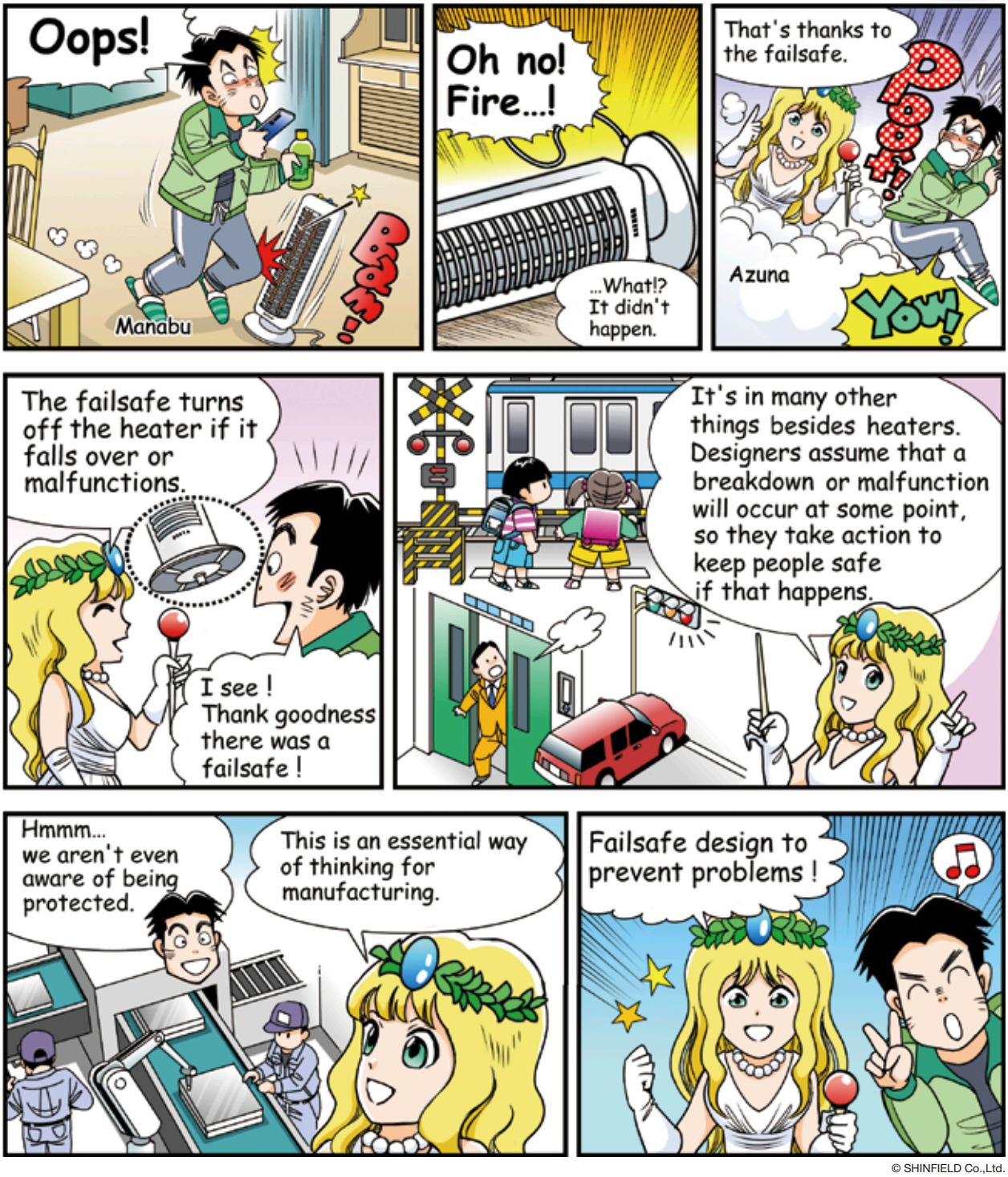
A to Z Vol.40

Keyword

Failsafe

Failsafe (or fail-safe) is the idea of designing and incorporating a mechanism that automatically provides safety in the event of malfunction or erroneous operation of devices, equipment, facilities, and systems used in various locations, including production sites at factories.



Safety design based on the premise that “things will break”

Devices and equipment operating in various locations such as homes, stores, and factories may not function properly due to damage or deterioration of components. Systems may malfunction or operators may make a mistake. It is possible to prevent failure to some extent by increasing the durability of components with design improvements and appropriate maintenance. However, it is difficult to completely avoid damage and deterioration, so you need to recognize that systems will malfunction and devices and equipment will fail.

If a malfunction or failure occurs and the equipment can no longer function properly, it can pose a threat to safety, depending on the type and use of the equipment. The idea of a failsafe is to anticipate these risks and design products to have a mechanism that will always provide safety in the event of a malfunction or failure.

Shutdown upon problem detection, putting the priority on safety

A familiar example of a failsafe system in Japan is seen at railroad crossings. Electricity is normally used to raise and lower the gate, and electricity is also required to keep it raised. The mechanism is designed so that in the event that there is no power due to a failure of the control device or power outage the gate's own weight will keep it down. This prevents passersby from entering the crossing, thereby eliminating the risk of an accident.

Some products are designed with not only equipment failure but also with disasters and human-induced accidents in mind. For example, electric heaters are equipped with a mechanism that turns off the power when vibration from a fall or an earthquake is detected. There are many Japanese kerosene heaters on the market that are equipped with a similar automatic extinguishing mechanism in case of an earthquake. In other words, if the heater falls down and is no longer able to provide its heating function safely, it will automatically operate to eliminate the risk of fire and ensure safety.

Failsafe systems are also essential for preventing work-related accidents at manufacturing sites where various factory equipment and machine tools are in operation. This includes a function that automatically stops machine operation immediately when something abnormal is detected, or an emergency circuit that operators can use to stop operation if something is wrong or if there is some problem during work. It is a basic requirement at manufacturing sites that machines and equipment be equipped with various safety devices.

Advanced safety design creates safe workplaces, preventing work-related accidents

As mentioned above, failsafe design is a safety concept based on the premise that things break and people make mistakes, and it ensures safety even if there is a failure, operator error, or disaster. Design concepts similar to this are *fault tolerance* and *foolproof design*.

Failsafe is a design concept that stops the function of a product, whereas fault tolerance ensures safety by maintaining the function of equipment, etc., even if a failure or malfunction occurs. Fault tolerance is applied mainly in fields where the loss of functionality could be fatal, and centers on the use of redundant configuration, where backup devices (backup power supply, etc.) are installed. Aircraft are a typical example. If the flight function stops due to equipment failure, it can lead to a catastrophe. By providing multiple engines and redundant flight control equipment, it is possible to provide fault tolerance and thus maintain safety.

Foolproof design is based on the premise that people make operational mistakes. The idea is to create a system that will not put people at risk or damage equipment, even if the equipment is used incorrectly. Examples of foolproof design include preventing the drum of a washing machine from rotating unless the lid is closed, and preventing the engine of a car from starting unless the brake is being pressed. Machine tools, facilities, etc., at manufacturing sites incorporate many mechanisms to ensure that operating errors do not directly lead to physical danger and to prevent incorrect use from occurring in the first place.

In the future, even more personnel equipped for work in the global workplace will be required in a wide range of fields including, of course, in industry. In order to prevent work-related accidents and fully ensure safety in workplaces where operators with different languages, cultures, and customs work, it is essential to introduce safety concepts such as failsafe design. There will be an increasing demand to adopt mechanisms that increase the safety of facilities, devices, and equipment, and to further advance the related technology.

This article was published in April 2024.