# SAFETY IN MACHINEY: THE LOST ISLAND

**C** These are my son's feet. There is a right foot and a left foot.
**C** Now he’s wearing a sock on his right foot and in this picture, **C** he's wearing a socks and a shoe on his right foot.

Last year I was on holiday with my family in a **C** European town. We were in **C** a theatre... more precisely in the foyer **C** of a theatre, and we were going down the **C** escalator hand-in-hand with our children when this **C** happened.
My eldest son, who was only seven years old then, **C** got his shoe stuck in the escalator a few seconds before he reached the end.

Fast like children are, **C** my son managed to pull his foot out of the sock and shoe **C** just in time.

Now I know I've got your attention we can start the talk. My name's Cristiano Giavedoni and this presentation is called **C** Safety in Machinery: the lost island.

The word **C** safety means the state of being safe, unharmed.
A very simple concept. **C**
It's the condition of being protected against the consequences of possible malfunctions, **C** damage, faults, errors, accidents or hazards which may be considered "undesirable", unpleasant.
Safety can also be defined as **C** the control of recognized hàzards to achieve an acceptable level of risk.

We are safe when undesirable things do not happen. The fact that certain events do NOT happen, leads to safe conditions.

Safety therefore means something bad, something ugly,…it doesn’t happen.

**C** The hard hat a rigger has to wear **C** cannot prevent objects falling. It can only make sure the consequences of falling objects are reduced to an acceptable level.
The same goes for other personal protection devices and machinery.

**C** Escalators are considered very safe statistically. Don't worry, I won't go on about escalators for the *hole* presentation.
Only one person **C** in ninety million four hundred and seventy thousand dies in the United States every year in accidents due to escalators. **C** the other ninety million four hundred and sixty nine thousand nine hundred and ninety nine... were safe.
1 out of 90,470,000 **C** means an unsafety percentage of 0.000000011%, which is considered exceptionally low, tiny, irrelevant.

Although it's very hard for me now to explain to my son that escalators are safe machines, the statistics prove me right.

Mankind's inclination towards **C** controlling the consequences of events is innate, to such an extent that great thinkers, politicians and theorists in the past have designed **C** perfect societies and communities and have often drawn up their guidelines.

When a community, no matter how big or small it is, such as the rigging community for example, **C** seeks to build a behavioural social structure governed by desirable qualities and objective procedures, such as standards, certifications, qualifications, et cetera, they're in all respects building what the ancient Greeks called a **C** Utopia".

The word Utopia means an ideal place that exists and lives as a concept **C** and whose validity is only confirmed theoretically, but there are only a few sporadic examples of its actual existence.

Safety is a *iutòpian* condition in all respects. The word *Iutòpia* itself is a combination of two words, **C** topos, meaning **C** place, and *iu*, **C** which means **C** not. **C**
*(pause)*
No place, good place.
Safety is a non-place consisting of the non-occurrence of undesirable events. It's a triple negative.
In my personal opinion, there is only one place where it's possible to set a discussion on safety: the place/non-place par excellence.

**C** On an island.

Islands have always fascinated explorers, and in the past they got them into more or less fortuitous adventures.
Among the many islands that intrigued adventurers in bygone days, there were, for example, the island that doesn't exist. **C**
If you want to follow me on this fantastic journey, non existent islands are not very interesting for safety purposes, but we'll look at them anyway.
There are two types of islands: **C** those that **don't exist by definition**, such as Peter Pan's island, and **C those that pretend to exist**, such as Stevenson's and Verne's islands, but which everyone knows are the fruit of a fertile imagination.

Let's start from the latter, the islands that pretend to exist.

The wiring diagram **C** of a one-channel control system for a fixed-speed three-phase motor is quite simple.
The three phases reach the main contactor **C**, which distributes them to a wired reversing contactor **C** so that the three output phases are linear on one side, and inverted on the other.
Two of the phases supply a transformer **C** that provides low voltage current the coil on the main contactor **C**, (normally open), and the coils on the **C** reversing contactor, which are also normally open.
Using a selector and a GO button, or two **C** GO buttons, one for each direction, it's possible to let the current through and allow the motor to move clockwise or anticlockwise, making the machine to move in one direction or the other.
**C** Look, this makes it clearer.
If one of the parts in the system fails, you can hit the emergency stop button.
The low-voltage power supply is mechanically cut off and the main contactor coils are de-electrified. Consequently the contacts mechanically break, power is no longer supplied to the circuit and the motor stops running.

A contactor has three components **C**. **The contacts** are the current carrying part of the contactor. This includes power contacts, auxiliary contacts, and contact springs. **The electromagnet** (or "coil") provides the driving force to close the contacts. **The enclosure** is a frame housing for the contacts and the electromagnet.

When current passes through the electromagnet, a magnetic field is produced, which attracts the moving core of the contactor. **C** The moving contact is propelled by the moving core and the force developed by the electromagnet holds the moving and fixed contacts together.

Because *arking* **C** and consequent damage occurs just as the contacts are opening or closing, contactors are designed to open and close very rapidly.
However, the heat energy contained in the resulting electrical *ark* is very high, ultimately causing the metal on the contact to migrate with the current.

With the continual occurrence of *arks*, if the metal parts are rusty or damaged by weathering or aggressive environments, **C** the contactor contacts may fuse and "stick" together.

If this occurs and a contact get stuck, what happens is, even if you release the GO button, the motor does not stop because the current continues to flow through the contactor to the motor.
In these cases, you have to hit **C** the emergency button as soon as possible to cut the power off to the primary circuit and stop the motor.

Ok, let's stop here because this isn't a training session, but a talk.
We have analysed the electric circuit of a one-channel motor control system together in just **a** few minutes.
**C** Now, contrary to what ethics and common sense would suggest, I'll reveal what type of control this circuit belongs to and I'll tell you the make and model.
I apologize in advance to the manufacturer, but conferences must have deep educational aspects too.
The control is called:

**C** Dizzy!

The electric circuit we analysed belongs to a three-phase cement mixer and it's in all respects identical to the electric circuit of one channel of a standard controller for electric chain motors.
I've studied plenty of them.

A cement mixer.

The system that controls a cement mixer is *adequte* for its function in its conditions of use and the way it's installed.
These parameters are almost identical for cement mixers in many parts of the world because "the intended use" of the machine does not vary so much.

Coming back to us and our world, the Event Industry, **C** multichannel systems, similar to Dizzy's, are often used to drive fixed speed chain hoists, although I think we all agree there are no 4, 8 or 12 channel cement mixers anywhere in the world. **C**

A pickle **C** should only be used when "preparing" the hoist for use. As soon as a load is applied, it should not be used even to operate a single hoist, despite what I've read in the draft of a new standard for portable control units. The reason is simple: it does not have an emergency button.
In the same way, moving pieces of scenery and structures over the artists' or audience's heads requires monitoring systems ... probably different from Dizzy's.

A few months ago I read an article about a band on tour, just like many other bands.
The rig described by the lighting designer involved moving some lighting trusses over the band.
What struck me in the article was where the lighting designer said: “… the automation was made in the good old fashion way, by a man pressing a go button sitting on the side of the stage”.

The islands that pretend to exist are harmless if their existence is limited to our imagination.
In this case they're symbolic islands **C** which introduce us to worlds that - although they are not real - can be explored, perhaps only for educational reasons.
**C** As soon as these imaginary places become concrete in the real world, they do it in the form of myths which are very difficult to eradicate and sometimes very dangerous.

The belief in "good old fashion ways" must today measure up to the social and legal concept of acceptable risk, which might be very different from what was considered acceptable ten or twenty years ago.

That’s enough about non existent islands. I could give you loads more examples, but they're not very interesting for one simple reason: nobody goes looking for them... children don't go to sea in search of Peter Pan's island, and adults don't look for Captain Nemo's.
We Hope.

Beside non existent islands, we also find **C** islands **that exist too much**: the islands of redundancy".
Islands that exist too much embody the myth of excess: cornucopia.
These islands of excess are islands that look different when seen from different points of view, but in the end are the same island; or they may look like the same island, but are actually completely different ones.

On sailors' maps, there is evidence that **C** *Selón* was believed to be Taprobane for a long time.
Taprobane was an island that you always found, even when you weren't looking for it.

It was harder to find *Selón*, which you only got to if the maps put it south of the Indies.
Pliny said that Taprobane had been discovered at the time of Alexander the Great, but it's only in Medeville's travels that we begin to suspect that *Selón* and Taprobane are the same island.

An island with **C** two identities, or two islands that, once you find the first one, you automatically lose track of the second?

In the world of rigging, there are (or have been) similar cases, where the nature of a **C** thing is double.
The case recently solved in Britain of the double identity of the STAC Chain is an example. **C**
In the past, depending on how you looked at it, **C** it was sometimes **C** a lifting accessory and therefore subject to certain laws that don't allow its use in particular circumstances, or it could magically become **C** lifting equipment, which could be used freely, but subject to completely different criteria.
Now there is a code of practice **C** that finally puts an end to this *surreal* case of double identity.
Note, I am using the term STAC improperly for a long link chain. There are several makes, like Crosby and others I can't think of at the moment.
To be precise, this Code of Practice aims to solve the confused identity of all long link chains.

Another episode of islands that exist too much, of unnecessary redundancy, can be found in the **C** safety coefficients vs overload devices.

In engineering, redundancy is the **C** duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

The two functions of redundancy are **C** passive redundancy and **C** active redundancy. Both functions prevent performance decline from exceeding specification limits without human intervention using extra capacity.
**C** If active redundancy uses active and passive components, **C** passive redundancy uses excess capacity to reduce the impact of component failures. One common form of passive redundancy is the extra strength of load chains or steel wire ropes. Extra strength allows some structural components to fail without machinery collapsing.
**C** The extra strength used in the design is called the margin of safety.

**C** To leave loads suspended or to move loads above people, several codes of procedure and European standards state you must de-rate the loading capacity or you have to use machines with a safety factor of 8:1, in some cases, or 10:1, in others.
I know we have talked about it every time at every conference for years, but why **C** not 7.5 or 9.25.
Even before the standards and laws, **C** no manufacturer would ever have designed an object with a safety factor of 1 since, as soon as it was used at full load, it would have broken.
This is obvious.
Therefore the manufacturer would have **C** doubled the safety coefficient to increase the endurance of the component.
Then came the European Directives. **C** One very well known one – the machinery directive - states that four is an appropriate safety factor, twice what a manufacturer with common sense would have applied by default.
**C** Although the word "redundancy" doesn't appear in the machinery directive, I agree with the approach since it's correct and logical:

the legislator has applied the concept of passive redundancy **C** to the letter by doubling the safety coefficients in order to reduce the risk of mechanical failure to an adequate level.

There was no need for complex engineering calculations, just a simple multiplication, the same one the manufacturer did: times 2

But suspending and lifting loads over people's heads is outside the scope of the machinery directive and this is where the European standards come in.

When loads are suspended or moved over people's heads, the passive redundancy in many European standards and codes of procedure is ... **C** multiplied again, creating a double redundant machine.

Up to this point, we can accept it as "expensive" *excess of zeal*, which can be justified by the **C** relative unreliability of direct acting capacity limiters, (clutches) which do not always (actually very rarely) prevent overloading in the range considered acceptable.

We gladly accept the concept: clutches are not reliable.

However when we read in several European standards that since clutches are not considered reliable they cannot be used as overload protection devices, and that to stop the movement in a multihoist systems – in case of overload -, the hoists must be fitted with **C** indirect load control devices, i.e. load cells ... then the double redundancy is multiplied again and becomes – in my opinion – excessive at times.

**C** All this while the coefficients at the hanging points remain unchanged at the values they once had, between 1.6 and 4. At this point I ask myself and ask you a question:

**C** Do we really need all this expensive, heavy and onerous redundancy?

Are we certain that our *douts* about safety on machinery are dispelled by all this extra extra extra strength?

**C** Is the lost island really there?

When redundancy is applied to safety components and the safety related parts of a control system, in other words when redundancy refers to the active parts of a system, we move on from the island of overengineering, towards the *arkipelago* of unfound islands, **C**. We enter the stormy seas of inaccuracy and this is where ... we start to enjoy ourselves.

A long time ago navigators **C** only had the stars to guide them.
With instruments, such as the astrolabe or sextant, you measured the *hait* of a star above the horizon, you calculated the distance from the Zenith and, knowing its **C** declination, you could discover which parallel you were on, in other words how far north or south you were of a known point.

**C** The principle of the sextant is based on the presence of certain fixed points, **C** such as the Sun, the Moon and certain stars or constellations.
Without fixed points it's hard to find **C** an island and, if you find one by chance, you can't be sure you will be able to find it again when you leave port.

Using safety devices and functions in a control system is certainly one way of reducing risk, but it is only one.

Moving loads without a **C** load cell is like driving a car without a speedometer: you have a clear perception of the movement, but you're not sure what speed you're going at.

Also it's a difficult task to guarantee the safety of moving systems made up of several machines interacting with each other (such as hoists that lift trusses or grids) without being in control of their **C** position and their operation.

The European guidelines on the subject of lifting in the entertainment industry establish quite rightly that machines and control systems without **C** "minimum basic" safety measures may not operate where there are people under the load, not to mention using them to carry or suspend people.

If you want to work with acceptable safety margins, "Dizzy-like" architectures are no longer sufficient to guarantee an acceptable level of risk, and **C** the control systems that move the most powerful and fastest machines must be equipped, if necessary, with safety devices that are suitable for the complexity of the lifting system.

The safety equipment needed for a control system **C** varies according to the stars and recommend redundancy as a way of reducing risk.

We find it in the German **C** and British standards, and - although restricted to the integrity of control system safety devices and functions - it's well explained in a well known **C** international standard the EN 61508

If we follow the stars and we trust them, it would in theory be enough to equip every machine and every control system with redundant safety devices… **and Mario's your uncle!:** safety would be guaranteed.

Therefore a lifting machine with two brakes, four-position limit switches, a dual encoder, a load cell, a thermal sensor on the motor and an on-board PLC controlled by a control system with safety functions would be safe.

It would be safe because the level of risk would be reduced to an acceptable limit and I could prove the risk has been reduced.

How wonderful ...

According to the system integrity level, the amount of redundancy that is applied, the number of components or functions that are doubled and monitored and the soundness of the system architecture, you can achieve control systems with functions that correspond to three different values of a safety scale **C** that few people understand, but which many fear:

**C** SIL
“Hey did you know I have a new control system, and it’s SIL3”
“Really, wow, that’s great! And what does the system do?”
“No idea… but it’s safe!”

A machine (a hoist or winch) cannot be SIL1, SIL2 or SIL3 ... it can't be, by definition.
SIL only applies to electrical, electronic or programmable electronic devices and safety functions.
**C** A hoist can therefore have a SIL3 component, an encoder for instance, which means it's built in such a way as to have a very low PFH (Probability of Failure per Hour).
Or a safety feature can be considered SIL2 or SIL3. In any case it refers to a complete system since integrity can only be achieved by a logical combination of components, functions and software.

These elements may be different from each other and, taken individually, they might not achieve the desired SIL level on their own.
Unfortunately there's a common tendency to generalize and simplify concepts we are not able to grasp and we increasingly confuse the value of a certificate with the broader sense of safety.

**C** On that day, in that theatre, looking at my son's shoe and sock horribly stuck in the escalator, I asked the maintenance man, called in by the theatre management to investigate the incident, if things like this were rare or common.
The maintenance man told me in a low voice " **C** you should see how many crocs get stuck in escalators in the summer".
I repeat: "you should see how many ... in the summer".
If you want to lose your appetite and a few nights' sleep, type **C** "crocs escalators accidents" into Google Images.

Thousands of children every year end up with their feet stuck in escalator *coumplates* and are horrifically mutilated.
Of course we are talking about escalators that comply with **C** ISO 22201-2: 2013, Lifts (elevators), escalators and bla bla bla.
Certified escalators.

However, the thing that made me shudder was not finding out that episodes like the one that had just happened to my son was known to the experts. What made me think deeply was what he said after that.

I asked the technician what would have happened if my son's foot had also ended up in the *coumplate* together with his shoe and sock. I asked him what I could have done to reverse the escalator, free his foot and run to the nearest hospital.

He told me: "When the safety devices trip, there is no way to start the machine up again. You have to wait for the fire brigade to arrive to remove the *coumplate* and release the victim."

**C** *Coumplate* impact devices or *coumplate* safety switches are certified devices manufactured by European multinationals "that are designed to shut off the motor and activate the brake in the event *coumplate* movement is detected horizontally or vertically or to stop the escalator in case objects become trapped between the comb teeth and the moving step band.

At that moment I imagined my son with his foot stuck, bleeding and in agony from the pain, and my powerlessness to help.
No one would be able to free him apart from the fire brigade because there is no way to restart the machine, since the *coumplate* impact switch has no override.
What if the accident had happened elsewhere, perhaps in an area where few people pass, like a remote terminal in an international airport late at night?

This is when **C** we lose the islands, quick as a flash.

Long pause ... (drink)

**C** I don't know how many people know that New York and Naples are on the same latitude, but I'm sure everyone knows they're not in the same place.

The issue that caused sailors big problems until almost the end of the eighteenth century **C** was that there was no sure way to measure *longhitude*, in other words to say how far east or west you were of a certain point.
That's why many islands were found… then lost again.

The great European maritime powers fought for centuries to find a way to "fix a point" and were willing to pay huge figures to anyone who could come up with the correct method.
Navigators, men of science and adventurers designed all sorts of things. There was a method based on lunar eclipses, and one on variations in compass needles.
**C**
All these methods turned out to be unsatisfactory.
Well, actually ... there was one way: take a clock on board that keeps the time of a known meridian, measure the local time in place X and, based on the fact that the globe is divided *longhitudinally* into 360 degrees and that the sun travels 15 degrees in an hour, calculate the difference in longitude of place X.

The problem was not telling the local time in place X, but finding a highly accurate clock to take with you.

Without meridians, islands get lost.
Let's outline some of the meridians we have to consider in the search for our safety island.

**C** Competence
Rescue plans

Risk Assessment
Chain of responsibility
Maintenance
Qualification
Inspection

Machinery certification **C** gives only a two-dimensional view of risk and is useless unless it's crossed with the meridians of common sense and competence.

Redundant systems and glittering certificates only provide the outline of the safety we are striving for. They give us the tools, but not the context to use them in. **C** Sometimes we can foresee the situation we are about to face from just a few clues thanks to experience and knowledge.

But believe me, there is nothing more elusive **C** than an island you only know the outline of.
In the same way it was once possible to perceive an island that was not there among the reflections on the sea, it was also possible to mistake two islands that look identical and never find the one you wanted to go to.

I often receive emails from operators and head riggers seeking advice on automation and frequency drive systems.
Many times the questions relate to the conformity of this or that system with standard X or regulation Y.
Nobody - I repeat nobody - ever goes to the *hart* of the matter and discusses the details of what they should do with the control system they intend to use.

**C** Months ago, a highly cooperative head rigger sent me the risk assessment of a rig because an international venue had demanded the system to be SIL3.

I received the risk assessment, and after I read it, if I had been the venue or an inspector ... I would have asked for ALL the control system safety functions to be SIL3 and for ALL the hoists to be equipped with redundant safety devices.
Why? Because it was impossible to understand exactly what the system did from the risk assessment.

It didn't say how many scenes there were, how many movements the system had to do, how long the machines had to work for and at what speed. I had a vague idea of how evenly distributed the hanging loads were, but there was no reference to the frequency of exposure to risk, how many actors/performers would be found under or beside the load, if the danger was avoidable or not, and the extent of the consequences resulting from a breakdown or malfunction, if there had been one.
In short ... it was impossible to understand the magnitude of the scenic movements, so – rightly – the venue and the inspectors imposed the maximum level of safety.

**C** It only took a morning, not a month, to explain how he should break down the scenic movements and how he should proceed with calculating an adequate SIL for the possible risk in the event of an accident.

The result was that most of the movements only needed SIL1 and only a few needed SIL2.
But the outcome might have been different.

The rigger integrated his equipment with adequate protection devices, produced a true safety concept, informed the production, got approval from the venue and inspector, and the show took place without incidents.

**C** Whenever we do a risk assessment seriously, whenever we write the pros and cons of a particular choice on a sheet of paper and analyse the consequences, we are forced to make thousands of small decisions.
For some decisions, we only have to think and use common sense, the means at our disposal and our expertise. For others, we have to ask for assistance from other qualified people because the answers are out of our field. However, regardless of how these small decisions are made, they reveal and examine many – if not all – of the risks that we have to consider, including residual risks.
Without assessment, there is improvisation, and with this many of the assumptions behind machinery safety come crashing down.

In the choice of equipment, we need less Dizzys, but also a reasonable number of extra super redundant machines. We should prefer certified systems, but it's important to understand that they are only one step toward achieving a safe rig.
No acceptable level of safety can be achieved without a thorough risk analysis.

So maybe, if we cross the adequate equipment latitude with the risk reduction measures longitude with patience and diligence, **C** we can aspire to finding the right point on the map: the lost island that many seek and few manage to find, hidden somewhere, between Naples and New York.

Thank you