2 Accidents, Case Studies, and the Need for Safety Systems

INTRODUCTION

While the modern workplace is safer today than at any point in human history, people continue to suffer injuries from robotic systems. As this book was in the final stages of editing, in November 2023, a worker was killed by a robot in South Korea. The robot in question was a material handling robot installed in a vegetable packing plant in the county of Goseong and activated, trapping a technician against a conveyor belt. Alarmingly, the technician who was killed worked for a systems integrator that had extensive experience installing and configuring robots. While the incident was still being investigated at the time this went to press, initial findings suggested that the cause of the incident was human error rather than a material defect in the robotic system or a design flaw. Accidents like this continue to occur, especially as more and more robots begin being installed in small and medium-sized businesses, and many seem to occur during the troubleshooting activity.

MODES OF HUMAN PERFORMANCE

The fact that many robotic incidents occur during troubleshooting is not a coincidence. Troubleshooting is one of the most dangerous activities that industrial maintenance technicians are tasked with performing. In the mining sector, nearly 24% of all non-contact electrical injuries (arc flash or arc blast) occurred while troubleshooting equipment, according to a 2004 presentation at the IEEE IAS Electrical Safety Workshop. Many electrical safety programs observe similar results, suggesting that this finding is not specific to mining and could be generalized to all electrical workers.

Why is this the case? What makes troubleshooting inherently dangerous? The answer is complex but critical to understand, as troubleshooting will continue to remain a significant part of working duties for systems integrators, robot maintenance technicians, and other personnel in facilities around the country. In part, it is due to the fact that equipment may be behaving anomalously, triggering the need for troubleshooting. This errant behaviour can introduce new hazards that a technician may not be prepared for. For example, it is typically safe for workers to stand outside of cabinets containing electrical switchgear when equipment is working normally. However, when equipment begins to fail, it is possible for an arc flash event to burn a hole through cabinet materials and expose a worker to plasma that could cause serious burns. Workers would typically be spending time outside the cabinet of a

 DOI: 10.1201/9781003288169-2

malfunctioning piece of equipment when troubleshooting, increasing the risk of an accident or event.

Further, effective troubleshooting often requires workers to selectively energize equipment in order to observe a fault. For example, if a robot program regularly fails in operation, a technician cannot disable the robot completely and effectively observe the source of a problem – instead, in many cases, he must energize the robot, run the program, and observe the failure to better understand the context. Many systems have safety features like reduced speed operation and a "step" mode that allows programs to be executed step-by-step, but if a problem only occurs at full speed in continuous operation, it may be difficult to observe using these tools.

Troubleshooting is an activity that requires humans to utilize one of the most unsafe modes of human performance: knowledge-based activity. Modes of performance are useful categories to classify human behaviour in industrial operations as well as the larger environment. Generally speaking, most types of activities can be classified as skills-based performance, rules-based performance, or knowledge-based performance. In order to understand the dangers of knowledge-based performance, it is helpful to consider all three modes.

Skills-based performance is a mode of human activity where a person relies on physical skills in order to complete an activity. Experienced workers may even benefit from a type of muscle memory where they are able to go on "autopilot" to complete a task. In sports, this is seen when a baseball player at bat automatically begins running as soon as they hit the ball. The player does not mentally consider if it is foul or fair – as soon as contact is made, they instinctively begin hurtling towards first base. Similarly, accomplished musicians will describe periods of playing a piece where they become distracted and do not think about how their fingers must hit certain keys or valves. With appropriate skill development, humans seldom make errors in this mode of performance.

Practically speaking, many robot technicians will experience this when clearing faults on a teach pendant. Given enough experience, a technician will be able to automatically depress a deadman's switch, reset faults, and activate the robot without necessarily thinking about the sequence of keys. FANUC technicians, for example, will often automatically press [RESET] or [SHIFT] + [RESET] when attempting to jog a robot without necessarily thinking about why. They know that in manual operation, a deadman fault must be cleared before jogging, and given years of experience, will automatically take the steps needed to perform this activity (Figure 2.1).

In skills-based performance, mistakes are rare, in the sense that workers rarely fail to execute a well-developed skill. For example, a baseball player will never begin running towards third base, and a FANUC technician will never press the wrong buttons when clearing faults on a robot. A skill may not necessarily apply to a given situation, and clearing faults may not enable jogging if there is an underlying condition that must be corrected, but regardless, errors in this mode of performance are unusual, except in the case of inexperienced technicians. Inexperienced workers must be monitored, mentored, and trained in order to ensure that they are learning skills correctly – before automatic operation is achieved. It can be challenging to unlearn bad habits, especially if they have become truly ingrained.

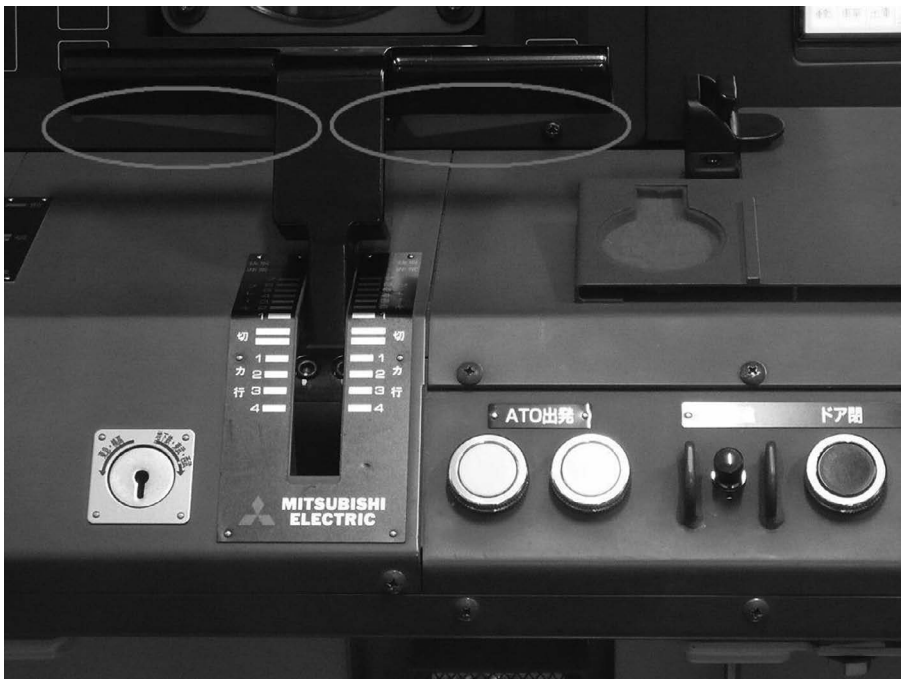

FIGURE 2.1 A deadman switch can be found in non-robotic devices, as well. This example shows such a switch in the controls of the Tokyo Metro cab car. (Photo credit: The RW place.)

An effective way to think about skills-based modes of human performance is to imagine a scenario where a worker encounters a new event. If they are relying on skills-based performance, they will use their skills to cope with and handle this event.

Rules-based performance stands in contrast to this. In rules-based performance, workers are encouraged to use a set of rules or procedures to complete a task or activity. This could manifest itself as a checklist, standard operating procedure (SOP), safe job procedure (SJP), or other written list of rules that specify how a job is to be performed. The idea of rules-based performance is that when an unknown situation is encountered, a worker need only identify the correct set of rules to follow, reducing the chances of making an error in judgement.

Rules-based performance is often found in the aviation industry – pilots rely on checklists to perform many tasks related to the normal operation of an airplane and have checklists they can rely upon when encountering an unusual set of circumstances, such as an engine failure. Checklists are not intended to replace the judgement of a pilot but rather are carefully designed to ensure that critical pieces of information do not get omitted due to the dullness of routine or the chaos of emergency. The contents of many checklists have been revised in response to accidents or disasters, so they are often a living reflection of mistakes of the past (Figure 2.2).

FIGURE 2.2 A U.S. Air Force 1st Lt. completing a preflight checklist before taking off on a mission. For complex tasks like air refuelling, checklists are essential to successful, reliable operations.

Many employees resent the use of checklists, believing that they somehow infantilize the worker or take away agency in operation. Unfortunately, this ego-centric thinking can lead to mistakes from overconfidence and hubris. In a study described by Harvard surgeon, Atul Gawande, the use of checklists in surgery reduced complication rates by 35% and deaths by 47% in hospitals around the world. Sailors on nuclear submarines describe how the use of checklists leads to the vessel working as a well-oiled machine during a red alert or other emergency situation. Yet, the use of checklists has been slow to spread in industry, largely due to overconfidence and complacency. In the case of the accident in the Tesla factory described earlier, if a checklist had called for de-energizing adjacent robots, even if they were not being worked on, the worker in question may have avoided injury.

Knowledge-based performance lies somewhere in between. Knowledge-based performance is a state of operation where humans rely on their knowledge or prior learning in order to identify an appropriate way to address a situation. For example, when troubleshooting a piece of equipment, a worker may check a schematic or think back to a concept covered in a vendor training course in order to decide on a course of action. Knowledge-based operations can be extremely dangerous. First, selecting the correct source of knowledge to drive activity can be a challenge, especially when parsing information in real-time. Which lecture covered the right way to de-energize this capacitor? What was the step I had to perform before that? Can I read this wiring diagram in the shadow of a piece of equipment?

Additionally, when engaged in knowledge-based performance, it is extremely difficult to track the context of an activity in real-time. In effect, this means that a technician may be able to effectively identify the next logical step in a troubleshooting process but fail to identify all of the necessary practical or safety factors that should accompany that step. For example, most electricians know the danger of performing energized electrical work. Many have company policies that require the completion of an energized electrical work permit. Yet when troubleshooting a piece of equipment, technicians will quickly go from listening to an errant hum, to removing a panel cover, to making voltage measurements, without necessarily donning appropriate PPE.

An IEEE study illustrates just how dangerous this can be. In a survey of 5000 electricians, respondents were asked to identify the amount of experience they had in the electric field, the amount of training they had worked on live circuits and whether they had worked on live circuits in the past month. Among all of the electrical workers who reported that they had not worked on energized circuits in the past 30 days, nearly 85% of them reported completing activities that qualified as energized work – such as voltage testing, removing or installing circuit breakers, and repairing energized parts (Figure 2.3).

The same principles apply to robotic operation. Workers may understand the appropriate de-energizing procedures for working with robots that are normally operating, but when troubleshooting a particularly challenging fault, a technician may believe it is appropriate to temporarily energize a system, run a single step in a program, or bypass a safety fence "just for a minute" in order to obtain information needed to continue effectively troubleshooting. Because safety systems are only as good as the humans enforcing their operation, it can be too easy to take a shortcut that seems appropriate in the moment, but actually exposes a technician to significant risks. This is the primary reason that most accidents occur during troubleshooting. Tunnel vision when trying to solve a technical problem is real, and is often the underlying cause of "human error" as described in a media report.

CASE STUDIES

Because the relative number of human-robot injuries is small on an annualized basis, the best understanding of the factors that cause these incidents can sometimes be captured from case studies, anecdotes, or media reports about recent incidents. A handful of incidents are described in the section below and selected for their relevance to robotic safety systems.

1979 – AGV Accident in Ford Manufacturing Plant

This incident is considered to be the first case of a human being killed by a robot in operation. Ford Motor Company had installed a large parts retrieval system in a casting plant in Flat Rock, Michigan. The parts retrieval system could be thought of as a precursor to today's advanced automated storage and retrieval systems (ASRSs). It was five stories in height and relied on a system of carts with mechanical arms to place castings on storage shelves and remove them when needed. Each of the

FIGURE 2.3 Regular electrical safety training is essential to ensuring that electricians and workers encountering energized equipment always rely on safe operating practices. This brochure is in Russian and was found in the Chernobyl exclusion zone. (Credit: ArticCynda.)

automated carts was termed a transfer vehicle and weighed one ton – heavy duty systems that were suitable for transporting large castings.

Unfortunately, the system was prone to errors, according to contemporaneous reports, and technicians were required to climb into the racks in order to retrieve castings when the unit lost count or was unable to operate properly. Some sources also claim that workers performed manual retrieval when the system was underperforming. The system had provisions for LOTO, but as these manual interventions were often required, adherence to protocol began to slip. On the day of the incident in question, a technician entered the storage rack and was hit by one of the transfer vehicles. The collision happened when he was facing away from the vehicle and the overall noise of the plant combined with the rubber tyres meant that the technician was likely unaware of the approaching vehicle. Because the system was not designed to account for humans climbing in the storage racks, the transfer vehicles were not equipped with sensors required to prevent collisions with workers.

The worker's name was Robert Williams, and after the incident, his body remained in the parts retrieval system for approximately 30 minutes until co-workers investigating his absence discovered his remains. Unfortunately, his name will forever be remembered as that of the first human being to be killed by a robot. Litigation ensued, and Williams's estate was able to recover $15 mm from the manufacturer of the parts retrieval system, Litton Industries.

Several conclusions can be drawn from this tragic event. First, Ford did not send workers who would be interfacing with the robotic system to manufacturer training. This prevented technicians from truly understanding how the system they were forced to work with actually functioned. If Williams knew that the carts had no way of detecting human presence, he might have planned his activity in different way or insisted on the application of safeguards. Williams also entered the system without engaging LOTO – something recommended by the manufacturer. LOTO is a fundamental part of industrial maintenance, and when it is overlooked, disastrous consequences often result. The case of Williams is no different.

Interestingly, despite the fact that the above issues could largely be attributed to the actions of Ford Motor Company, Williams's estate was able to recover damages from Litton Industries. The argument made was that Litton was negligent in "designing, manufacturing and supplying the storage system and in failing to warn [system operators] of foreseeable dangers in working within the storage area". The litigation in this case showed robotic device manufacturers of the need to anticipate workplace hazards, even if said hazards are contrary to defined, published operating procedures.

1984 – Incident with a Die-Casting System

Approximately five years after the incident at Ford Motor Company, an additional incident happened in an automotive production facility – this time involving a robot similar to the Unimate system. In this incident, a worker was collaborating with a die-casting system that used a robot to remove a casting from a machine, quench it, and transport it to a press for further operation. The process resulted in flash and scrap metal surrounding the robot that needed to be periodically cleaned up by

workers in the processing area. In this case, the workers engaging with the robotic system received a 1 week training course, highlighting important robotic safety issues and conditions that could arise from automation.

The worker involved with the incident had years of experience in the die casting facility and was familiar with the robot operations, though he was not usually the individual tasked with cleaning up scrap metal. The robot did not have a safety fence installed around the workcell, but instead had a safety rail installed – which provided a visible indicator to operators and technicians of the work envelope of the robot, but could be easily scaled by humans in case of troubleshooting. Signs were posted, warning employees against entering the workcell in operation, and technicians reported warning this operator against entering the cell with the robot in motion.

On the day in question, the operator entered the workcell equipped with an air gun, presumably to clean up flashing surrounding the robot. The robot engaged in a predictable pattern of activity, completing its tasks in a 60 second cycle before restarting the sequence. However, the operator became fixated on the end of arm tooling (EOAT) of the robot and was careful to avoid coming into contact with the working end of the robot. He failed to account for how the rear of the robot moved simultaneously and became pinned between the back of the unit and a steel safety pole serving as a mechanical backstop for the robot. When contact occurred, the operator was pinned by the chest, and the robot stalled, ceasing operations (Figure 2.4).

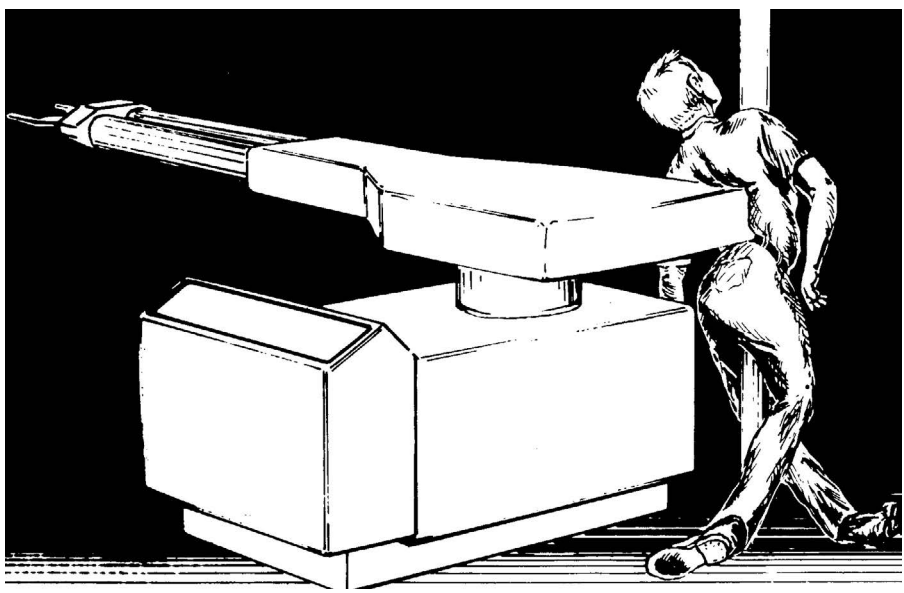

FIGURE 2.4 A drawing of the incident in question, produced by NIOSH. By becoming fixated on the EOAT, the worker was unaware of a potential pinch point from the moving parts at the rear of the robot.

As a result, the worker's heart and breathing stopped, and he was later pronounced dead. Emergency crews were able to initially resuscitate the worker, but he remained in a vegetative state and was unable to regain brain functioning. Subsequent investigation revealed damage to brain tissue from which recovery was not possible. The worker was not crushed and had no signs of broken bones. The National Institute of Occupational Safety and Health (NIOSH) believes that this is the first incident of a worker killed by a robotic arm in the United States.

This event had a major impact on safety systems used to encapsulate robots. First, employee training was modified to show all dangerous parts of a robot, including stationary components that could become crush hazards in the event of certain movements. Training was also revised to include discussion of stationary hazards in the workcell, such as the safety pole in this case. Additionally, the use of a safety rail was replaced by a chain link fence that was impossible for employees to scale in practice. This prevented operators and technicians from engaging in practices that casually ignored safety protocols. While initially, technicians respected the safety rail, once they got used to quickly "hopping over it" to perform some quick maintenance, the practice became endemic within the facility.

Today's workcells often have robots surrounded in solid plastic mesh or metal fencing that is neck high or higher. Workers are forced to enter workcells through predefined entry points that have safety interlocks at door and gate latches. While workers may be trained to not circumvent a safety rail, forcing them to comply is impossible, and a safety barrier that can be overcome will almost certainly be overcome. Witness how many people circumvent caution tape in public spaces. As a result, safety fencing that relies on an operator's voluntary compliance is seldom used in industry.

2015 – Contractor Crushed Inside Safety Cage

Accidents involving humans and robots are not limited to the United States. In 2015, an incident occurred when a technician was crushed to death by a robot operating inside a Volkswagen manufacturing plant. This incident is different from those previously described, as it did not involve Volkswagen employees circumventing safety regulations. Instead, the victim was a contractor working in the facility – specifically to install and set up the robot in question. At the time of the incident, the robot moved unexpectedly in the safety cage and crushed the unfortunate worker who was pinned to a metal plate. Unfortunately, as with the previous case, the worker was resuscitated but later died in a hospital from injuries.

While details of the Volkswagen incident are sparse in the English-speaking media, at the time of the incident, the company made clear that the robot did not suffer a catastrophic malfunction and that the surprising motion was due to human error. Additionally, prosecutors were exploring the possibility of criminal charges to individuals who may have been involved in the incident – the individual who was crushed was part of a team jointly participating in setup and configuration.

However, the incident does show a particular vulnerability in terms of robotic safety controls: the fact that policies for safe operating procedures often only apply to employees of a company. Independent contractors visiting a site may be unaware of internal procedures and use their own documents to establish safe working practices.

In this case, after the incident, many in the media asked questions like, "how could Volkswagen allow a worker to be injured in their facility"? In reality, the worker in question was a contractor with expertise in this particular brand of robotic system. Was it realistic for VW to establish an SOP for outside contractors to perform specialized tasks?

Many, including large automobile manufacturers, would argue that it is not practical for companies to establish detailed procedures for specialized technical tasks that outside consultants are required to complete. If a company doesn't have the internal knowledge or resources, it should not be creating a procedure – the result would likely be a document that could not practically be followed. However, applying a general set of safe working practices to all contractors could be a recommended activity. Many companies prohibit their own employees from conducting business while driving, and will hang up on contractors who take calls from the car. Similarly, best practices for working within safety cages could have been applied to internal Volkswagen employees and contractors alike. These could have included tasks like announcing motion verbally before action occurs, having a designated spotter to watch an individual in a workcell at all times and arming that spotter with a portable emergency stop, requiring activity to be performed in a human free workcell before allowing humans to enter, or other similar tasks.

Interestingly, this case study also presents a useful narrative in understanding the media's engagement with robotics. While the contractor in the Volkswagen plant was simply crushed during robot motion, many media sources like Inverse (BDG Media) describe that the robot "suddenly grabbed him" and "crushed him against a metal plate". Many writers cannot resist latching onto the narrative of a subjugated robot rising up and rebelling against a human operator. The result of this sensationalism can be public fear of robots and discourse that does little to promote actual, tangible improvements in worker safety.

2018 – Amazon Robot Creates Hazardous Environment

The use of mobile robots presents a unique set of challenges for worker safety. The global giant Amazon is one of the largest users of mobile robots in warehouses. Interestingly, compared to other warehouses, Amazon has a much higher rate of incidents. OSHA data from 2022 revealed that there are 6.6 annual injuries per 100 workers in Amazon's warehouses and fulfilment centres, compared to 3.2 annual injuries per 100 workers at non-Amazon facilities. A study published by the Center for Urban Economic Development at the University of Illinois Chicago found that 51% of employees who worked for Amazon for three years or longer reported suffering an on-the-job injury. Causes have been attributed to high production quotas for workers, a culture of surveillance and other factors beyond the scope of this text.

In 2018, multiple workers in an Amazon facility in New Jersey suffered hospitalization as a result of an incident where a robot struck and punctured a can of bear spray, releasing the capsaicin-containing compound throughout the facility. Workers in the surrounding area suffered injuries to their lungs and eyes and were hospitalized for treatment. Fifty-four employees required treatment by first responders, twenty-four were hospitalized and one suffered injuries that were so severe that the media reported him to be in critical condition.

Amazingly, this was not an isolated incident. When reporters began digging into the 2018 event, they found that the company had two additional incidents of bear spray discharge in 2015. In one case, a robot ran over a can of bear spray in Texas, puncturing the can and releasing the contents. In another case, a worker accidentally dropped a can of bear spray being manually handled, triggering the discharge.

Members of organized labour strongly criticized Amazon's pervasive use of robots, with one union President stating to ABC news that "Amazon's automated robots put humans in life-threatening danger today, the effects of which could be catastrophic and the long-term effects for 80 plus workers are unknown…. The richest company in the world cannot continue to be let off the hook for putting hard working people's lives at risk".

The incident highlights several core issues: first, there is a trade-off between robot productivity and safety. If a mobile robot stops every time an unknown obstacle or object is encountered, the safety of those in the surrounding environment can be increased. However, the performance of the robot will be reduced. Imagine a typical Amazon fulfilment centre or warehouse. Because workers deal with thousands of products, there could be small amounts of debris in walkways – bits of cardboard or plastic. If a mobile robot would stop every time one of these was encountered, it may lose a significant amount of productivity. It is possible that an operator puts in a threshold for detection – programming the robot to ignore all objects smaller than some predefined size and stop for large objects like humans or pallet racks. If the bear spray was smaller than the size threshold, the robot could run over the object and cause the incident in question (Figure 2.5).

FIGURE 2.5 Robots in operation in DuPont's Amazon fulfilment centre. The orange robots are manufactured by Kiva Systems and are capable of moving large quantities of product around a warehouse without human intervention.

While it is easy to say that robot programming should err on the side of worker safety, in practice, it is difficult to make a business case for this. Today's Advanced Driver Assistance Systems (ADAS) (ADAS) encounter many sources of data on the roads – if a car slammed on its brakes every time an errant reflection was encountered, the result would be a system that was unusable or so erratic that it posed a threat to the safety of surrounding drivers. Similarly, no facility would tolerate a robot that remained stationary every time a harmless object was encountered. In the case of Amazon, the history of previous incidents suggests that the company should have taken precautions to deal with bear spray in particular, but first-time incidents are notoriously difficult to predict.

This incident also highlights the use of robots in consumer-centric distribution centres. While robots working in large manufacturing facilities may work with dangerous chemicals or compounds, they are usually doing so within the context of a well-defined process. In warehouses that contain consumer goods, this is not always the case. As noted, Amazon warehouses deal with thousands and thousands of stock keeping units (SKUs), many of which can contain hazardous materials. Should robots take special precautions when they are working in a facility in which bear spray could be present? What about lithium batteries that could suffer thermal runaway when punctured? Perhaps Amazon should have segregated potentially hazardous chemicals into a different area of the warehouse and prepared workers for potential exposure.

Unfortunately, the Amazon incident also highlights an issue with the rapid pace of technical evolution with robotic systems. Amazon is infamous for being a company on the bleeding edge of technology. The company has invested heavily in R&D efforts to design robots for use in its own facilities, choosing to establish this core competence as a key competitive advantage. When new robots are released and installed in an Amazon facility, they often involve cutting-edge sensors, computer vision systems, and artificial intelligence (AI) algorithms that far outpace corresponding regulations. Workers interacting with these robots are often unaware of the fact that they may be beta testers in a large-scale data collection exercise. Companies should clearly train workers on both the presence of workers, but also the basics of automated operations. If a worker knows how a robot will make a path planning decision, he may be better equipped to keep himself safe if the robot begins acting erratically.

2018 – Russia's Deployment of the Uran-9 Autonomous Tank

Previous examples of human robot incidents focus on specific events, in which a robot – operating as designed – encounters a scenario where that activity leads to the injury or death of humans in the area. However, robots can also injure people when they fail to operate as designed – when an autonomous system that is supposed to perform a task that is one of the three D's fails to do so and requires human intervention to rescue the robot and complete the mission, endangering lives in the process (Figure 2.6).

While the politics of the Russian Federation are complex, problematic, and beyond the scope of this text, the case of the Uran-9 can be discussed in the context

FIGURE 2.6 The Uran-9 is shown in a rehearsal for a parade in Moscow in May 2018. (Photo credit: Dmitriy Fomin.)

of technical limitations. The Uran-9 is an autonomous tank that is about half the size of a manned vehicle (such as a T-90). It is driven by a diesel engine, and is controlled by a Unified Tactical Management system that allows for a squad of four tanks to be jointly controlled and establishes mesh networking between the units in case any lose the central control signal. Some level of autonomy is present in the tanks, and military analysts speculate that the tanks are intended to be able to identify and engage with enemy forces without human intervention. Earlier members of the Uran series, such as the Uran-6 can perform simpler tasks autonomously, like detecting and clearing improvised explosive devices, but the Uran-9 was expected to be a major improvement in warfighting capability.

Russia deployed the Uran-9 on the battlefield in Syria and reported results at the Kuznetsov Naval Academy for an audience of Russian military members. In particular, the Uran-9 failed to achieve battlefield objects in the following ways:

- The unit's effective range of engagement was 1/3 the published specifications. The Uran-9 was supposed to detect enemies 3.75 miles away in daylight, and failed to detect enemies more than 1.25 miles away.
- The robot did not have stabilization capability operating on any of the warfighting payloads. Firing any weapons was ineffective while the device was moving and communication errors often led to significant delays between command and response.
- Traction units failed due to harsh desert conditions and the use of unreliable parts that were not previously field-tested.

- Electromagnetic interference jammed control signals – a hallmark of operations in Syria. The tanks could only be controlled at distances of 400 meters, whereas operating specifications called for 2900 meters of range. Remote control of the units was lost for nearly 90 minutes in several cases.

The use of the Uran-9 raises several significant issues for robotic safety. First, many devices that are used to engage enemy fighters are typically used in a teleoperated sense. A warfighter in a control room watches the battlefield through a camera mounted on the robot and makes the decision of whether or not to fire weapons on an enemy. A robot may identify a target, but a human operator confirms that identity and makes the decision to utilize lethal force. While the capabilities of the Uran-9 are not fully known to the west, a system that can autonomously identify and attack suspected enemies poses serious questions for rules of engagement and international law. It also should clearly show the voluntary nature of moral codes, such as Asimov's First Law.

However, from a practical perspective, the failure of this robotic unit in a wartime scenario almost certainly put human lives at risk. Presumably, the Uran-9 was deployed in Syria to engage with enemy fighters so that Russian soldiers could remain at a safe distance. Unfortunately, when the propulsion system of the device failed, human technicians had to enter the battle field, resuscitate the device, perform repairs, and resume operations, at great risk to individual safety. When the control system of the device fails, not only could the technology fall into enemy hands, but any autonomous routines could not have been halted by an operator. If the Uran-9 began attacking innocent civilians, its controller could not have prevented or halted the autonomous behaviour if he were unable to communicate with the device.

While it is expected that very few readers of this text will be preparing UGVs for the Russian military, lessons from this are found in many industrial robots that are currently deployed in manufacturing facilities. First, many connections to robots are established through hard-wiring of sensors and control systems. Even though wireless technology has become pervasive in consumer devices, the risk of jamming or a signal loss rendering communication with a device impossible is simply too great for industrial robots. Some robots will refuse to continue autonomous operation if control signals are not present, ensuring that if a cable is cut, a human will be unable to accidentally expose himself to danger.

Further, robots often use technology that is several generations behind the cutting edge. This is not to say that today's robots are not sophisticated or advanced, but rather that consumer-grade central processing units are not immediately installed in robotic control cabinets. If a robot is expected to operate 24/7 for several months of operation, using a chip that may have an undiscovered thermal issue could lead to premature failures, excessive human intervention, and increased risks to technicians. Many robots use processor cores that have been validated through extensive tests that can last more than five years. Some units feature two or three instances of these chips to provide a level of redundancy that is absent in all but the most expensive enterprise servers.

Finally, robots are often tested extensively before being deployed in a real operation. While there are many differences between the Russian military and a U.S.

domestic auto manufacturer, one of the key ones is the testing and certification that technology must go through prior to deployment. New robotic technology systems are often tested in small-scale labs or innovation centres before being installed throughout a facility. No factory performs the equivalent of testing on the battlefield – robots are only adopted into new applications after they have been tested and retested multiple times.

This can slow the pace of technical progress. Many robot manufacturers have released cobots that are functionally equivalent to traditional robots while adding advanced safety features. Yet some of these cobots have not yet been validated through the millions of cycles a manufacturing line is likely to see. One particular cobot that is beginning to be deployed in industry suffered from a bug after a recent software update. This bug caused the cobot to incorrectly measure force on two axes relative to a predefined payload. When collaborative control was enabled, the robot would execute uncommanded moves in two directions. While the robot would still stop if it encountered a person, most units were equipped with welding equipment such as EOAT. In one case, these uncommanded moves brought welding tooling dangerously close to a technician's eye while he was troubleshooting the system. If these robots were installed on a production line by the hundreds, the results could have been catastrophic.

2016 – Security Robot Collides with Toddler

As robots became more able to navigate complex environments, their application spaces expanded from relatively-controlled environments like warehouses into spaces occupied by the general public. These new spaces can be extremely challenging as most people have not been trained in appropriate human-robot interactions and the range of human behaviour can be difficult to predict. Miscreants could attack a robot, children could run into a robot, criminals could try to lure or trick a robot, and the sensory impaired may not even be aware of the presence of a robot.

Japanese researchers performed an experiment to observe human-robot interactions in crowded settings. The research team programmed a robot that navigated through a crowded shopping centre. When a human would block its way, the robot would politely ask them to move. Interestingly, the research team found that adults typically stepped aside to help the robot accomplish its mission. Children stepped aside – but only when people were looking. When nobody else was around, children punched, kicked, and antagonized the robot. Researchers updated their path planning algorithm as a result: their robots now avoid any detected human that is less than 4 feet tall in order to avoid encounters with hostile children.

In 2016, a California shopping mall deployed the Knightscope K5 Autonomous Security Robot (ASR). ASRs are designed to automate some of the more mundane elements of security personnel or watchmen. Many will autonomously "patrol" a predefined environment, detecting the presence of humans and streaming observations back to a control centre via a high-definition video and audio feed. Personnel can teleoperate with the robot to look more closely into specific suspicious situations, follow individuals around a store or attempt to locate the source of a strange noise. Built in routines can automatically set off an alarm if a person is detected

after business hours, and computer vision can be used to automate tasks like license plate reading.

The K5 in particular has a few features that are worth noting: first, the robot uses a combination of lidar, sonar, GPS, wheel odometry and an inertial measurement unit (IMU) to navigate indoor environments and avoid hitting pedestrians. It weighs 398 lbs and travels at a relatively slow speed of 3 mph. It stands just over 5 feet in height and is explicitly designed to have a commanding physical presence and serve as a deterrent for would-be criminals. While the robot has no capability to engage in hostile action, it gives off an impression to the contrary. The robots also must be rugged – in 2017, a K5 was attacked by a drunk man, who tipped the robot over

Unfortunately, the robot was no match for the erratic behaviour of a toddler. In an event that the company described as a "freakish accident", a 16-month-old child began running towards the security robot. The ASR attempted to avoid the child, but continued moving and the child collided with the robot. The robot continued moving, running over the child's leg, and continuing on with its patrol. The child suffered minor injuries – swelling and bruising, and the parents reported a significant amount of sustained crying. Bystanders wondered why the robot was unable to detect when it was impinging on a child's leg and why the robot continued onward, leaving the scene of the incident.

Events like this showcase just how difficult it can be to design a robot that is intended to safely interact with the general public. Human behaviour is extremely unpredictable and individuals range in size from tiny toddlers to full-grown adults. Clearly, the K5 struggled to adapt to the presence of an erratic child. A more conservative motion planning algorithm would have caused the robot to stop completely and wait for the child to leave the scene instead of continuing to move and attempting to veer out of the way. Motion and vibration sensors calibrated to an uneven indoor surface did not have the sensitivity to detect contact with a child's leg and clearly should be recalibrated.

While this incident is not serious, it shows just how hard it can be to make robots that work in a public environment. Because mall security does not clearly fit into the 3 D's, one could argue that it is not the best choice as an automation target, especially given the difficult task of optimizing a mobile robot to perform in a complex indoor environment. Knightscope updated the programming on the K5 as a result of the incident, but the device remained imperfect. In 2017, nearly a year later, a K5 unit working in an office building independently navigated itself into an indoor fountain, tipped over, and fell in, destroying the robot in the process.

Unfortunately, these incidents highlight a major lack of regulations for robotic systems: there is no safety standard that must be met before robots are deployed to the general public. Companies are free to beta test new robots in crowds, try different path planning approaches in response to different settings, and learn from mistakes that could result in injury to others. For a robot to be deployed in a public space, a manufacturer need only find a willing facility owner. The threats of potential litigation and negative media coverage are some of the only deterrents against using potentially dangerous robots in crowds or public spaces. No company has yet been charged with criminal negligence for a robot-caused injury in public, but the day will almost certainly arrive as more and more robots find themselves navigating alongside and around humans.

2021 – Crash of Tesla Operating under Full Self-Driving (FSD)

Fortunately, the automated security robot operated at a slow speed and the victim of the accident was only mildly injured (though perhaps will grow up to have a fear of robots). As robotic systems become larger and operate at higher speeds, the risk of injury increases significantly. Nowhere is this more evident than in the realm of autonomous vehicles. Tesla has been at the forefront of adding elements of autonomy into their electric vehicles, and an automobile that can autonomously propel itself, steer itself, and navigate at a higher level could definitely be considered a form of a robotic system.

Some discussion of vehicle automation will help set context for the Tesla accidents described in this section. Unlike other robotic systems, the degree of automation for self-driving vehicles is heavily regulated both by the automotive industry and government bodies like the United States Department of Transportation (USDOT). The Society of Automotive Engineers (SAE) has defined six levels of automation for autonomous vehicles – many government bodies have gone on to adopt these same classifications. The levels are defined as follows:

- Level 0 – No automation at all. The human is responsible for driving the vehicle and systems do not engage in any "Dynamic Driving Tasks" (DDT), such as automatically steering. Older vehicles are classified as Level 0, but so are some newer vehicles, especially those released in developing countries. In particular, some safety behaviours do not count as DDT, so vehicles with standard cruise control or emergency braking systems are still considered Level 0. A system that intervenes briefly in a hazardous situation is not a DDT. With a Level 0 vehicle, a driver is expected to fully focus on the task of driving.
- Level 1 – Driver assistance systems. In this classification, some part of the driving process may be automated through the use of a technical system. Sensors or cameras may feed a computerized system that can perform functions like adaptive cruise control, where a vehicle can automatically slow down in response to traffic ahead. Another example is lane-keeping assist (LKAS), where steering can be automated to keep a vehicle in a lane on the highway without drifting into neighbouring vehicles. Level 1 technologies have been available since the 1990s when high-end automakers began introducing radar-based cruise control systems. The driver is still expected to maintain control of the vehicle at all times. LKAS may resist a vehicle drifting into another lane, but the driver should not be removing his hands from the steering wheel.
- Level 2 – Partial Automation of DDT. This level increases the hierarchy of automation significantly by allowing systems that can completely perform basic duties while requiring the driver to manage the tactics and strategy of driving. Many vehicles that qualify as Level 2 autonomous vehicles have a suite of ADAS. ADAS are designed to improve a driver's ability to react to hazards on the road and improve the overall safety of a driving. These systems may include elements of Level 1 automation, but add in traffic signal

detection and recognition, automated road sign scanning and interpretation, and more. A Level 2 automated system can "take over" the mechanical aspects of driving (steering, acceleration, and braking) while requiring a driver to keep their hands on the steering wheel to intervene if necessary. Almost all "advanced" autonomy in consumer vehicles in 2023 qualify as Level 2 automation – a few examples include: Volvo's Pilot Assist, Ford Blue Cruise, Tesla's Autopilot and Full Self Driving, GM Super Cruise, and Kia's Highway Driving Assist. Many of these systems integrate high-resolution mapping to engage in more effective driving behaviours but still require an attentive and alert operator.

- Level 3 – Conditional Automation of DDT. There is a significant jump from Level 2 to Level 3 autonomy. In all Level 2 vehicles, drivers are expected to remain alert and focused on the road. Level 3 vehicles officially allow the driver to disengage focus. In other words, in Level 2 and below systems, the driver is actively driving, even when any autonomous system is activated. In Level 3 and above systems, the driver is not driving – the system is performing DDT when engaged. Level 3 is termed conditional automation because the autonomous systems can only engage in specific situations where they are qualified to do so. Situations could include a closed highway, where accurate mapping is available. Mercedes-Benz has Level 3 autonomy available as an option in some vehicles (such as the S-Class sedan), and terms their technology Drive Pilot. When Drive Pilot is engaged, a driver can safely play games on their smart phone, while the system takes care of driving. When conditional awareness causes the system to lose the capability for autonomy, an alert is triggered, requiring the driver to take control within 10 seconds. If the driver fails to do so, the vehicle will pull over and come to a complete stop. Honda's Legend also has Level 3 capabilities, though it was only released in small quantities in Japan. It is significant to note that Level 3 automation requires regulatory approval. Mercedes received approval from the German government to classify Drive Pilot as Level 3 automation on public roads – in the United States, where decisions about classification are left to state agencies, Drive Pilot is only classified as a Level 3 system in Nevada. While many OEMs would like to release Level 3 systems, relying on a government body to make a classification system can be a slow and time-consuming process. This is because a Level 3 system shifts the burden of legal responsibility. If a driver is sending text messages while their Level 2 vehicle is involved in an accident, the driver is deemed responsible. If that same driver was sending text messages and their Level 3 system was in an accident, the driver's lack of focus would not be responsible for the accident – remember when a Level 3 autonomous system is engaged, the driver is not "driving," even if an individual is in the driver's seat.
- Level 4 – High Automation of DDT. Level 4 autonomous vehicles can fully engage in driving tasks without human intervention. If a system failure is encountered, Level 4 systems are designed to halt operation in a safe way. A Level 4 autonomous vehicle is able to complete driving tasks in *many circumstances*, meaning these vehicles may be geofenced or speed limited.

Self-driving taxis operated by Waymo are considered to be Level 4 vehicles – in many cases, these driverless cars do not have a human operator present but are limited to operations in specific parts of Arizona. The Waymo fleet has driven more than 10 million miles, but many YouTube videos still show how objects like a misplaced traffic cone can stymie even the most advanced systems, backing up traffic and causing gridlock. Of particular note are some of the navigation strategies Waymo vehicles use to interact with human-controlled vehicles. While conservative approaches to merging and driving may seem safer on paper, they can actually create risk when deployed in scenarios where such behaviours are not the cultural norm. Imagine a Level 4 vehicle patiently waiting to merge on I-695 outside of Boston – a cultural mismatch would barely begin to describe the chaos that would ensure. Many manufacturers of Level 4 vehicles are requesting permission to deploy their vehicles without human controls – no steering wheels or foot pedals. In regulatory filings, this is claimed to promote safety, since humans should not be intervening in these vehicles during operation. In practice, the result can be unsettling.

- Level 5 – Full Automation of DDT. Level 5 automation represents the ambition of the autonomous vehicle industry and is best represented in quotes from personalities like Elon Musk. In Level 5 systems, the only interaction a driver would have with such a system is the task of inputting a destination. After that, the vehicle would take care of all driving and navigational tasks required to meet that destination. Level 5 autonomous vehicles are not geofenced and have no limits on driving tasks. A Level 5 autonomous vehicle has not been released to the public and likely remains several decades away, according to many industry experts. The benefits of Level 5 automation are tantalizing – Musk asks Tesla owners to imagine a world where their vehicles become revenue streams: when a Tesla owner is not using their vehicle, they could activate a robotaxi mode, allowing the car to respond to ride requests automatically, ferry individuals between locations, and return home when complete. In 2019, Musk claimed that nearly one million Tesla vehicles would be transformed into moonlighting robotaxis in 2020, allowing operators to net $30,000/annually. While visionary thinking is certainly required to advance the state of autonomous vehicles, at the time this work went to press in 2023, no Tesla was able to earn a living for its owner.

These levels of autonomy are critical to understand in order to place accidents involving self-driving vehicles into context. Crashes involving Tesla vehicles have dominated the news for years – in 2017, a vehicle driven by Joshua Brown was operating under Tesla's Autopilot system when it slammed into the side of a tractor trailer crossing the road. Brown was killed, and a National Highway Traffic Safety Administration (NHTSA) investigation revealed that Brown was instructed by the Autopilot system to put his hands back on the steering wheel seven times before the accident occurred. Tesla successfully showed that Brown was not properly utilizing the Autopilot system in a safe way, but the accident sparked a dialogue about the implications of Musk's grandiose predictions. Does naming a system Autopilot

FIGURE 2.7 The wreckage of Joshua Brown's Tesla Model S after his fatal accident. This photo is from the investigation of the National Transportation Safety Board.

accurately convey the fact that it is a Level 2 automation system? If a user activates "Full Self Driving" (FSD) capability on a Tesla, does the name of that system accurately represent the fact that the driver should keep their hands on the wheel at all times? Should Tesla be held more accountable for how it describes its systems in marketing or promotional material? (Figure 2.7).

In 2021, a Tesla Model S was involved in an accident on the Bay Bridge in San Francisco. According to the driver of the vehicle, the Tesla was engaged in FSD when the accident occurred. A police report states that the Tesla dramatically dropped its speed from 55 to 20 mph and changed lane positions. A chain reaction involved eight vehicles, and two children were injured. Traffic on the bridge was ensnarled for hours after the incident. Phantom braking has been widely reported by drivers of Tesla vehicles operating in autonomous conditions, especially since the company moved from an approach involving sensor fusion (lidar + radar + cameras) to techniques that exclusively rely on computer vision. After the accident, Tesla reminded regulators and the public that vehicles using FSD are "not autonomous". When a driver activates FSD capabilities, a dialogue box warms them that the system "may do the wrong thing at the worst time" and the product remains in "beta" or prerelease status, despite being deployed on the public roads.

In the 2021 accident, the driver of the Tesla would have been responsible for the vehicle's accident since, as with any Level 2 system, a driver is expected to remain engaged and ready to take over for a robot at any time. However, this legal requirement belies a practical fact: when technology makes it easier for individuals to complete a task, they naturally lose focus and cognitively consider things other than driving. Do Level 2 systems make drivers safer if they allow their

minds to wander while expecting them to regain control of a vehicle in less than a second? Tesla's systems require "active driver supervision" but while this is a legal requirement, from a practical perspective it remains paradoxical, at best. GM's Super Cruise system uses a camera to perform eye tracking and ensure that a user remains focused on the road while autonomy is engaged. The switch or interface between autonomous operation and manual control remains poorly defined, at best. Simply alerting a driver to take over does not equate to promoting safe operation, especially if an autonomous system begins to fail under truly challenging conditions.

2022 – Drone Mishap During Delivery

Robotic accidents are not limited to terrestrial devices. The final case study in this section examines an event that occurred when an unmanned aerial vehicle (UAV or drone) collided with some critical infrastructure. Drones are some of the most heavily regulated robotic devices, mainly because they operate in a tightly controlled environment: airspace. In every country, airspace has been heavily regulated to allow the safe transport of people and goods in manned airplanes. In the United States alone, the Federal Aviation Administration (FAA) regularly spends $20 bn to maintain the infrastructure that is critical for an aviation industry, including air traffic control systems, security standards, pilot education and licensing requirements, and other factors. While most UAVs are small systems, they have the potential to pose a serious risk to manned aircraft and are heavily regulated. In the United States, commercial drone operators are required to pass a licensing exam that tests knowledge of aeronautical concepts, airspace classifications, safety requirements, and more. In general, U.S. drones are restricted from flying through certain areas, are not to exceed 400 feet above ground level (AGL) unless near a structure, and should not exceed 87 knots in speed. Similar laws exist in countries around the world.

Further, current licensing requirements require drones to be in contact with a visual observer – either the pilot in command or a dedicated individual. Companies can receive waivers to engage in beyond visual line of sight (BVLOS) operations, but typically use multiple visual observers or a tailing aircraft. Drones have significant automated routines built into their flight control systems – many drones can effectively stationkeep without drifting, return to a home location in the event of signal loss or batter degradation and avoid obstacles perceived in a flight path. FAA and regulatory requirements have severely limited the number of truly autonomous drones – devices that can engage in higher-level decision-making and flight planning without human intervention.

Some entities have experimented with these techniques. Swiss Post and Matternet collaborated to develop an autonomous delivery system that used drones. In this system, drones could fly between specific take-off and landing points in order to deliver small payloads – in particular, blood samples or other lab tests. Swiss Post estimated that the drones were able to reduce transit times by up to 45 minutes in the case of critical samples, and the Matternet system managed traffic above delivery waypoints, changed out drone batteries, and enabled flight distances of 20 km. The

Swiss Post drones were equipped with parachute systems, designed to deploy in the event of a failure and protect humans and objects on the ground from a crash of the 22 lb systems. Unfortunately, a crash in 2019 occurred when the drone severed the cords of the parachute and crashed within 50 m of a group of children. Swiss Post ultimately exited the drone delivery system for economical reasons in 2022, though Matternet was able to take over operations.

Alphabet (neé Google) operates a fleet of drones under its subsidiary, Wing, which has been piloting a food delivery service in Australia. In 2022, a Wing drone made contact with 11 kV overhead power lines near Brisbane and became ensnared during an emergency landing. The drone immediately caught fire and had to be removed by utility personnel. Retrieving the drone caused a 45 minute power outage for more than 2000 individuals in the area. Despite this incident, Wing notes that the company has made more than 200,000 food deliveries, serving 100,000 individuals.

However, the crash involved an element of luck. While the Wing drone caught fire, it was quickly caught by operational staff and removed by utility workers, preventing a larger issue. In areas where wildfires can quickly escalate and spread beyond containment measures, the use of drones for delivery is concerning. If the lithium-ion battery in a drone were to rupture during a flight incident, it could create a high-temperature fire that is difficult to extinguish – injuring personnel on the ground or starting a wildfire. In certain parts of Australia or U.S. states like California, this fire could become a major incident, threatening thousands of homes. Most drones do not contain provisions for self-extinguishing fires, making the threat of explosion serious, especially if operated in remote areas. Previous major forest fires have been started by items as small as a discarded cigarette butt – a drone fire burning at more than 2000 °C could produce results that are just as catastrophic, if not more so.

IMPLICATIONS

The above case studies clearly show that accidents caused by robotic systems remain a part of everyday life for individuals around the world despite the existence of well-defined safety requirements. In part, difficulties stem from the voluntary compliance with these protocols – while industrial robots should be deployed within a safety fence, a company can override protections with a minimal amount of technical knowhow.

More significantly, the safety issues detailed in this section tend to arise at the onset of deployment of new robotic technologies. Early uses of robotic arms led to safety incidents while operators learned best practices for managing risk. Unfortunately, many of these incidents drove the development of the safety practices that will be outlined in later sections of this book. Similarly, incidents with drones and autonomous vehicles are occurring during the nascent years of these technologies – as society gains decades of experience with self-driving cars and UAVs, the incident rate is expected to decrease.

It is crucial that any operator or implementer of a robotic system consider the context of their own operations. It is not sufficient to blindly implement a safety

standard without considering a particular application or operational environment. System integrators and asset owners must think critically about how a robot is going to operate, who will be in the area, and how exactly tasks will be performed in order to consider all of the safety implications of operation. Robots in workcells must pass material into and out of the cell, and these interfaces are often the source of accidents. Additionally, accidents seldom occur when a robot is operating normally – users must consider carefully failure modes, repair practices, and how exactly systems breakdown in order to implement and apply safe working procedures. The next chapter of this book will outline existing standards and help the reader integrate those practices into effective operation.