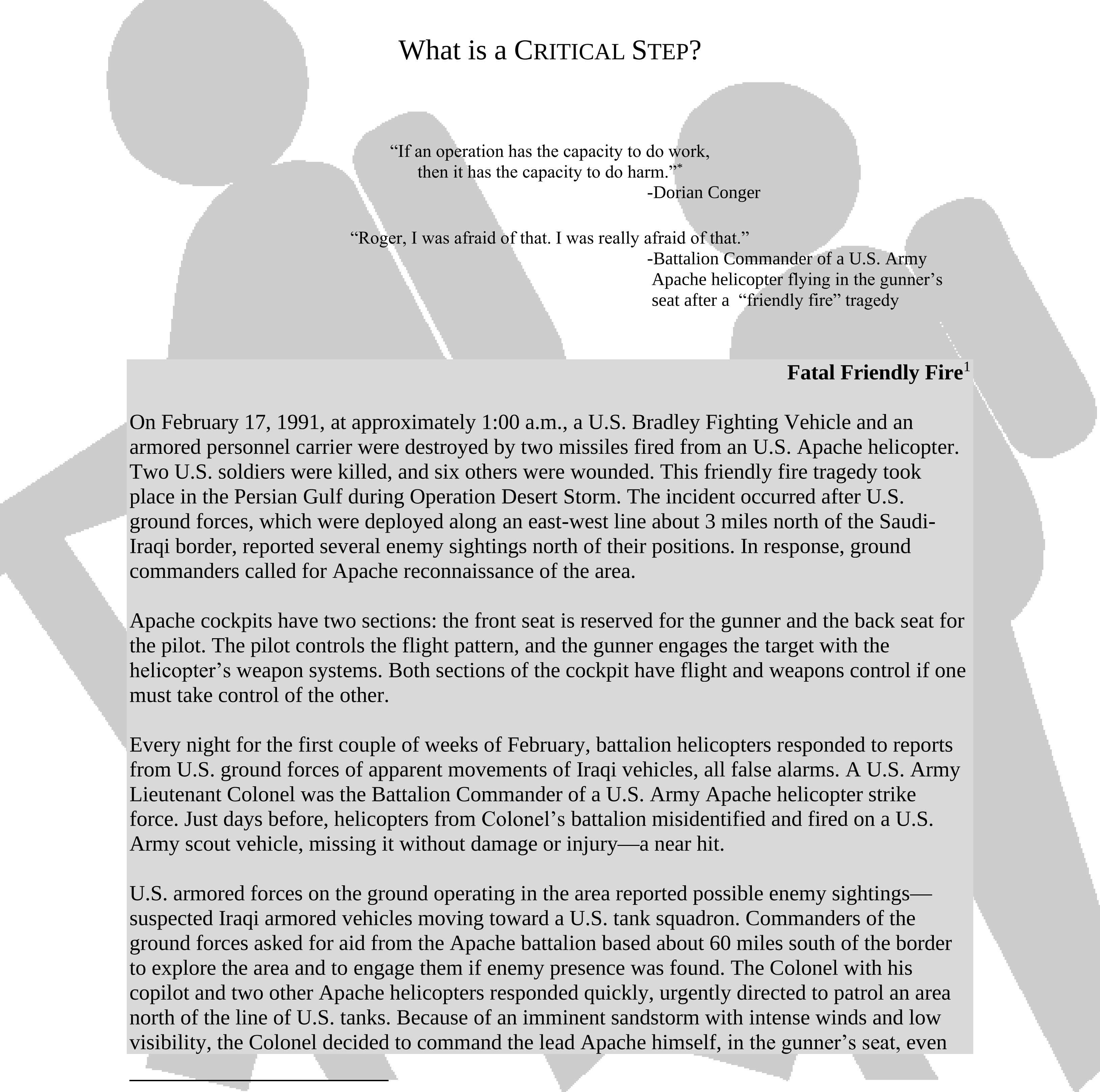
Complementary chapter from the book *Critical Steps: Managing What Must Go Right in High-Risk Operations*



Chapter 1

What is a Critical Step?

“If an operation has the capacity to do work,
then it has the capacity to do harm.”[*]
-Dorian Conger

“Roger, I was afraid of that. I was really afraid of that.”
-Battalion Commander of a U.S. Army
Apache helicopter flying in the gunner’s
seat after a “friendly fire” tragedy

Fatal Friendly Fire[1]

On February 17, 1991, at approximately 1:00 a.m., a U.S. Bradley Fighting Vehicle and an armored personnel carrier were destroyed by two missiles fired from an U.S. Apache helicopter. Two U.S. soldiers were killed, and six others were wounded. This friendly fire tragedy took place in the Persian Gulf during Operation Desert Storm. The incident occurred after U.S. ground forces, which were deployed along an east-west line about 3 miles north of the Saudi-Iraqi border, reported several enemy sightings north of their positions. In response, ground commanders called for Apache reconnaissance of the area.

Apache cockpits have two sections: the front seat is reserved for the gunner and the back seat for the pilot. The pilot controls the flight pattern, and the gunner engages the target with the helicopter’s weapon systems. Both sections of the cockpit have flight and weapons control if one must take control of the other.

Every night for the first couple of weeks of February, battalion helicopters responded to reports from U.S. ground forces of apparent movements of Iraqi vehicles, all false alarms. A U.S. Army Lieutenant Colonel was the Battalion Commander of a U.S. Army Apache helicopter strike force. Just days before, helicopters from Colonel’s battalion misidentified and fired on a U.S. Army scout vehicle, missing it without damage or injury—a near hit.

U.S. armored forces on the ground operating in the area reported possible enemy sightings—suspected Iraqi armored vehicles moving toward a U.S. tank squadron. Commanders of the ground forces asked for aid from the Apache battalion based about 60 miles south of the border to explore the area and to engage them if enemy presence was found. The Colonel with his copilot and two other Apache helicopters responded quickly, urgently directed to patrol an area north of the line of U.S. tanks. Because of an imminent sandstorm with intense winds and low visibility, the Colonel decided to command the lead Apache himself, in the gunner’s seat, even

[*] This statement is attributed to Dorian Conger, who made this statement to students during the introduction to a MORT cause analysis class. (MORT: Management Oversight Risk Tree).

though he had only 3 hours sleep in the previous 24 hours. They launched at 12:22 a.m. Due to the urgency of the request, a normal, detailed pre-mission briefing was not done.

Upon arriving on station at 12:50 a.m., the helicopter's target acquisition system detected the vehicles. Two suspicious vehicles appeared near the eastern end of the line of U.S. ground forces, noting the targets' locations by measuring their distance from the aircraft with a laser beam, automatically entered into the weapons fire control computer. The Colonel estimated the suspicious vehicles were about a quarter mile in front, the first mistake. He misread the grid coordinates of the alleged targets on the helicopter navigation system, reading instead the search coordinates that he manually entered into the navigation system while in route early in the flight. As a result, he misidentified the target vehicles' location as being north of the line of friendly vehicles, which coincidently were in the exact location of previously reported enemy sightings.

A discussion ensued between the three Apache pilots and the ground commander to authenticate their identity. Apache helicopters were not equipped with IFF—an automated system referred to as "Identification Friend or Foe." In the darkness, the vehicles could not otherwise be identified.

The ground commander insisted that no U.S. forces were ahead of the line, that the vehicles must be enemy, and twice replied to the Colonel, "Those are enemy. Go ahead and take them out." Pilots of the other two Apaches also thought the vehicles were enemy. More ominously, there were persistent search-radar alerts being received in the cockpit, adding to the stress of the moment. These alerts, responding to radar emitted by friendly forces, were misidentified by the Apache computers as an enemy system. Even the Colonel's copilot prompted him, "Do em!" more than once. Yet he felt uneasy as to the identity of the vehicles. the Colonel is recorded to have said, "Boy, I'm going to tell you, it's hard to pull this trigger," asking for help to verify current helicopter heading and bearing to and grid coordinates of targets. He states the targets' grid coordinates aloud, again misreading them, the second mistake. No one recognizes the error. His copilot states, "Ready in the back."

The Colonel decided to fire on the vehicles with the Apache's 30-millimeter cannons (machine guns), which would have inflicted less damage than a missile just in case they were friendlies. The gun emitted only a few rounds before jamming (sand). He then fired two Hellfire missiles[*] at the suspected vehicles—the third, but deadly, mistake. Shortly thereafter, the Apaches received a cease fire order. The missiles had already been fired and both vehicles, a Bradley Fighting Vehicle and an armored personnel carrier, were destroyed, killing two U.S. soldiers inside. The Colonel softly said, "I was afraid of that, I was really afraid of that."

The Colonel knew the point of no return: pulling the trigger! He said it. But human fallibility entered the decision-making process, hampered by sleep deprivation, a fierce desert dust storm, inadequate human factors in the cockpit, inferior teamwork, and the stress of combat that worked against him, his team, and even ground commanders. *He did his best* under the circumstances. Would you have done anything different? Be honest. The system and the battlefield worked against him. Sometimes doing your best isn't good enough.

[*] The laser-guided Hellfire missile is the main armament on the Apache helicopter, designed for the destruction of armor and other hardened targets.

Work = Risk

When you do work something changes.[*] Physical work is the application of force over a distance ($W = f \bullet d$). Work is necessary to create value. Except where automation is used, work requires people to touch things—to handle, manipulate, record, or alter things. Jobs and tasks comprise a series of human actions designed to change the state of material or information to create outputs—assets that have value in the marketplace. The risk of harm to those assets emerges when people do work, without which nothing of value is created. *Work is energy directed by human beings to create value*.[2]

Because the use of force (f) requires energy from a built-in hazard to create the d in work, all work involves some level of risk. Occasionally, people lose control of these hazards. Human fallibility is an inherent characteristic of the human condition—it's in our genes. Error is normal—a fact of life, a natural part of being human. The human tendency to err is not a problem until it occurs in sync with significant transfers of energy, movements of matter, or transmissions of information.[3] In an operational environment, human error is better characterized as a *loss of control*—a human action that triggers an unintended and unwanted transfer of energy (ΔE), movement of matter (ΔM), or transmission of information (ΔI).[4] Human performance (**Hu**) is the greatest source of variation in any operation, and the uncertainty in human performance can never be eliminated. If work is not performed under control, the change (d) may not be what you want; work can inflict harm. *Work involves the use of force under the condition of uncertainty*.[5]

When performing work, people usually concentrate on accomplishing their immediate production goal, not necessarily on safety.[6] Most of the time, people's attention is on the work. If people cannot fully concentrate on being safe, thoroughly convinced there will be no unintended consequences 100 percent of the time, then *when* should they fully focus on safe outcomes?

Value Added vs. Value Extracted

Recall Dorian Conger's quote at the beginning of this chapter, "If an operation has the capacity to do work, it has the capacity to do harm." All human-directed work intends to accomplish something that meets customer requirements, to add value. However, when people manipulate the controls of built-in hazards, there is a corresponding risk to do harm that can extract value instead of adding value. The greater amount of energy transferred, matter transported, or sensitive information transmitted during a human action, the greater the potential harm. Those human actions or procedure steps that can trigger serious harm must go right the first time every time. If the severity of harm potentially suffered by an asset would be considered *intolerable*, that action would be considered a Critical Step. An event/incident/accident is a form of value extraction.[7]

Referring to Figure 1.1 below, work may involve interactions with several assets, in this case two. At least two assets are in play for every work activity: typically, the person doing the work from a personal safety perspective and the product of their work from a business perspective. Figure 1.1 illustrates that steps 8 and 12 involve interactions with asset one (1), and steps 4 and

[*] Work is the application of physical strength or mental effort to achieve a desired result, whether a force over a distance or careful reasoning (still a force over distance, though at a microscopic level).

17 require interactions with asset two (2). If the performer loses control of the work at step 4, while doing work on asset two, the amount of work done at that step would not trigger enough harm to the asset to exceed the degree of harm deemed intolerable, albeit some harm ensues. However, if the performer loses control at step 17, again working with asset two, it is possible for asset two to suffer sufficient harm that would exceed a level of severity that managers previously deemed intolerable. The same logic applies to work on asset one. Consider the following points to better understand the illustration:

- The horizontal line (x-axis) represents steps (denoted by dots) in a work activity, whether directed by a procedure or skill-of-the-craft.
- The vertical axis (y-axis) represents value added (above the horizontal line) or value extracted (below the horizontal line).
- The length of vertical lines denotes the degree of value (work done), either added or extracted.
- Intolerable harm is denoted by horizontal dashed lines for each asset.
- Some steps/actions involve one or more assets, or none.

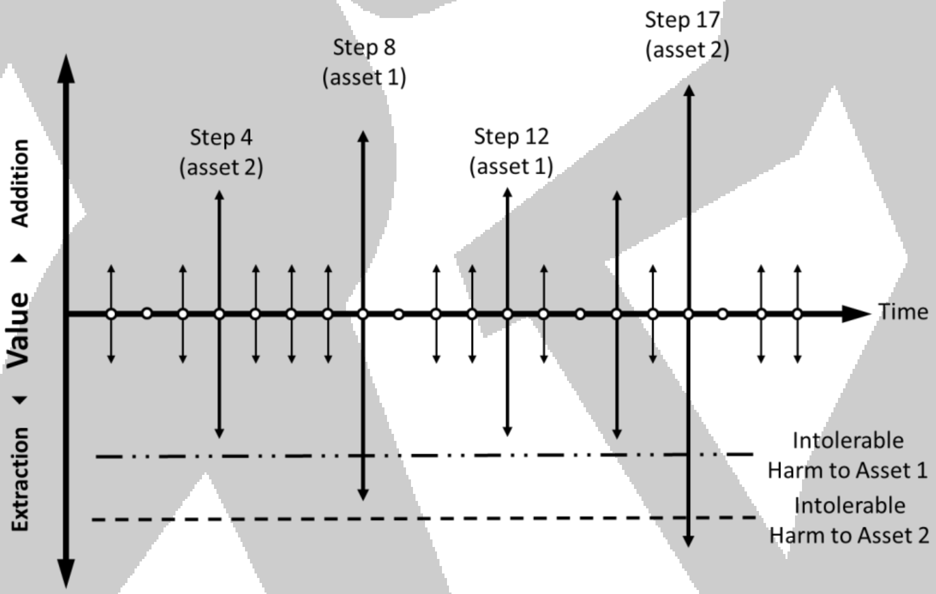


Figure 1-1 Value added vs. value extracted (harm) during work. If an operation has the capacity to do work, it has the capacity to do harm.

The degree of intolerable harm to a particular asset should be understood before work (usually a management decision) to designate a particular step as a Critical Step.

> **Note**: Not every action that has a point of no return is a Critical Step. Just because an action cannot be undone does not, by itself, constitute a Critical Step. The designation of an action as a Critical Step depends primarily on the *degree of harm* experienced after a loss of control of that specific action, what managers consider *intolerable*.

On that fateful night, the Colonel was uncertain as to the identity of the two vehicles thought to be enemy. He initially attempted to engage the vehicles with the Apache's machine guns, which would have inflicted less damage than a missile, less likely killing anyone inside. Less energy, less harm. But those guns jammed.

Critical Step Defined

DuPont de Nemours, Inc., commonly known as DuPont, defines *operational discipline* (or OD) as, "…the deeply rooted dedication and commitment by every member of an organization to carry out each task the right way every time. Do *it* right the first time, every time."[8] But, *it* can be almost anything—*it* must be more specifically defined. We call *it* a Critical Step. Does every human action have to be performed perfectly? Let's conduct a simple thought experiment.

Thirty-year-old Jill arrives for work well rested after a good night's sleep. She's conscientious, enjoys good health, and has strong family support. Personal problems do not weigh her down. In short, Jill is well-trained, mentally alert, and physically fit and faces minimal emotional distractions—an ideal worker. For illustration purposes, let's assume that Jill is 99 percent reliable[*] for the task she is given when she arrives at work.[9]

Jill's supervisor assigns her a task that consists of exactly 100 actions. Let's assume the working conditions for every action are the same throughout the job—the chance for success is the same for step 100 as it is for step 1. Here's the question. What is the likelihood that Jill will perform *all* 100 actions without error?

Jill's performance is a simple probability calculation. The chance for success on step 1 is 0.99; the chance for success in step 2 is the same, 0.99; and the chance for success on step 3 is—you guessed it—0.99, and so on to the 100th action. The mathematical equation for the probability of successfully completing *all 100 actions without losing control* is:

$$p100 = 0.99 \times 0.99 \times 0.99 \cdots 0.99^{100} \cong 0.3660\ or\ \approx \mathbf{37}\%$$

It may astound you that the chance of performing just 100 actions without error is only 37 percent for someone who is 99 percent reliable.[10] There's a much better than 50-50 chance that Jill will do something wrong along the way (63 percent). The news is better if a person's reliability is near the top of the nominal human reliability scale—99.9 percent; but even then, the probability of successfully completing all 100 actions without losing control improves to just 90 percent. That still equates to a 1 in 10 chance of erring at some point in the 100-step task. A mistake at some steps may not matter. For most work, 99 percent reliability is acceptable. The question to ask is, "Which action absolutely has to go right the first time, every time?" These are the points in the task at hand, which Jill and her boss should identify for her to successfully complete the task without experiencing serious injury, loss, or damage.[11] So, let's restate our definition:

[*] Reliability is the likelihood of successful performance of a function.

**A CRITICAL STEP is a human action
that will trigger immediate, irreversible, and intolerable harm to an asset,
if that action or a preceding action is performed improperly**.[12]

Battlefields are complex adaptive systems that breed ambiguity, uncertainty, and volatility—otherwise known as a VUCA environment.[13] Misreading the grid coordinates to the alleged targets, misunderstanding friendly forces to be enemy, compelled by ominous radar alerts, his fellow pilots, and the ground commander, the Colonel let loose two missiles—the CRITICAL STEP. Once launched, the missiles were beyond control—they would follow the physics of their design and the environment, eventually fulfilling their deadly purpose. The Colonel and his copilot experienced VUCA and got things wrong, albeit unintentionally.

Maintenance Test Gone Wrong[14]

An operating furnace was inadvertently shut down during preventive maintenance on a safety-related instrument.

Each of two boilers was fitted with a temperature recorder-controller and a respective high-temperature trip function. The two recorders were positioned side by side on the front of the control room instrument panel, with A recorder on the left and B recorder on the right as shown in the following illustration.

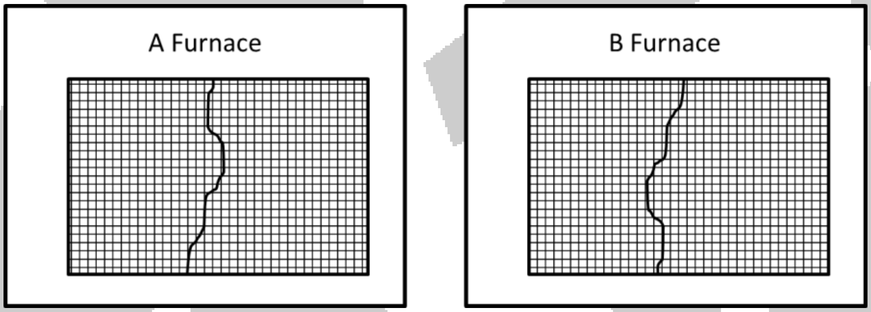


Figure 1-2 The view of the two strip chart recorders on the control panel, as seen when standing in the control room. Each recorder also functioned as a controller for its respective furnace.

An instrument technician was directed to check the calibration of the high-temperature trip feature on A furnace (a combined recorder-controller). The technician placed the controller in manual* and then walked behind the control panel to access the rear of the recorder-controllers. The next several steps of the procedure were to 1) remove the cover from a junction box, 2) disconnect (lift) the signal lead (electrical wire from detector) from the furnace temperature detector, 3) connect a test box to the controller, 4) apply a gradually increasing temperature signal from the test box, and 5) note the reading on the recorder at which the trip would occur.

* Placing the recorder/controller in manual bypasses the trip feature from the controller such that the temperature signal for furnace A is locked at the current temperature, and the furnace's fuel-supply valve position stops being driven by the controller.

Behind the control panel the junction boxes for A and B are in line with the recorders (front to back). Therefore, when viewed from behind the control panel, looking toward the control room proper, the B recorder-controller junction box is on the left as shown in Figure 1.3 below.

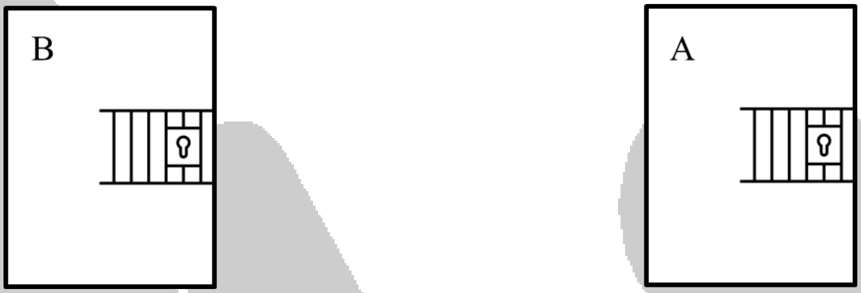


Figure 1-3 The view of the junction boxes from behind the control panel. The instrument technician was required to unlock the junction box to access the signal wire to the recorder-controller. No labels were on the rear faces of the junction boxes—the letters B and A are noted to let the reader know that from the perspective of the technician from behind the control panel, the B junction box is on the left and the A junction box is on the technician's right.

There was a label for each recorder-controller in the rear access area; but it was near the floor, not on the junction boxes, and the font was small. This was not necessarily a major factor in this incident because this technician had done this task several times before. Better labeling could have caught the attention of the technician before the fateful action. Remember, the A recorder/controller is in manual; the B recorder/controller is still active.

The technician removes the cover from the B junction box and disconnects the signal lead. Bang! The B furnace trips, shutting down. The A furnace is still operating. The effect of disconnecting the signal lead is the same as a failed temperature detector, which correlates to a maximum high temperature. The controller signals the fuel supply valve to close, and the furnace shuts down.

We hope you recognized the CRITICAL STEP—lifting the lead from the B furnace. Question: The harm is an interruption of services provided by the B furnace. Does disconnecting the lead satisfy the definition of a CRITICAL STEP? The asset is the furnace and the service it provides, and the hazard is an interruption of fuel.

- Will the human action result in a change in state of the furnace? Yes – shut it down by closing the fuel supply valve.
- Is the change in state immediate? Yes – mere moments, faster than humans can respond to avoid the consequence.
- Is the change in state irreversible? Yes – the furnace shuts down, terminating services for a period of time.
- Is the change in state harmful and intolerable? Presumably, yes. If the furnace was supplying vital services, it may involve serious losses or damage to customers or other assets. (Management must decide what level of harm is considered intolerable.)

Would lifting the signal wire to A furnace recorder-controller be considered a CRITICAL STEP, even if the channel is in manual? Yes! Both actions to lift the signal lead are critical to the operation of their respective furnaces. The A furnace would not trip because its respective recorder/controller was in manual, while the B furnace controller was still active ("in control"). At the conclusion of chapter 5, we reveal that CRITICAL STEPS are *always* considered critical. Chapter 4 will do a deep dive on *Risk-Important Actions* (RIAs). Placing the controller in manual was an RIA for the CRITICAL STEP of disconnecting the signal lead, allowing the recorder-controller to respond to a simulated signal without triggering an inadvertent protective control action.

Would you recognize a CRITICAL STEP if you saw one? What criteria would you use to conclude a procedure step or other human action is a CRITICAL STEP? To help you accurately identify a CRITICAL STEP, it is necessary to know its attributes, which are embedded in the definition.

Attributes of a CRITICAL STEP

Notice that the central idea in the definition of a CRITICAL STEP is the degree of *harm* to something of importance—an asset. An asset is anything of substantial or inherent value to an organization, such as people, property, product, and even productivity. Other factors are important to what actions would be considered CRITICAL STEPS. But without "intolerable harm," a human action that satisfies all other attributes would not be a CRITICAL STEP. A CRITICAL STEP's attributes, which are described in Table 1.1 below, are derived from Dr. David Embry's work in human reliability analysis (HRA). His research provides insight into the development of these attributes.[15]

A methodology for identifying a critical task was first developed by Dr. Embrey in a 1994 book he wrote for the American Institute of Chemical Engineers, *Guidelines for Preventing Human Error in Process Safety*. Dr. Embrey developed a framework for evaluating human sources of risk in an operating plant known as System for Predictive Error Analysis and Reduction (SPEAR). The SPEAR methodology focused on tasks with significant risk potential, identifying human errors. We borrow and expand on the concept of a critical task by focusing not on errors but on harm to assets. Although the term CRITICAL STEP was borrowed from the DOE, the principles and practices of CRITICAL STEPS introduced in this book springboard off the SPEAR logic, which was to identify the human interactions with a system that would have adverse impact on risk if errors occured. The screening process of the SPEAR methodology asked the following questions:

1. Is a hazard present in the area of the operation? (potential to cause harm – severity)
2. Given that a hazard is present, could any human interactions cause harm? (hands-on manipulations by people who could trigger release of the hazard)
3. Given that workers interact with hazardous systems, how frequently would they err in this critical task? (likelihood of error; i.e., losing control of the hazard)

Answers to the above questions are used to rank the risk potential of various work activities for a more detailed HRA, which is not within the scope of this book. In 1997, Dr. James Reason made a practical observation about this process in his book *Managing the Risks of Organizational Accidents*. He mentioned that non-specialists in HRA, such as procedure writers, quality inspectors, and managers, should pay less attention to human error and more on the *consequences* of it to the system and its products.[16] We agree. CRITICAL STEP MAPPING, which is described in Chapter 7, provides a similar analytical method for systematically identifying perpetual Critical Steps in operational processes and procedures. This is our focus.

Table 1-1 Attributes of Critical Steps. The goal is to help identify human actions or activities that pose the greatest risk to an organization's assets during production operations. Consequently, definitions of words used to define a Critical Step are important to understand.

Attribute	Description	Common Examples
Human	Hands-on performance by front-line workers; persons in direct contact with assets or control of related hazards during operations	• operator / electrician / craftsman • nurse / surgeon • pilot • information technology (IT) tech Not: equipment, knowledge-worker
Action	Physical activity by people that involves hands-on exertion of a force on an object (act of commission)	• push / pull / lift / turn / flip • handle / tap / punch • walk / run / kick / nudge • depress (enter) Not: think, decide, speak
Will	• Certainty; complete assurance that energy will be transferred, matter will move from one place to another, or information will be transmitted • Assurance of the onset of harm to an asset	• unavoidable burn after touching hot stove • inescapable after stepping into a bear trap • irrevocable after pulling a fire alarm Not: maybe, likely, could
Immediate	Faster than a human can react or respond to avoid consequences	• instantly (explosion / spark) • split second (spill / crack) • moments (loss of cooling flow) • seconds to minutes (overheating) Not: delays, hours, days, weeks
Irreversible	• One or more critical parameters of an asset are exceeded, resulting in permanent change • Past the point of no return • No undo—the onset of harm is inevitable • Inability to reestablish conditions prior to action	• brain damage (and intolerable) • burned toast (not intolerable) • un-ringing a bell • returning bullet to a firearm's chamber after shooting it Not: irrecoverable (equipment damage is recoverable at a cost; human life is not)
Intolerable Harm	• Disabling injury or death • Significant damage, or substantial loss • Defined for every asset • Severity of harm meets organization's definition of an event; reportable to a regulator • Severity defined by what regulatory agencies consider unacceptable	• Death / permanent disability • severed limb • damage/cost exceeding $50,000 • unacceptable quality to a customer • loss of mission functionality • loss of market share / out of business

Attribute	Description	Common Examples
	• Dependent on what the managers consider important to safety, quality, the environment, production, etc.	Not: paper cut, embarrassment, minor water spill, $50 cost

> **Caution**: On the surface, the concept of Critical Step appears to be simple and straightforward. The mistake made most often is that too many actions or steps are labelled *critical*. People tend to conflate RIAs with Critical Steps, which strongly suggests they haven't internalized the attributes of a genuine Critical Step. As the old saying goes, "If everything is important, then nothing is important."

To be useful in managing human performance risk, the concept of a Critical Step must be reserved for 1) what is vital to the life and health of workers and the public, 2) the essential functioning of safety-critical plant equipment, 3) the quality of goods and services delivered to customers, and ultimately, 4) the economic survival of the organization. Front-line workers, procedure writers, supervisors, and others who do hands-on work must discipline their use of Critical Steps in operations.

The following list offers a few everyday examples of human actions that satisfy the definition and criteria of a Critical Step. You might be surprised by a few.

- depressing the 'Trip' pushbutton on a circuit breaker's physical control panel that supplies electric power to a hospital
- walking through the opening into a confined space (possible oxygen-deficient atmosphere)
- making an incision on a patient during surgery
- turning on the kitchen sink garbage disposal unit
- pulling a fuse or an integrated circuit (IC) card from a digital control system
- grasping a bare electrical cable or wire
- clicking "Send," "Submit," "Start," or depressing the "Enter" key
- loosening bolts on a pipe flange or manway cover on a high-pressure system
- touching the shaft of an operating pump (rotating at 1800 rpm) with your hand
- extracting a tooth
- leaping across the open door of an airborne aircraft while skydiving
- depressing the accelerator of your automobile
- walking across a street

In every example, there is a human action (verbs ending with 'ing'), and a transfer (or interruption) of energy (electrical, mechanical, heat, etc.), a movement of matter (solid, liquid or gas), or a transmission of information (data, information, software, signals, authorizations, etc.) that could trigger immediate, irreversible, intolerable harm to something important.

Technical Expertise – the Bedrock of Critical Steps and Risk-Based Thinking

When an asset suffers serious harm, the boundaries of what is safe for the asset were exceeded. If front-line workers are to protect assets from harm during everyday work, they must possess the prerequisite technical knowledge and understanding of the safety boundaries for all the assets they work with on the job. To exercise Risk-Based Thinking, the presumption is that the person understands the technology. Otherwise, how could a person *know* what to anticipate, *know* what to monitor, or *know* what to do to exercise positive control and to protect assets?

Because of their expertise and humility, the best performers have a *deep-rooted respect* for the technology as well as their own fallibility. Expertise is more than technical knowledge. Expertise includes understanding, experience, and proficiency. Practitioners, operators, and craftsmen not only understand the safe and proper means for transfers of energy, movements of matter, or transmissions of information; they also understand the when and how pathways between built-in hazards and assets are created and how they could trigger harm—if they lose control. Top performers continuously update their awareness of hazards and their proximity to assets. Consequently, they more readily anticipate the worst, recognize the mistakes they dare not make, and equip themselves to respond appropriately.[17] This level of knowledge and skill becomes a key ingredient to "expert intuition," which will be discussed in Chapter 2.

> **Caution**: Some line managers ascended to their positions, not because of their technical background, but due to their administrative skills. While most line managers don't need to possess the same level of technical expertise as their subordinate front-line workers, manager also must possess a deep-rooted respect for the technology.

But in the long run expertise applied without the input and corroboration of other competent persons is more vulnerable to error, increasing the workers' potential to lose control. Hence, the importance of group conversations characterized with robust dialogues that reveal the technical realities of high-risk work. Recent experience shows that technical expertise practiced collectively is more powerful than when it is practiced individually.[18]

Critical Steps Improve Efficiency

Identifying and controlling Critical Steps help you navigate the safety/production space, optimizing the use of already scarce safety resources. Critical Steps improve the efficiency of human performance by highlighting those human actions, steps, or phases of work that must go right the first time, every time. Tradeoffs between efficiency and safety are normal and occasionally necessary to meet deadlines. You cannot always be completely thorough from a safety perspective and still stay competitive. It's inefficient (and impossible) to attempt to prevent human error on every step and human action of every operation. And you cannot operate with 100 percent efficiency, because some resources are redirected toward safety functions—controls, barriers, and safeguards.[19] But you always want to meet your commercial deadlines, safely, with the required quality committments. You have to navigate a middle ground to accomplish both safety and profitability goals during work.

For complicated operations, procedures prescribe a series of human actions organized in a preferred sequence to accomplish production and safety goals. But which actions require vigilance and heightened attention—which ones absolutely must go right? Most human actions in an operation can be described as non-critical. At those times it may be acceptable to err on the side of efficiency, considering nominal human reliability. Good enough (99.9 percent) is good enough when nothing is at stake. Recall Figure 1.1 and Jill's 100-step task thought experiment. For low-risk operations, we believe it is acceptable to speed things up to reduce costs.

Incorporating the principles and practices of managing CRITICAL STEPS into your operations has as much to do with efficiency and productivity as with safety. You have the option to expedite those portions of a task that have little to no risk to safety and the business, but you must absolutely slow down for those that do. Slowing down is roused by a chronic unease,[*] expert intuition, conversations, and RISK-BASED THINKING. By isolating the more relevant and important human risks, identifying and exercising positive control of CRITICAL STEPS enhance both safety (thoroughness) and productivity (efficiency).[20]

Excellence is NOT Good Enough!

Excellence is always described in relative terms as possessing an outstanding quality or superior merit; remarkably good, *compared to others*. People do things right most of the time. Nominal human reliability drifts between 99 and 99.9 percent, depending on local factors.[21] Is 99 percent good enough? Furthermore, is 99.9 percent good enough for CRITICAL STEPS? We think not. As the Colonel experienced, sometimes doing your human best is not good enough.

But when it comes to doing the right thing and doing the right thing right, such as a CRITICAL STEP, it becomes imperative to avoid losing control. When nothing significant is at stake, 99 percent is satisfactory. This performance level is fine if the person is simply taking care of household chores—making the bed, brushing one's teeth, setting the table, washing dishes, vacuuming the carpet, painting a bedroom, or reading a book. Around the house, for instance, most people rarely experience a genuine problem by performing at that rate of human reliability.

On the contrary, precision and accuracy in execution are more important than speed in high-risk performance situations.[22] High-risk work MUST slow down to allow front-line workers to think and act mindfully—to be deliberately certain that assets are protected from harm despite production pressures. Therefore, it is strategically essential to define and understand what must absolutely go right; without doing so, the cost of failure lies in the harm to key assets. The business case is self-evident. Managers, engineers, supervisors, and workers must all know, understand, and agree on what must go right, especially during high-tempo operations that experience schedule and budget pressures. It is important to recognize that bias toward speed and efficiency is NEVER appropriate at CRITICAL STEPS and RIAs. The risk is simply too great. When a loss of control must be avoided, **precision execution is the ONLY acceptable standard!**

[*] Generally, the experience of concern about risks, exemplified by a healthy skepticism about one's decisions and the risks inherent in work environments. Operationally, an ongoing wariness of hidden threats in the workplace that could trigger harm, spawned by a deep-rooted respect for the technology, its complexities, and its built-in hazards.

Key Takeaways

1. A Critical Step is a single human action that will trigger immediate, irreversible, and intolerable harm to an asset, if that action or a preceding action is performed improperly.
2. If an operation has the capacity to do work, then it has the capacity to do harm. Work is energy directed by human beings to create value. Therefore, work involves the use of force under conditions of uncertainty—that is, risk.
3. The central attribute in the definition of a Critical Step is the degree of *harm* (intolerable) to something of importance—an asset.
4. To be useful in managing human performance risk, the concept of a Critical Step must be reserved for what is profoundly important to safety, quality, reliability, and productivity.
5. Critical Steps improve efficiency of human performance by highlighting those steps or phases of work that absolutely must go right. All other portions of the task that have little to no risk to safety, quality, reliability, and productivity may be performed with deference to efficiencies, while maintaining a mindset of chronic unease.
6. A comprehensive understanding of the technology and its hazards—a deep-rooted respect—is necessary to reliably recognize Critical Steps.
7. Excellence is not good enough at Critical Steps. Precision execution is the only acceptable performance standard.

Checks for Understanding

1. Which of the following actions with a handgun is a Critical Step?
   a. Loading the firearm with bullets
   b. Cocking the firearm – pulling the hammer back
   c. Pointing the muzzle at a target
   d. Moving the safety lever off SAFE
   e. Pulling the trigger

2. Which attribute of a Critical Step is most important?
   a. The harm is irreversible.
   b. The harm is immediate.
   c. The harm is intolerable.

3. True or False. Donning safety equipment, such as hardhats, eye and ear protection, gloves, is a Critical Step.

(See Appendix 3 for answers.)

Things You Can Do Tomorrow

1. Develop an operational definition of a Critical Step that is relevant to each work groups' work. Verify it satisfies all the attributes of a Critical Step.
2. Print several posters with the Critical Step definition. Display them prominently, able to be read from across a room, in work areas and production meeting rooms, especially where prework discussions would occur, and in training settings.

3. Identify operations or tasks currently scheduled that are high-risk or potentially costly if control is lost. Using your definition, pinpoint Critical Steps and the potential harm to assets. Explore means to exercise positive control and to limit harm (to fail safely).
4. Using a previous human performance event as a case study, ask your work group to identify the Critical Steps using this book's definition. Ask the group to judge whether the proposed Critical Steps satisfy the definition.
5. Just before performing high-risk work activities, ask workers to pinpoint those one, two, or three actions that must absolutely go right the first time, every time. Compare those actions with the definition of a Critical Step.

References

[1] Adapted from U.S. General Accounting Office (June 1983). *Operation Desert Storm – Apache Helicopter Fratricide Incident, Report to the Chairman, Subcommittee on Oversight and Investigations*, Committee on Energy and Commerce, House of Representatives (GAO/OSI-93-4).
[2] Muschara, T. (2018). *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations*. New York: Routledge (p.24).
[3] Center for Chemical Process Safety (1994). *Guidelines for Preventing Human Error in Process Safety*. New York: American Institute of Chemical Engineers (pp.207-211).
[4] Hollnagel, E. (2004). *Barriers and Accident Prevention*. Burlington: Ashgate (pp.76-78).
[5] Muschara, T. (2018). *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations*. New York: Routledge (p.25).
[6] Hollnagel, E. (2009). The Four Cornerstones of Resilience Engineering. In: Nemeth, C., Hollnagel, E., and Dekker, S. (Eds.). In: *Resilience Engineering Perspectives Volume 2, Preparation and Restoration*. Farnham: Ashgate (p.29).
[7] Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Farnham: Ashgate (p.2).
[8] Rains, B. (2010). Operational Discipline: Does Your Organization Do the Job Right Every Time? Wilmington, Delaware: *DuPont Sustainable Solutions*.
[9] Nominal reliability rate derived from general human error rates described in Kletz, T. (2001). *An Engineer's View of Human Error* (3rd ed.). Boca Raton: CRC Press (pp.138-139).
[10] Crosby, P. (1984). *Quality Without Tears*. New York: McGraw-Hill (p.76).
[11] Muschara, T. (2018). *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations*. New York: Routledge (p.103).
[12] Ibid. (p.271).
[13] Barber, Herbert F. "Developing Strategic Leadership: The US Army War College Experience." *Journal of Management Development.* Vol. 11, no. 6 (1992): 4-12.
[14] This incident is adapted from one described in Kletz, T. (1994). *What Went Wrong? Case Histories of Process Plant Disasters* (3rd ed.). Houston: Gulf (pp.69-70).
[15] Center for Chemical Process Safety (CCPS) (1994). *Guidelines for Preventing Human Error in Process Safety*. New York: American Institute of Chemical Engineers (pp.207-211).
[16] Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Burlington: Ashgate (p.91).
[17] Weick, K., and Sutcliffe, K. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (2nd ed.). San Francisco: Jossey-Bass (p.46).
[18] McChrystal, S. (2015). *Team of Teams: New Rules of Engagement for a Complex World*. Portfolio/Penguin (pp. 167-169).
[19] Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Burlington: Ashgate (p.28). It's also notable that the second law of thermodynamics means there is always some energy wasted in a process.
[20] Hollnagel, E. (2009). *The ETTO Principle: Efficiency-Thoroughness Trade-Off: Why things that go right sometimes go wrong*. Burlington: Ashgate (pp.25-30).
[21] Swain, A. and Guttmann, H. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report* (NUREG/CR-1278). Washington, D.C.: U.S. Nuclear Regulatory Commission.
[22] Hollnagel, E. (2009). The *ETTO Principle: Efficiency-Thoroughness Trade-Off*: *Why Things That Go Right Sometimes Go Wrong*. Farnham: Ashgate (p. 52).