an SEU resulting from a space particle relatively low for devices installed at low altitudes. Of course, at high altitudes or at an installation in the northern latitudes, the probability of a cosmic ray (or derivative particle) causing an SEU is higher. For alpha particles resulting from integrated circuit packaging material, microprocessor manufacturers are working to limit the impact of trace elements in packaging material. Integrated circuit suppliers have made significant improvements on packaging material quality and the number of impurities present. However, we cannot practically remove the sources of alpha particles or prevent the exposure of protective relays to them.

B. Bit Flip Mechanism

Now that we have established the sources of high-energy particles responsible for SEUs, we can share an example of how a high-energy particle causes a bit to flip. When an alpha particle collides with semiconductor material, it creates electron-hole pairs. This is theoretically possible in nearly every type and variety of memory element, processor, or gate. All digital components, from static RAM (SRAM) to dynamic RAM (DRAM) to field-programmable gate arrays (FPGAs) and more, have a non-zero SEU occurrence rate. However, certain digital components and their designs make SEUs more likely. Fig. 5 shows the sequence of events that leads to a bit flip from a 0 to a 1 in a single dynamic memory cell.

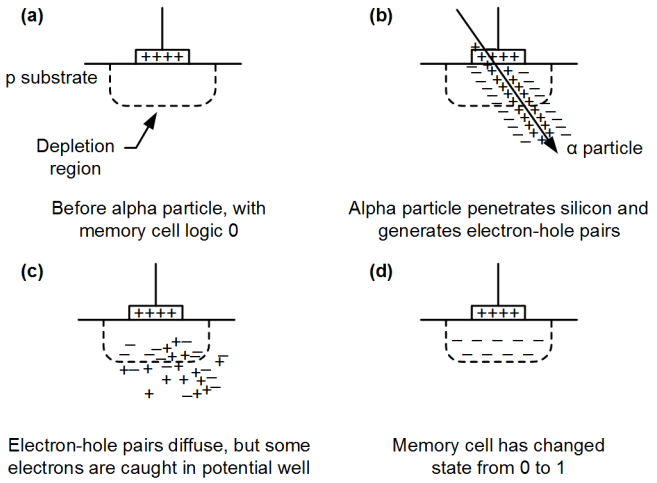

Fig. 5. Process of memory change from 0 to 1 because of alpha particle collision

The high-energy particle creates electron-hole pairs as it passes through the semiconductor material (Fig. 5b). An alpha particle with an energy of 5 MeV can create approximately $1.4 \cdot 10^6$ electron-hole pairs and typically penetrates 25 µm in silicon [2]. Most of the electron-hole pairs diffuse through the substrate material, as shown in Fig. 5c. However, the potential well captures some of these electrons and repels the holes. It is these captured electrons in the depletion region that result in a state change from a 0 to a 1 in this dynamic memory cell (Fig. 5d). The electrons trapped in the potential well diffuse over time. However, in certain systems, if a clock edge occurs before the electrons diffuse, the errant memory or bit flip is made permanent. The location, geometry, and arrangement of the semiconductor device, the amount of critical charge, and other factors impact how a particular device experiences an SEU. In addition, many of the same factors impact what type of SEU is generated and whether there is a bit flip from 0 to 1 or from 1 to 0.

II. Statistical Likelihood of SEUs and Measurement and Testing of SEU Rates

The estimated statistical likelihood of an SEU occurring is expressed as units of failures in time (FIT). The FIT rate is typically measured in failures per billion hours. It is now common for digital component manufacturers to provide an estimated FIT rate specification for the component, be it a microprocessor, FPGA, or RAM variety such as synchronous DRAM (SDRAM). The total FIT rate for a protective relay is the combined FIT rate of all of the digital components needed for a relay to perform its required function. For example, if a process critical to the functioning of a protective relay relied on three different components, each with a FIT rate of 100 failures per billion hours, then the expected FIT rate for the relay is 300 failures per billion hours.

In addition to evaluating a component FIT rate, both component and protective relay manufacturers are interested in determining the likelihood of an SEU occurring. Statistical models that predict the FIT rate of a memory cell have been around since SEUs were first discovered [2]. Testing the validity of such models is as important now as it was then. If a protective relay has a FIT rate of 400 failures per billion hours, that would equate to one failure every 285 years on average. However, waiting that long for an SEU to occur in order to validate the estimated FIT rate is beyond impractical.

Many components allow error injection, a way to simulate a bit flip without high-energy particle exposure. Another way to attempt to measure FIT rates is to place components or products in an environment with a higher exposure to alpha particles (or similar high-energy particles) than ground level. There are several high-energy particle sources where, statistically, the particle flux is significantly higher than what is observed naturally in a substation environment. These include nuclear reactors, particle accelerators, or similar energy sources that can generate high-energy particles. Fig. 6 shows microprocessor-based relays at a testing facility.

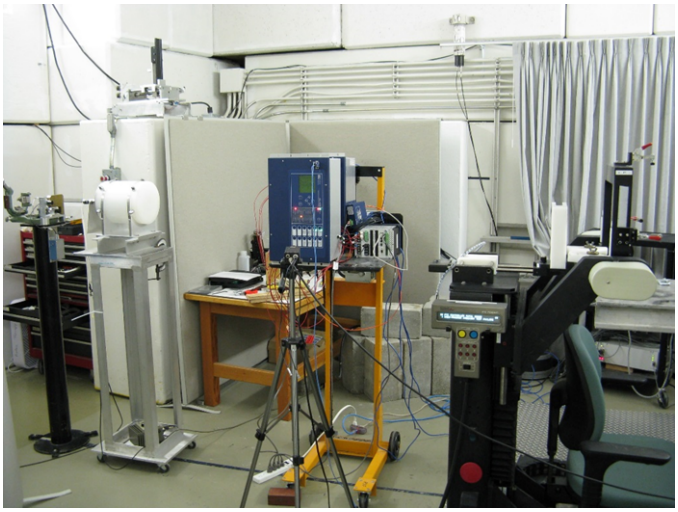

Fig. 6. SEU testing of microprocessor-based relays

Microprocessor-based relay manufacturers' interest in SEU testing is not only to evaluate the FIT rate, but more importantly to test mitigation techniques, which are discussed later in this paper. By putting the relays in an environment where SEUs occur much more frequently, we can evaluate the effectiveness of a variety of mitigating techniques.

Microprocessor-based relay manufacturers consider the overall quality and reliability of a component, as well as a component's features, supplier, price, and more. FIT rate is also considered. One design approach being implemented is to limit SEU rates to a mean time between SEUs (MTBSEU) of 500 years, equating to a FIT rate of approximately 228 failures per billion hours [1]. That means not only using FIT rate as a criterion for evaluating individual components but also considering mitigating techniques for SEUs as part of overall relay designs.

Gathering records of SEUs from field-installed relays can be more difficult. One corrective technique for an SEU is for the impacted device to restart or power cycle. Restarting the device overwrites the impacted device memory or instructions in a processor and removes the error. Most relays now log a time-stamped entry in the Sequential Events Recorder (SER) report when a relay restarts.

III. Impact on Protective Relays

The potential impact of an SEU can vary greatly. Microprocessors, FPGAs, and memory components are part of nearly every aspect of protective relaying, including analog-to-digital conversions, protection element algorithms and logic, and tripping decisions. An SEU that impacts a memory address related to a communication protocol may only result in a temporary loss of supervisory control and data acquisition (SCADA) communication or a report of an errant SCADA point. An SEU that impacts a measurement related to the power system current that is used by a protection algorithm may result in an incorrect measurement that could cause a protective element to incorrectly pick up. An SEU that directly impacts a word bit could result in an undesired operation. As these examples illustrate, the impact of an SEU can range from minor to severe.

The event report in Fig. 7 shows an undesired trip of a line current differential protection system that has been attributed to an SEU [9]. There is no fault on the line, and the differential element and TRIP87 word bit assert for no clear reason.

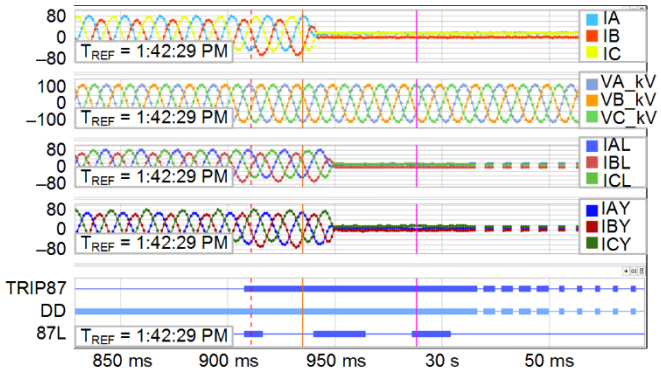

Fig. 7. Event report showing line relay trip as a result of an SEU

Most microprocessor-based relays come with mitigation capabilities to prevent undesired operations resulting from SEUs and, in some cases, to help the relay recover from SEUs gracefully and with minimal impact to protection. Furthermore, the statistical likelihood of an SEU causing an undesired operation is small. Based on field data, the mean time between undesired operations (MTBUO) due to SEUs over a five-year period (2012–2016) is greater than 50,000 years. Stated another way, if 50,000 relays are in service for one year, we will see one or fewer undesired operations due to SEUs.

IV. Mitigation and Prevention Techniques

Microprocessor-based relay manufacturers use several techniques to mitigate the effect of SEUs (see Table I). Note that SEUs can go undetected and/or result in undesired operations despite mitigation techniques.

TABLE I
MITIGATION AND PREVENTION TECHNIQUES AND CONSIDERATIONS

Consideration	Technique
Part selection	Select parts with low FIT rates, and balance build requirements with better SEU tolerance.
Design	Create and use internal relay data to assist in diagnosing relay memory if an in-service relay fails. Use error-correcting codes (ECCs) to detect and correct bit flips in real time. These require more memory and therefore impact hardware design. This method is used in hardened computers and in some microprocessor-based relays [10].
Relay disable	If an error is detected, clear the memory, assert the relay alarm or word bit (e.g., HALARM), and disable the relay. Relay users can cycle power once to see if the relay recovers. If a fault occurs while a relay is disabled, protection is disabled.
Diagnostic restart	If an error is detected, restart to maximize relay availability. Some relay models have automatic diagnostic restart functionality. Many of these models disable relay and alarm contacts for multiple restarts in a specific time frame. The number of restarts and the time frames vary between relay models. Many relays create a time-stamped entry in the SER report when a diagnostic restart occurs.

It is important to note that bit flips can also be the result of non-SEU events, such as component failures or manufacturing defects. One key distinction is that an SEU is random (particle emissions are random, and exactly when and where they hit the earth is random, but we can predict particle emission statistics). The statistical likelihood of having a repeated SEU on the same relay is small. Or, put differently, SEUs are very unlikely to be repeating errors. If we consider a relay with a FIT rate of 1,000 failures per billion hours, that rate equates to approximately one failure every 114 years.

In 1996, one microprocessor-based relay manufacturer began to enable devices to automatically restart in the event of a detected error. This particular relay had a setting named ERESTART [11]. If a critical RAM (CR_RAM) error is detected when ERESTART is set to Y, the relay automatically restarts. In addition, several commands are available to users so they can gather diagnostic information should a relay fail. Diagnostic restart is now part of the design of many other microprocessor-based relays.

V. Control Logic Design Considerations

As discussed in Sections III and IV, the most likely result of an SEU bit flip in a relay is a temporary alarm condition. If the relay is designed or set to automatically restart, the protection is disabled but restored within a few seconds. It is also possible for an undesired operation to occur due to an SEU (per Section III, one in 50,000 relay years). Even if these occurrences are infrequent, it is useful to evaluate how protection reliability is affected by SEUs and what remedial measures protection and control engineers can take.

Protection system reliability measures the certainty that the protection system will trip when required (dependability) and not trip when not required (security). Protection system reliability must be evaluated by considering all protection components, not just the relay.

Many industries, including nuclear, process control, rail, machinery, and aerospace, have developed standards like [12] to discover and eliminate design errors and to improve the reliability or safety margin of a device or system. In the following sections, we evaluate and compare a few of these approaches for transmission and distribution protection systems.

A. Transmission Lines

For transmission lines, many utilities deploy dual redundant schemes like the scheme shown in Fig. 8. Using the fault tree method demonstrated in [13] and [14], we compare the security and dependability of a protection system using line current differential and distance combined in one relay (87L/21).

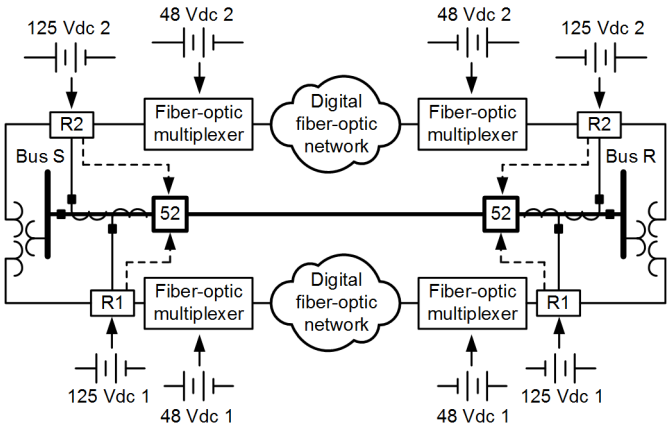

Fig. 8. Transmission line using redundant protection systems

For comparison, we evaluate three different tripping schemes: dual redundant (Fig. 9), two-out-of-three voting (Fig. 10), and interdependent tripping (Fig. 11). Fig. 12 shows the dependability comparison and Fig. 13 shows the security comparison.

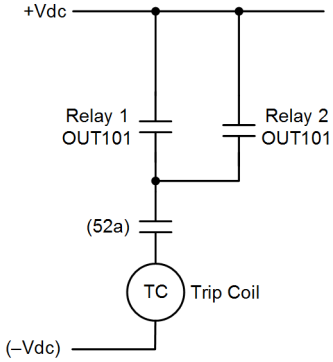

Fig. 9. Dual redundant tripping scheme

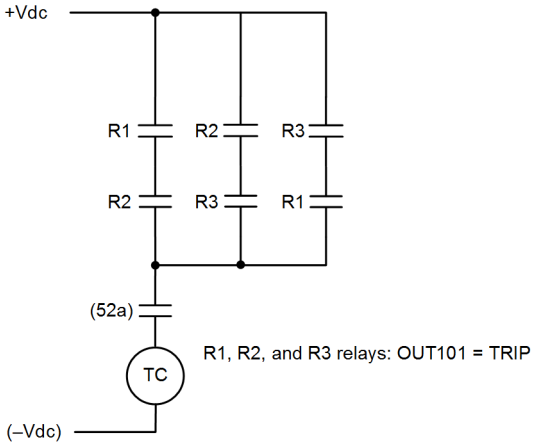

Fig. 10. Two-out-of-three voting scheme

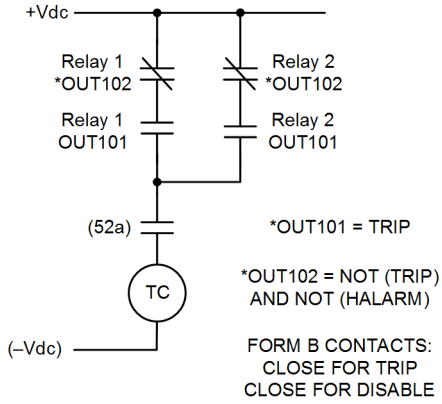

Fig. 11. Interdependent tripping scheme

The appendix shows several fault trees that are used to create the data in Fig. 12, Fig. 13, Fig. 16, and Fig. 17.

Dependability is excellent for both redundant and two-out-of-three voting schemes. The interdependent tripping scheme has poor dependability by comparison because both relay systems must trip for a fault to be cleared, unless the failure happens to be the relay.

Security is best when applying two-out-of-three voting schemes or interdependent tripping schemes. Dual redundant schemes are not as secure because any failed protection component of either scheme can cause an undesired operation.

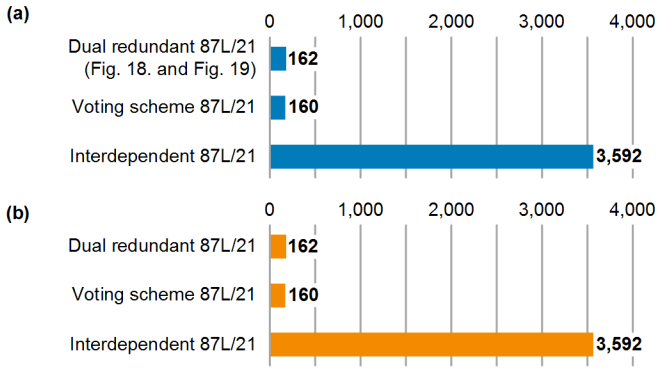

Fig. 12. Dependability comparison (unavailability) considering all undesired operations (a) and all undesired operations except those caused by SEUs (b).

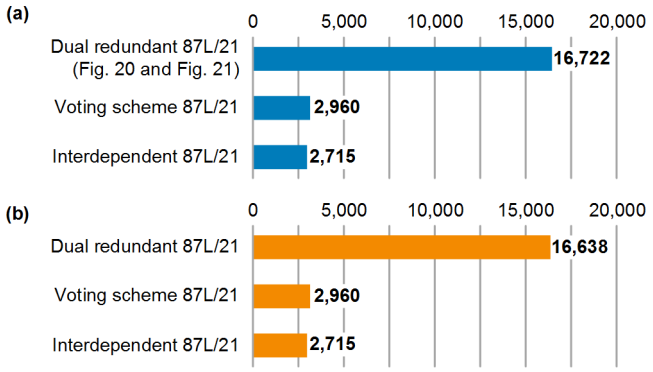

Fig. 13. Security comparison (failure rate) considering all undesired operations (a) and all undesired operations except those caused by SEUs (b)

In all cases, SEUs have little impact on the overall protection reliability. The main reason is because even if we eliminate all undesired operations due to SEUs, it has no impact on other factors—circuit breaker failure to interrupt current, breaker trip coil failures, dc battery failure, setting and/or application errors, current transformer (CT) and voltage transformer (VT) failures, communication equipment and channel failures, and all associated wiring errors.

B. Distribution Feeders and Motors

Most distribution feeders deploy simple overcurrent protection, as shown in Fig. 14.

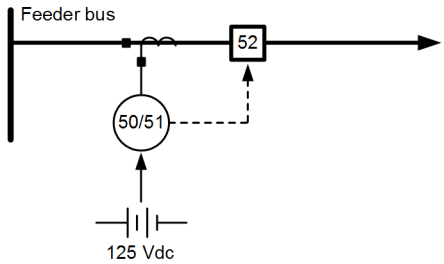

Fig. 14. Distribution feeder protection with 50/51

Like transmission, SEUs have only a small effect on distribution protection dependability and security because

unavailability due to relay failures is small compared with failures related to breakers, dc, and CTs.

However, some distribution applications have a much higher requirement for security. For example, some industrial processes and nuclear applications report using more secure tripping schemes (e.g., two-out-of-three voting scheme).

For comparison, we evaluate three different tripping schemes: single relay, two-out-of-three voting, and interdependent tripping. An interdependent tripping scheme is shown in Fig. 15. The comparison results are shown in Fig. 16 and Fig. 17.

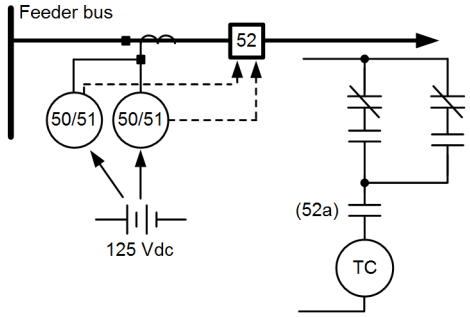

Fig. 15. Distribution feeder protection with dual 50/51 with interdependent tripping

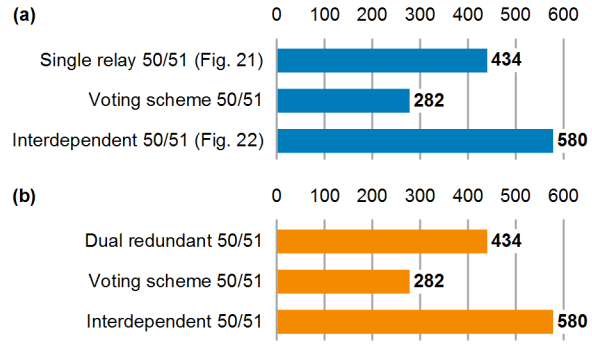

Fig. 16. Dependability comparison (unavailability) considering all undesired operations (a) and all undesired operations except those due to SEUs (b)

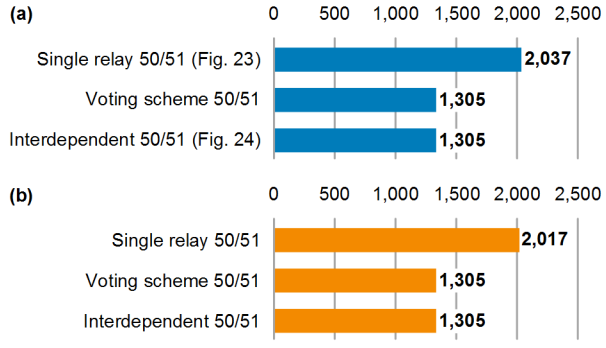

Fig. 17. Security comparison (failure rate) considering all undesired operations (a) and all undesired operations except those due to SEUs (b)

For these schemes, we assume a single breaker, one set of CTs, and a single dc supply. We can see all three schemes have good dependability, ranking from most to least dependable as voting scheme, single relay, and interdependent. The voting and interdependent schemes, as expected, have better security. As with transmission, the impact of SEUs appears to be very small.

Another possible impact of SEUs on distribution level applications appears to be on motors when "fail-safe" tripping is applied. Fail-safe tripping is when a relay alarm is set to intentionally produce a relay trip. However, only one such trip is documented in field data from 2012–2016.

VI. Recommendations

Based on field data, SEUs cause only a very small percentage of undesired operations. However, there are practical actions that users can take to reduce vulnerability to SEUs, including the following:

- Always monitor relay alarm contacts.
- Always collect SER data when available, which includes whenever a relay produces a diagnostic restart.
- Always act on service bulletins.
- Keep firmware and hardware updated to the latest versions when feasible, especially when the upgrade provides automatic diagnostic restart functionality.
- Ensure that the protective relay and protection system are secure during a diagnostic restart or power cycle [11].
- Use best practices and data to assess risk and to improve security and dependability [13] [14].

Automatic restarting clears the SEU. After restart, if the relay is still in failure mode, it is likely a hard failure. Relay users should contact the relay manufacturer and may need to return the device for such an occurrence.

VII. Conclusion

SEUs and their impacts on electronic devices have been known for decades but have become of increasing interest for protection schemes. Relay manufacturers have been aware of these phenomena and have applied mitigation techniques since at least 1996. The impact of most SEUs is causing a relay to disable or produce a diagnostic restart. In rare cases, an SEU can cause an undesired operation. This paper provides recommendations to reduce the risk of an SEU causing an undesired operation. Manufacturers and end users should continuously monitor quality and work toward improved overall system design, including the design of the microprocessor-based relays themselves.

VIII. Appendix: Fault Tree Analysis

Fig. 18 through Fig. 24 show fault trees used to calculate the data in the previous bar charts (Fig. 12, Fig. 13, Fig. 16, and Fig. 17). Not all of the fault trees are shown, but they are provided as an example of how the data was calculated.

The input data for the fault tree analysis in this appendix was derived from [13]. A few notable changes: the dependability for the relay mean time to repair was set to one day instead of five days. This is based on more relays having automatic diagnostic restart (thus, temporary failures take only seconds to restart) and due to increased reporting and regulatory requirements. Security relay failure information based on actual 2012–2016 field data were updated from [13], which stated an MTBUO for relays equal to 3,000 years (now 12,000 based on field data).

Also, it is likely that not all failures are reported. Therefore, we use data based on an estimation that 15 percent of undesired operations are not reported.

Fig. 18 shows the dependability fault tree for a single 87L/21 relay at each end with fiber-optic channels.

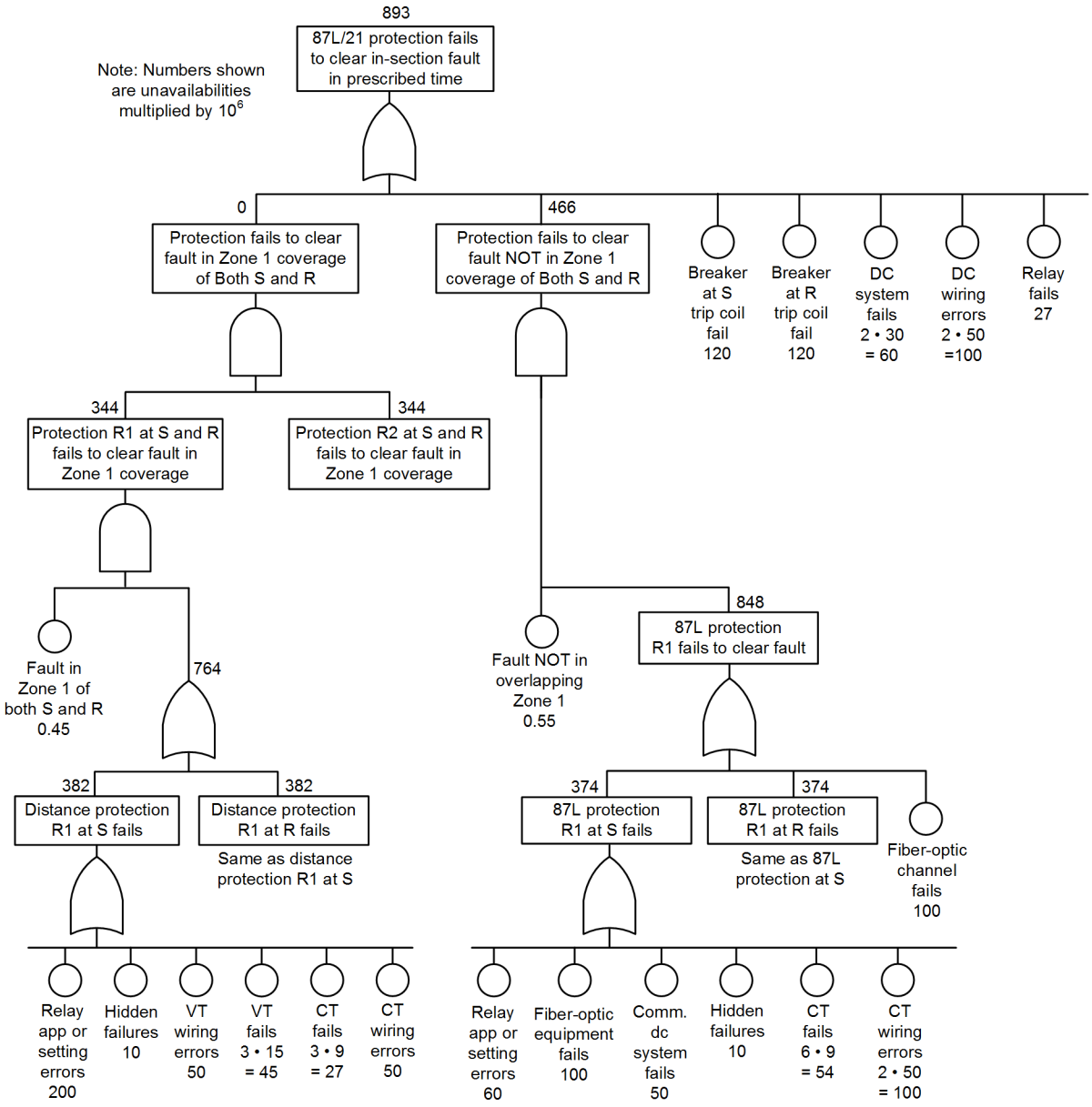

Fig. 18. Dependability fault tree (unavailability) for a single 87L/21 relay at each end with fiber-optic channels

Fig. 19 shows the dependability fault tree for dual redundant 87L/21 relays with fiber-optic channels.

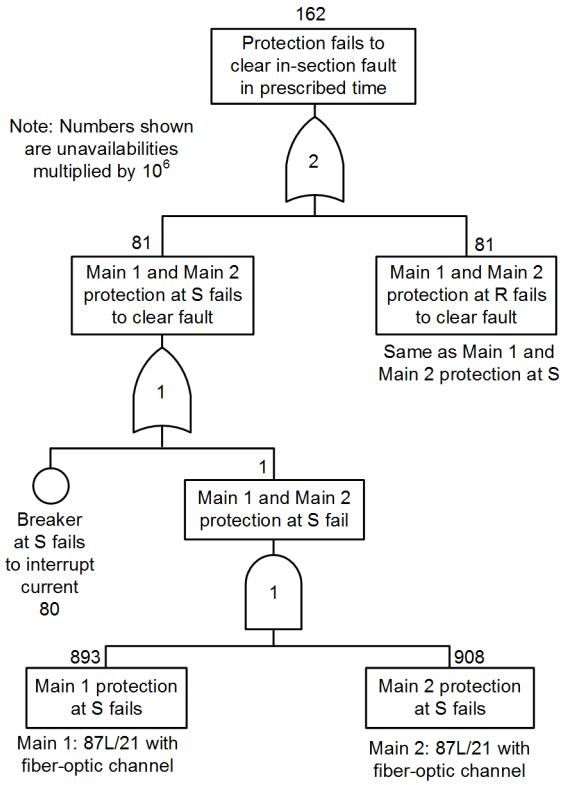

Fig. 19. Dependability fault tree (unavailability) for dual redundant 87L/21 relays with fiber-optic channels

Fig. 20 shows the security fault tree for a single 87L/21 relay with fiber-optic channels.

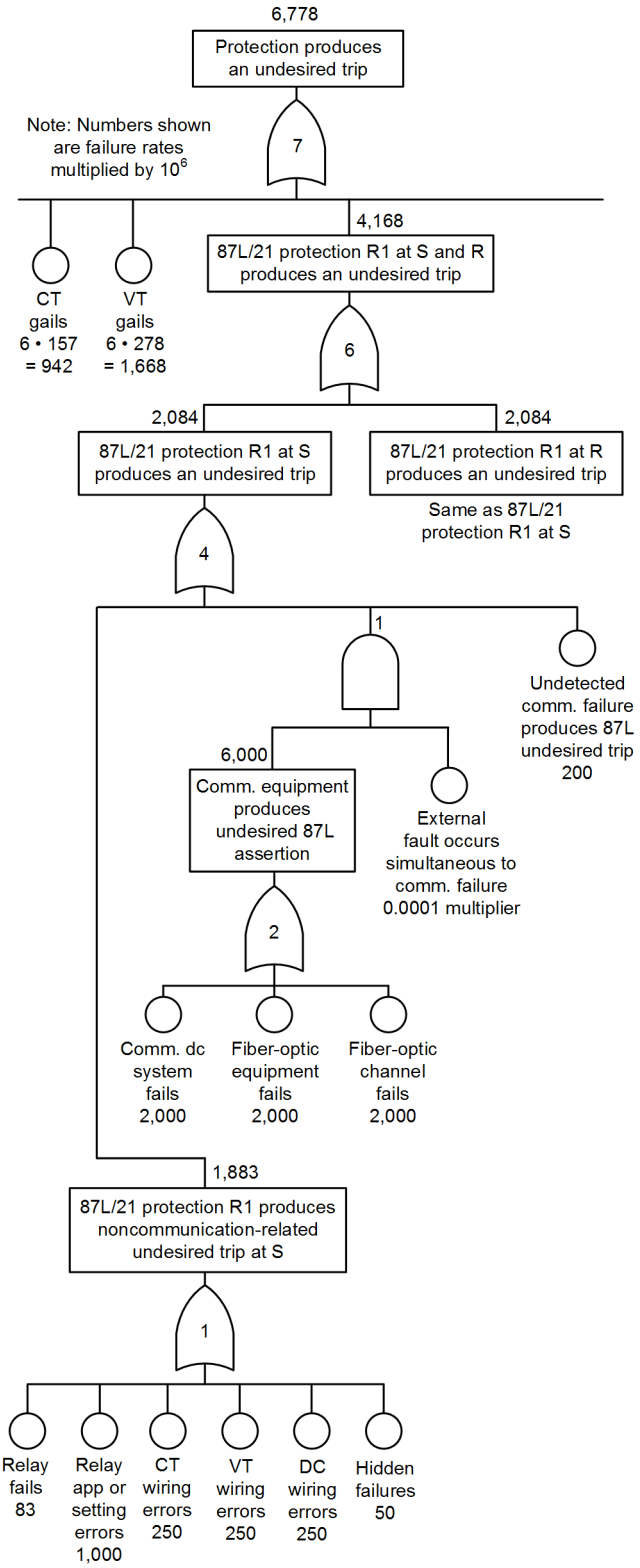

Fig. 20. Security fault tree for single 87L/21 relay with fiber-optic channels

Fig. 21 shows the security fault tree for an undesired operation of dual redundant 87L/21 relays with fiber-optic channels.

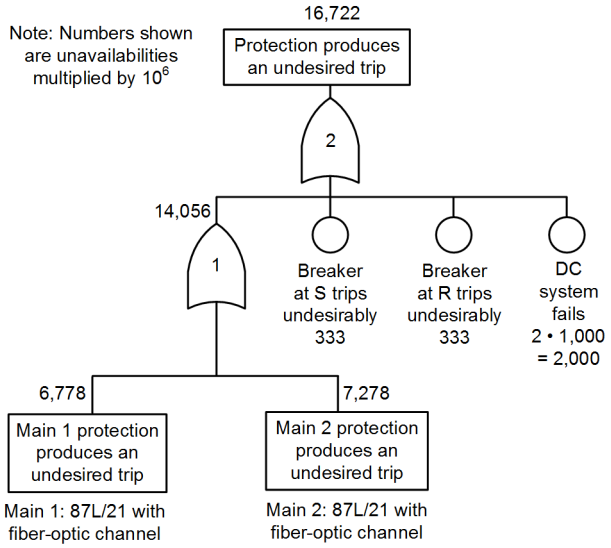

Fig. 21. Security fault tree for an undesired operation in dual redundant 87L/21 relays with fiber-optic channels

Fig. 22 shows the dependability fault tree for a single 50/51 relay on a distribution feeder.

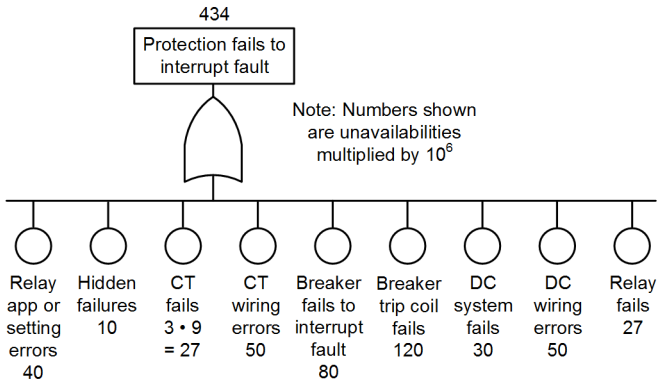

Fig. 22. Dependability fault tree (unavailability) for single 50/51 relay on a distribution feeder

Fig. 23 shows the dependability fault tree for dual 50/51 relays on a distribution feeder.

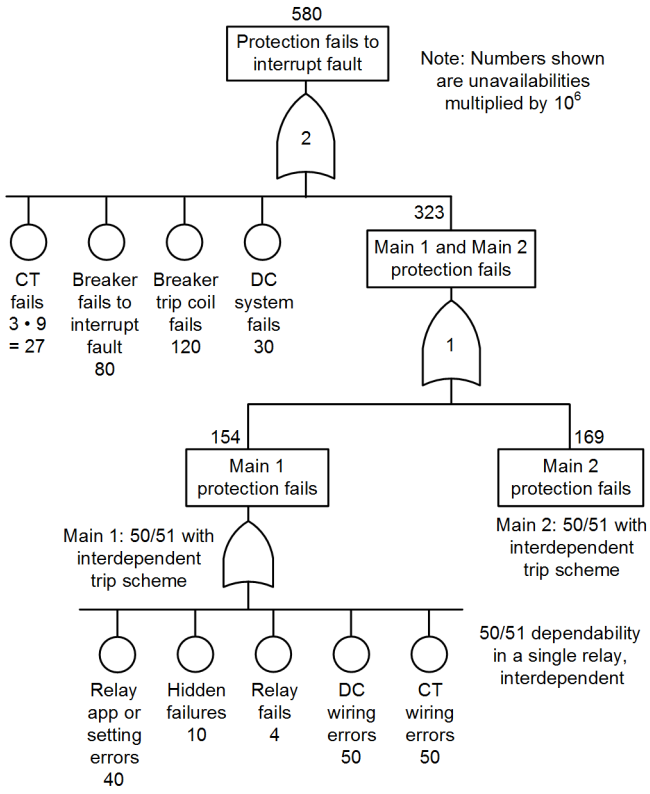

Fig. 23. Dependability fault tree (Unavailability) for dual 50/51 relays with interdependent tripping scheme

Fig. 24 shows the security fault tree for a single 50/51 relay on a distribution feeder.

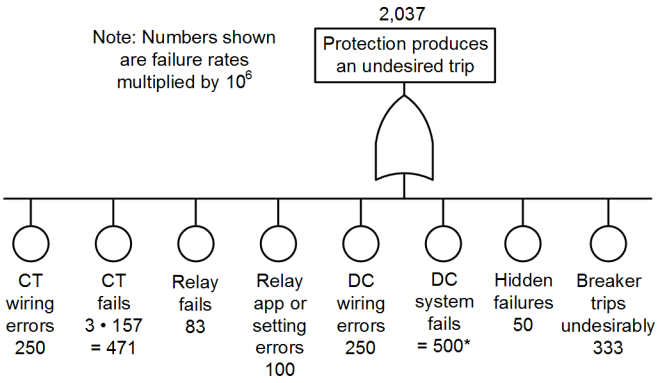

Fig. 24. Security fault tree (failure rate) for single 50/51 relay on a distribution feeder

Fig. 25 shows the security fault tree for dual 50/51 relays with an interdependent tripping scheme.

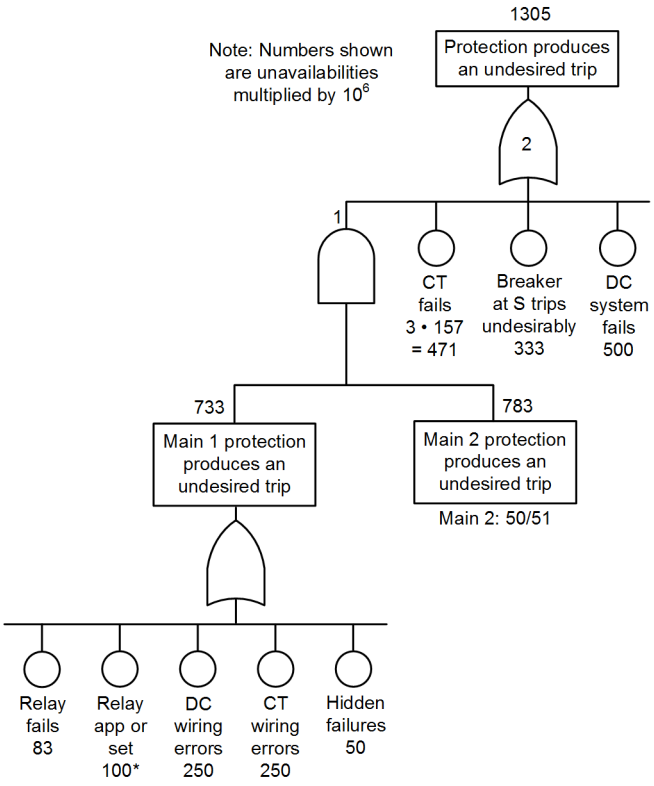

Fig. 25. Security fault tree (failure rate) for dual 50/51 relays with interdependent tripping scheme

IX. References

[1] D. Haas and K. Zimmerman, "Single Event Upsets in SEL Relays," March 2018. Available: https://selinc.com.

[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] 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.

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

[5] "Draft Single Event Effects Specification," Available: https://radhome.gsfc.nasa.gov/radhome/papers/seespec.htm.

[6] 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 IEE Radiation Effects Data Workshop, Seattle, WA, July 2005.

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

[8] O. Niemitalo, "Yamaha YMF262 audio IC decapsulated," Wikimedia Commons, May 2007. Digital image. Available: https://commons.wikimedia.org/wiki/File:Yamaha_YMF262_audio_IC_decapsulated.jpg.

[9] K. Zimmerman and D. Costello, "A Practical Approach to Line Current Differential Testing," proceedings of the 66th Annual Conference for Protective Relay Engineers, College Station, TX, April 2013.

[10] J. Harrell, "The Importance of ECC Memory in Your Substation Computer," July 2010. Available: https://selinc.com.

[11] K. Zimmerman and D. Costello, "How Disruptions in DC Power and Communications Circuits Can Affect Protection," proceedings of the 68th Annual Conference for Protective Relay Engineers, College Station, TX, March 2015.

[12] IEC 61508 International Standard, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

[13] R. Sandoval, C. A. Ventura Santana, H. J. Altuve Ferrer, R. A. Schwartz, D. A. Costello, D. A. Tziouvaras, and D. Sánchez Escobedo, "Using Fault Tree Analysis to Evaluate Protection Scheme Redundancy," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[14] H. J. Altuve Ferrer, K. Zimmerman, D. A. Tziouvaras, "Maximizing Line Protection Reliability, Speed, and Security," proceedings of the 69th Annual Conference for Protective Relay Engineers, College Station, TX, April 2016.

X. Biographies

Karl Zimmerman is a principal engineer with Schweitzer Engineering Laboratories, Inc. in Saint Louis. He is an active member of the IEEE Power System Relaying Committee and chairman of the Line Protection Subcommittee. Karl received his BSEE degree from the University of Illinois at Urbana-Champaign. He received the 2008 Walter A. Elmore Best Paper Award from the Georgia Tech Relay Conference and the best presentation award at the 2016 PowerTest Conference. He has authored over 40 technical papers and application guides on protective relaying.

Derrick Haas graduated from Texas A&M University with a BSEE. He worked as a distribution engineer for CenterPoint Energy in Houston, Texas, until 2006 when he joined Schweitzer Engineering Laboratories, Inc. Derrick has held several titles including field application engineer, senior application engineer, team lead, and his current role of regional technical manager. He is a senior member of the IEEE and involved in the IEEE Power System Relaying Committee.