ATTACHMENT I DEVELOPMENT OF PPPL ELECTRICAL SAFETY CRITERIA

PPPL isolation criteria originated as a design requirement for stored-energy systems having high voltage/energy. Later it was represented as a general requirement imposed when high voltage/energy systems were operating. Current isolation criteria requires redundant, independent barriers between the hazard of high voltage equipment or circuits and the worker. Redundant barriers may also be necessary to reduce the hazard of low voltage systems. The probability of operator error should be evaluated.

ENERGY-ISOLATION CRITERIA DEVELOPMENT

1959-1960

PPPL Drawing No. SK5020, dated December 28, 1959, entitled "Isolation Practices on High Energy Storage Systems" shows design features that were considered to be acceptable for both equipment protection and personnel safety. These design features were available in contemporary high voltage and high energy experimental apparatus. It is the earliest document in our files that has the PPPL criterion of separation of energy sources and workers:

> "**The purpose of this isolation (practice on high energy systems) is to prevent damage to building electrical system, control panels outside the <u>high energy areas</u> in the event of faults. Such equipment, as well as personnel will not be damaged or injured in the event of any <u>two possible simultaneous equipment faults</u>.**" (Underlining as shown on PPPL SK5020.)

It is clear that a third barrier is contemplated in this 1959 failure criterion. This multiple barrier concept is illustrated in FIGURE 1

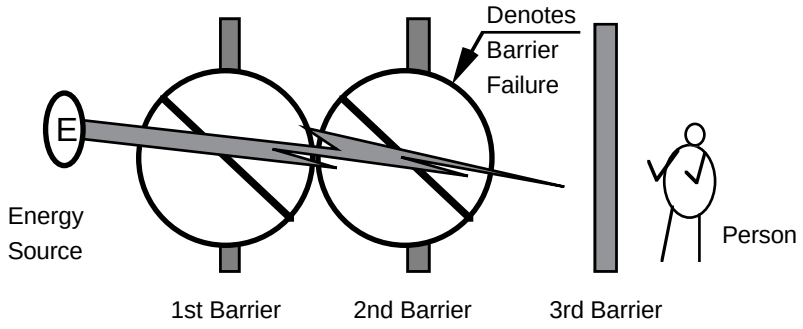


FIGURE 1

The earliest version of the PPPL Safety Manual in our files is a product of C-Stellarator Associates and it is dated April 11, 1960. This manual has a "General Requirements" section for Operating Conditions, which is different than that of the PPPL SK5020. The manual states:

> **"In general, two concurrent failures of components must occur before the equipment and personnel are endangered."**

This condition is satisfied if two barriers or energy isolation devices (EIDs) are provided between the energy source and the worker. When both barriers fail, the worker is endangered. This concept is illustrated diagrammatically in FIGURE 2.

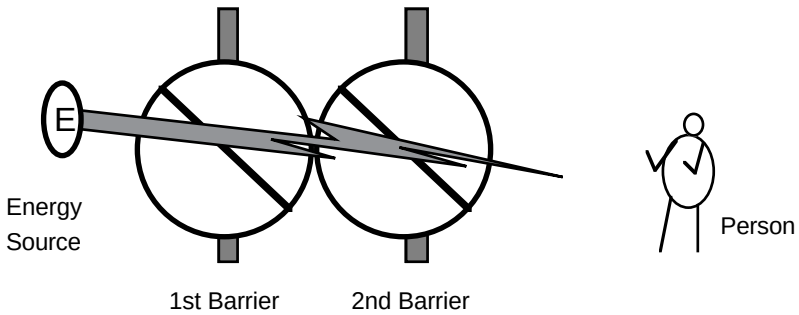


FIGURE 2

1975

The 1975 version of the Safety Manual restated the 1959 criterion. It was still in the form of an operating recommendation:

> **"When equipment is in operation, all parts accessible to personnel should be isolated from high voltage and high energy … such that two simultaneous (and independent) failures will not endanger the personnel involved. Failure of one isolating component should be improbable and independent of failures of other components."**

This condition can be satisfied only if three barriers or EIDs exist between the energy source and the worker which brings us back to FIGURE 1.

1982-83

The authors of the 1982/83 Revision 1 of Section 2.0, HSD 5008, the PPL Health and Safety Manual, reaffirmed the three-barrier rule (FIGURE 1) as a requirement when applied to Operating Conditions. It also provided two new ways to accept high voltage isolating devices.

A) Intervening components which have been manufactured as a standard product line and which have been type-tested … and installed …(per) generally accepted good engineering practices and (industry consensus standards).
B) PPPL products that have been individually tested and conform to (industry consensus standards).

1986

In 1986, the Department of Energy provided a quantified definition of the word "credible," i.e., having a probability equal to or less than $1x10^{-6}$ /year, to describe the likelihood of postulated failures. The term "simultaneous" was recognized to include conditions that lead to failures over time, such as position switches that have become loose or misaligned from vibration or lack of maintenance.

1988

Isolation criteria were improved in the 1988 Revision 2 of Section 2.0 through the introduction of barriers, barrier failure analysis techniques, including part of the IEEE single-failure criterion, and examples of acceptable barriers. For the first time, barrier philosophy included the DOE's limiting definition of "credible" events. Using this relatively new definition of credible, acceptance criteria for barriers became possible.

For all practical purposes, the terms "energized", "live", and "operating" represent the same hazards when referring to electric conductors. We presume, at any given time, some parts of the electrical systems at PPPL may be energized. Even if the offsite 138 kV and 26 kV power systems were shut down and isolated, we must consider the on-site generators, UPS's, and stored energy systems as potential sources of energy. We conclude that any workable isolation criteria must consider those circumstances during the facility or project's life-cycle under which workers approach potentially live electrical components. The high voltage criteria are:

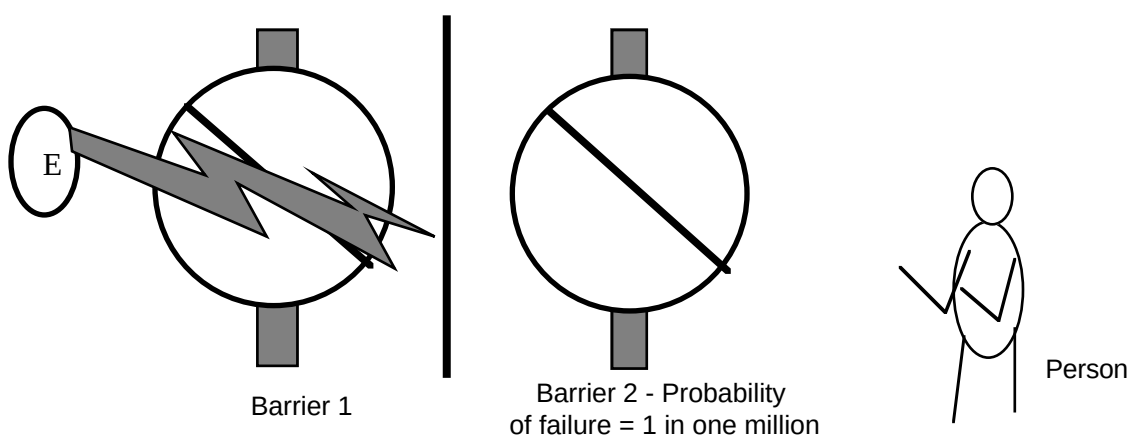
> **"2.5.4.1 Energized parts of high-voltage (above 600 V ac or dc) equipment and circuits shall be isolated from surfaces exposed to personnel by two acceptable, independent energy barriers, one of which shall be designed to survive any credible (i.e. having a probability $\geq 1 \times 10^{-6}$/yr) failure mode. Two acceptable, independent energy barriers are required between all ungrounded conducting parts that extend from high-voltage/energy sources or enclosures to areas or devices that are accessible to personnel. A safety barrier may be used in lieu of one of the above energy barriers."**

The criterion for circuits operated at 600 volts or below is:

> **"2.5.4.3 Energized parts of low-voltage (600 V ac or dc or below) equipment and circuits shall be isolated from surfaces exposed to personnel by at least one acceptable, independent energy barrier."**

Illustrated as follows:

No Common-mode Failure between Barriers



EQUIPMENT FAILURE AND HUMAN ERROR

There are two categories of equipment failures. Time dependent failures are in the first category. They are quantified as failure rates, e.g., one in two hundred per month or 5×10^{-3}/month.

Demand failures are the second category of equipment failures. They are stated as unitless probabilities, e.g., one in twenty-five hundred or 4×10^{-4}. Demand failures are most often used to quantify the failure of components that are required to change state. Components that are arranged in series form an "and" logic gate. The demand failures are multiplied to determine the demand failure of the set. For example, UL listed, molded-case circuit breakers are used as energy isolation devices when they are placed between an energy source and a worker. Representative samples of circuit breakers must survive 2500 test-operations under UL test procedures without failure. The probability of a demand failure of two such breakers connected in series, presuming no common-mode failures, is $(4 \times 10^{-4}) \times (4 \times 10^{-4}) = 1.6 \times 10^{-7}$.

A safety-tagged hard ground may be placed on the ungrounded circuit-conductors in lieu of LO/TO on the second circuit breaker. The demand failure for fixed grounding-switches is the same as that of circuit breakers. However, the demand failure for currently-tested portable grounding-sticks is considered to be on the order of 2×10^{-4}.

The probability of equipment demand failure should be evaluated in conjunction with the probability of human error. Human error is quantified as the probability that an authorized person fails to correctly perform a task such as restoring a system to the correct configuration after maintenance or testing.

In a probabilistic risk assessment (PRA), the probability of human error while performing a task on electrical equipment typically is conservatively assumed to be about 0.03 per task. This value may be reduced if any of the following recovery factors apply:

a. Errors can be assessed as recoverable by a factor of 0.01 by a compelling signal or activity such as the use of LO/TO or completion of accessing procedure before access to equipment is permitted.
b. Errors are recovered by a factor of 0.1 by post-activity tests if the tests are performed correctly. Examples include testing for "0" volts in a LO/TO procedure or the observation of currently calibrated instruments or meters.
c. If a second qualified person, or safety watch, is required to directly verify component status after completion of the activity by the original performer, then a recovery factor of 0.1 applies. No recovery credit is given for either activity unless a written check-off list is used during the activity.
d. If a shift or daily check of component status is required using a written check-off list, then a recovery factor of 0.1 applies to the probability of human error.

If the all these recovery factors are applied to a task, then the risk of human error is reduced to a probability of $(0.03) \times (0.01) \times (0.1) \times (0.1) \times (0.1)$ which is on the order of 3×10^{-7}.

When the probability of human error is considered along with that of demand failure, they form an "or" logic gate which is additive. It is evaluated as $(3 \times 10^{-7}) + (1.6 \times 10^{-7}) = (4.6 \times 10^{-7})$. If an activity requiring protection by these series-connected breakers were to happen twice each year, then the probability of failure would be evaluated

as 2/yr x 4.6 x 10^{-7} = 9.2 x 10^{-7}/yr. If the product of the number of annual occurrances of the activity and the sum of equipment demand failure and operator error exceed 1 x 10^{-6}/yr, then additional energy isolation devices should be used in the activity to lower the probability of failure.

VISIBLE BREAKS

The National Electrical Safety Code recognizes that circuit breakers in 5 kV or 15 kV metal-clad switchgear constitute a visible break when placed in the withdrawn position.

It is PPPL practice to consider that the grounded metal shutters of drawout type metal-clad switchgear circuit breakers constitute two breaks or two energy isolation devices (EIDs) for the purposes of a failure analysis. If the shutters are of non-conducting material, then the likelihood of common-mode failures, such as arc-over may also need to be considered.

REFERENCES FOR ATTACHMENT I:

DOE STD 1030-92 "Guide to Good Practices for Lockouts and Tagouts"
PPPL Dwg. SK-5020 "Isolation Practices on High Energy Storage Systems"
ESH-001 "Safety, Accident Prevention, and Equipment Protection Tags"
ESH-016 "Control of Hazardous Energy Sources via Lockout/Tagout of Energy Isolation Devices"

— Blank filler page —