Figure 1

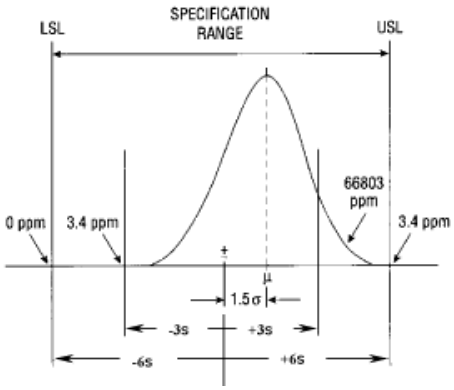
Introduction

Independent if a product is manufactured at high or at low volumes, often human quality control is either too expensive or too error prone. However, the problem to solve is always the same: How do we guarantee 100% defect-free products.

Even though, the control requirements of any kind of product are different, there exist still many similarities. This paper is a step-by-step guide to design a secure quality control system.

What makes clients angry?

Quality control cannot address all the quality features, but only a few selected ones. Otherwise quality assurance gets too expensive or too error prone. Therefore, it makes sense to choose the most important quality features.



Design for Six Sigma

Six Sigma compliance means that a product is 99.99966% defect-free. The primary goal of Six Sigma is to improve customer satisfaction, and thereby profitability, by eliminating defects.

if it needs to be safer

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

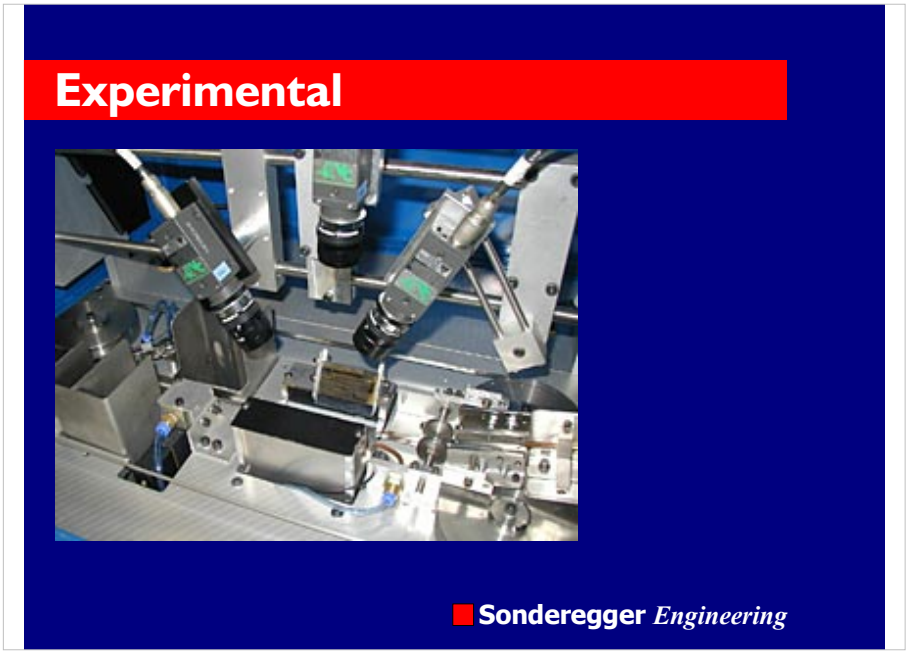


Figure 2

The hard way, however often done

The most apparent way to control quality is using cameras together with a computer. The important quality features are saved in a database. The sample is then compared with the database.

When everything is so easy, why should you search for another solution? Because it is not stable!
With time, there are changes in the behaviour of any technical system. Temperature, light, humidity have influences which are reversible. Over a period of months,non-reversible effects influence the device, like wear, shift and ageing. The most tricky changes are undocumented alterations done by maintenance staff.

To solve this dilemma of stability, the system developer tends to increase tolerances to avoid, that too many good parts are thrown away. On the other hand, if the tolerances are kept narrow, the system needs to be readjusted frequently.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

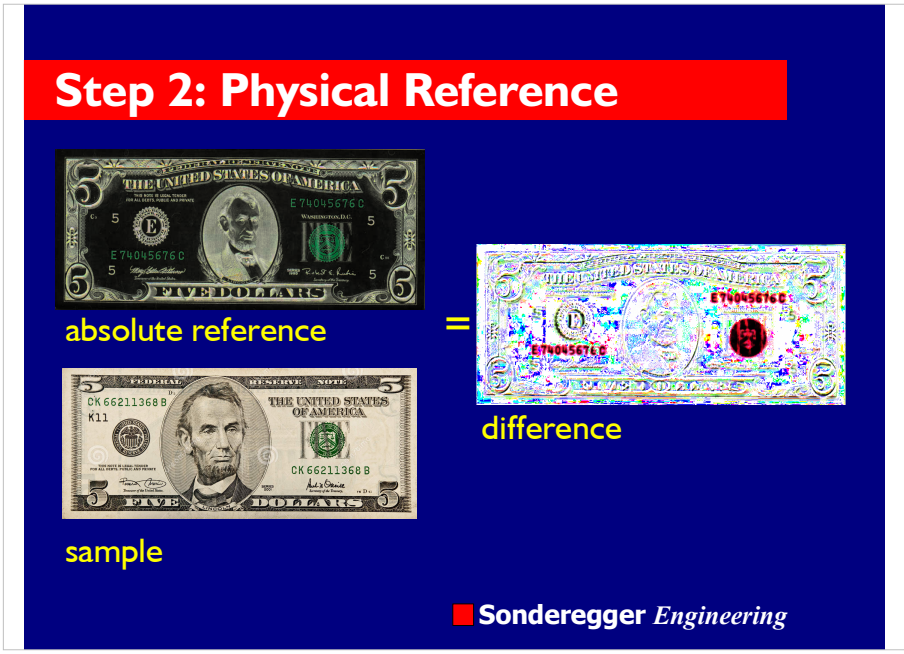


Figure 3

An example from daily life:
Parking garages have low clearance. To insure that cars entering the garage will fit, garages are fitted with a go/no-go gauge at the entrance. Hitting the swinging pipe will not damage the vehicle as much as driving into a concrete beam.

The right approach: Using an absolute reference

Instead of using software decision-making, we propose going back to the roots: Use physics as much as possible for decision making. Please, remember: Physics does not make mistakes, software and humans do!

Instead of using computers and technology, we always compare to an existing absolute physical reference. Please understand us right: We also use software, but as safe as possible.

„Working with physical references, drift has no effect“

if it needs to be safer

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

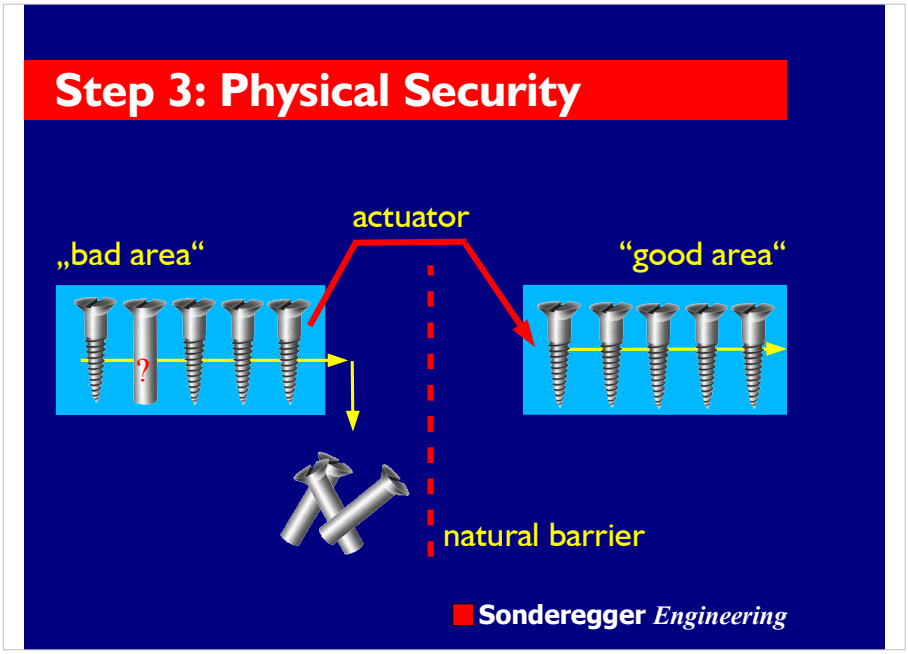


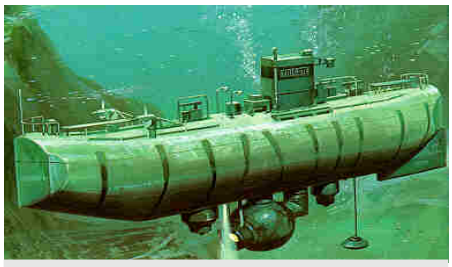
Figure 4

Physical Security:

Always suppose that 100% of manufactured parts have a defect before they pass the quality control device. Build a natural barrier to distinguish between the bad area and the good area (Figure 4). Only if the quality control device is working correctly, the good parts are moved to the good area. Otherwise, they are thrown out as having a defect.

All good parts are moved with an active external force, such as pressured airflow, or an electric manipulator.

Such a secure design is necessary, in case of of failure of an unexpected failure of the quality control device, which is -for whatever reason- not detectable. In such a case, a bad part cannot pass through the quality control since there is no active force.



This is not an everyday example of secure quality control. We hope you'll find it interesting nonetheless: The bathyscaphe is a deep water submarine used to explore the very lowest parts of the ocean. It is electrically powered. Once at the bottom, if the batteries or electrical system fail the best outcome would be for the sub to return to the surface. The designers made this outcome occur by holding the ballast in place with electromagnets. When power is lost, the ballast drops off automatically and the sub starts its ascent.

„We deliver only understandable quality control devices.

Because, our client needs to guarantee 100% defect-free products“

if it needs to be safer

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

Figure 5

Why making it robust:

The quality control device needs by definition a high reliability, otherwise it is worthless. High reliability can be reached through robust design. You need to consider the noise factors to increase robustness (vibration, dirt (Figure 5), manufacturing variation, and component deterioration).

Robustness needs to be addressed for each technology used: Mechanics, electronics, software and optics.

Mechanical robustness can be reached making all part as solid as possible: large diameters versus small ones; bold large wheels, instead of thin tiny wheels, etc.

Electrical robustness means transmission systems with low error rate. Electrical defects of switches and sensors need to be detectable.

Software robustness means testing software to see how effective it is at exception handling and recovery from operating systems crashes. Software robustness is the ability to tolerate exceptional input.

Optical systems are especially vulnerable for shift. The only solution that really works is fixation of the optical elements with glue.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

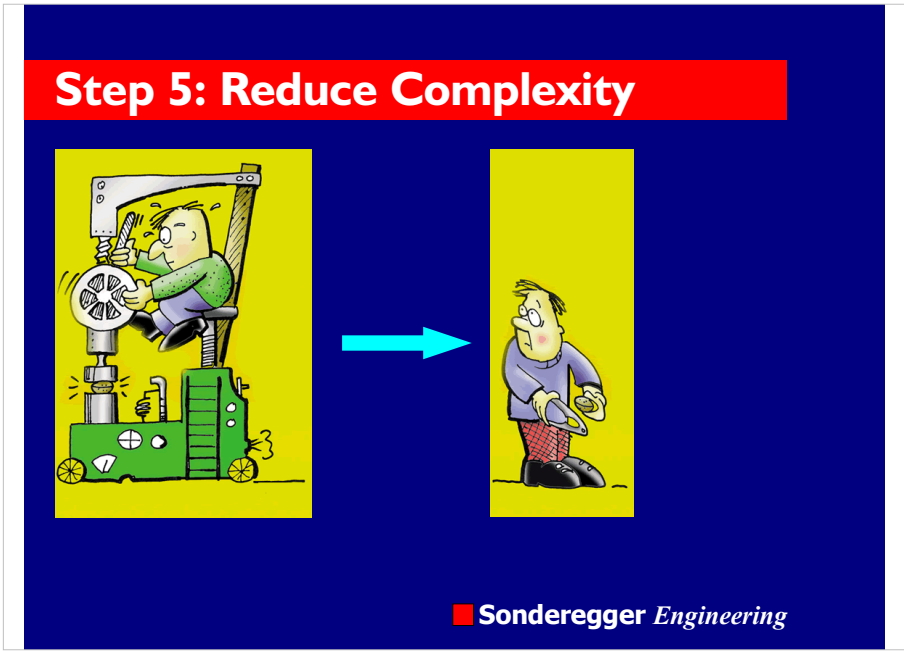


Figure 6

MURPHY'S LAW: "Anything that can go wrong, will go wrong!"

Reduce complexity

"Complexity is the worst enemy of security. Secure systems need to be simplified as much as possible. There is no replacement for simplicity" [Bruce Schneider, "Secrets and Lies"].

A mechanical design is less complex, if it needs less parts and has few interfaces (joints). An interface is where two parts can move to each other. Just looking at Figure 7, two nutcracker are shown, the old design has only 3 parts and one interface. Whereas the complex machinery on the left side needs numerous parts and interfaces. By common sense, we know, that the low-tech nutcracker is more reliable.

The same applies for computer code. You can measure the complexity of a function or method in the following way [MauriceDeBeijer,1992]. Start with one point for the existence of the function/method. Add one for every time a new variable is used. Add one for every decision point like IF, CASE, OR, AND, IIF, FOR, WHILE, SCAN, INLIST etc. The sum is the complexity of the function or method. To calculate the complexity of classes add the scores for each method and add one for every property.

Routines with a complexity of less than 25 are unlikely to contain bugs and if they do they are typically easy to fix. This is in part because less complex routines are easy to understand, easy to test and easy to debug. The opposite happens to routines with a complexity level greater than 100, they are much more likely to contain bugs.

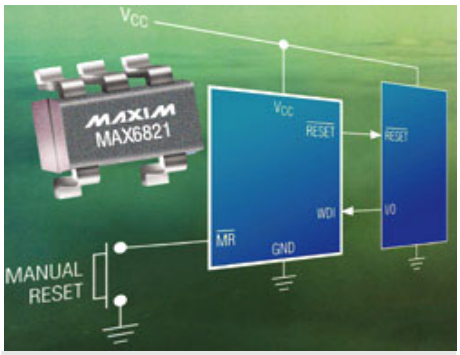
It is always worth looking at the designed equipment to see if they can be modified in such a way so that it would be impossible (or at least extremely difficult) to build it together wrong, called mistake-proofing.

```
PROCEDURE DisplayMessage && Score 1
LPARAMETERS tuName, tcMessage && Score 2
LOCAL lcName, lcMessage && Score 2

IF VARTYPE(tcMessage) = 'C' && Score 1
  lcMessage = tcMessage
ELSE && Score 1
  lcMessage = 'Hi there:'
ENDIF

DO CASE
CASE VARTYPE(tuName) = 'N' && Score 1
  lcName = LookUpName(tuName)
CASE VARTYPE(tuName) = 'C' && Score 1
  lcName = tuName
OTHERWISE && Score 1
  lcName = 'Stranger'
ENDCASE

WAIT WINDOW lcMessage + ' ' + lcName

RETURN
```

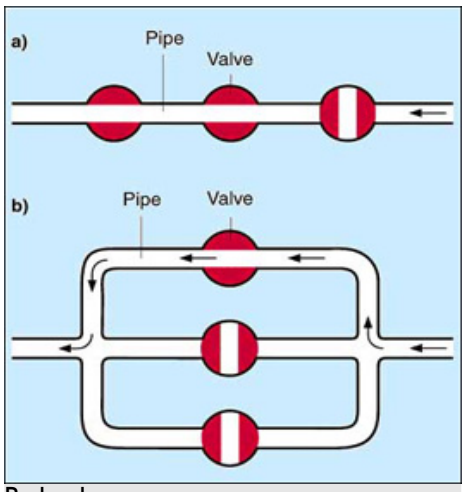
Listing 1
This procedure would score a total of 10.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

Figure 7



Integrated circuits features watchdog timer that detects code execution error and a manual reset input that allows for a reset without the power supply falling below the reset threshold.



Redundancy:
The multiple design of important technical systems is called redundancy.
Schematic diagram of redundancy for the closing function (a) and opening function (b) of valves in a pipe.
The idea is to duplicate the design so that if a fault occurs in one area, the whole system can continue to operate on the components that remain intact. This gives a massive boost to reliability. For example, if the probability of a failure in one path is 10%, the probability of the entire system failing is only 1%.

Watchdog

A watchdog is the typical hardware device, which handles recovery from absolute system failure. A quality control system always has the risk of intentional outwit by the staff.

A watchdog system is needed on each element which could be outwit.

Redundant information

Redundant elements like trigger pins prevent outwit of the control system. If the control system does not detect any errors produced by the redundant element for a certain period of time (for example 20 seconds), the system assumes that “somebody” manipulated the device.

Redundancy

Redundancy always means that two systems need to be built that have the same function, therefore doubling the cost of the qualtiy control device.
However, redundancy can easily be used for subsystems with almost no change to the cost.

Watchdog systems are less expensive than built-in redundancy.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

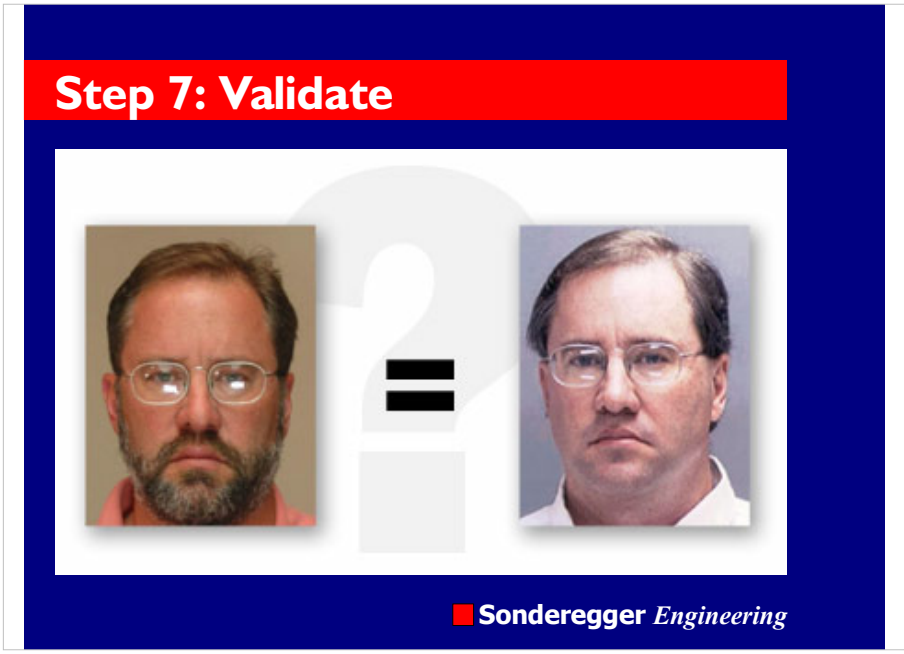
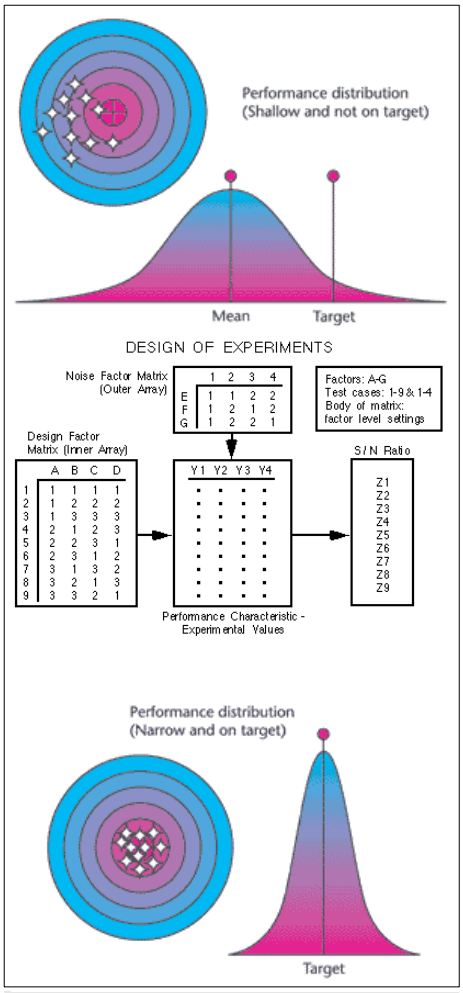


Figure 8



Design of experiment

Design for Six Sigma is about designing to be insensitive to variations. The quality control device should be challenged to discover how output changes as variables fluctuate within allowable limits. Whereas "Design of experiment" has become an essential tool for validation.

Validation

An important point of validation is how the control system would behave when it would fail itself.

Since we are here dealing with the detection of rare cases, the probability of a faulty part is often much smaller than 1%. It makes therefore sense to test the quality control device with good and bad samples which are close to the borderline of being faulty.

It is important to use original faulty products and not "artificially" manufactured specimens. Start to collect faulty parts at the beginning of the project is good practice. We cannot stress this point strong enough, since often there are not enough "bad" samples when validating the system.

It also makes sense to define test scenarios deducted from the previous conducted Failure Mode Effect Analysis (FMEA) to test the abnormal behaviour of the quality control device. It is worthwhile to imagine scenarios where someone tries actively to fool the device.

Because of ageing and wear during use, it is obvious that the system needs periodical control if the system still works within the limits (recalibration). If possible one uses the same samples as for validation.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

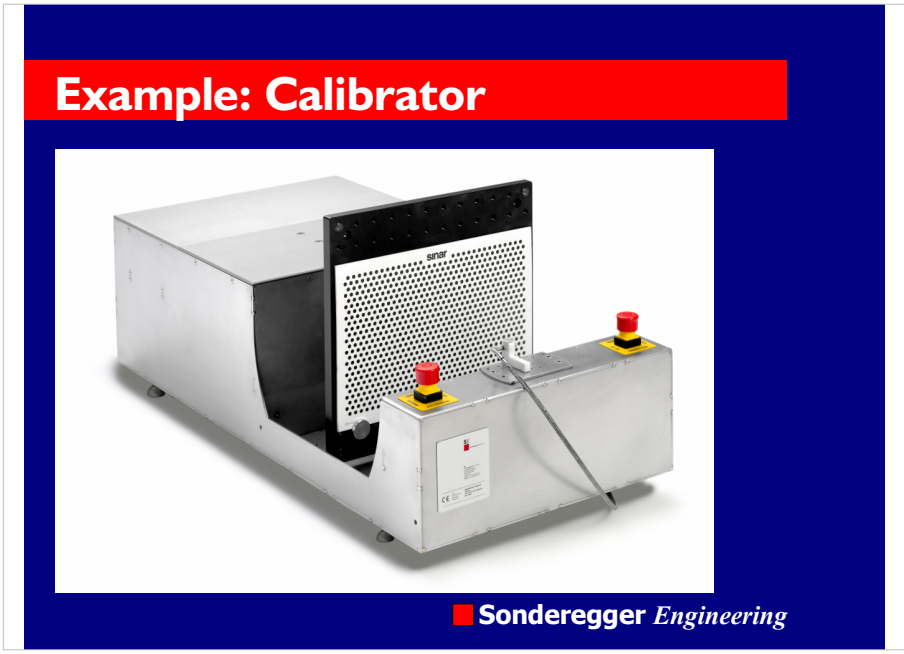
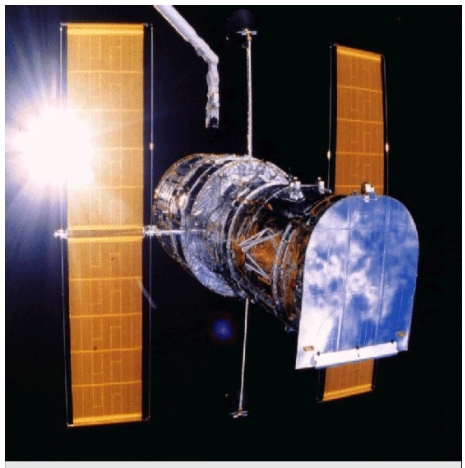


Figure 9



The Hubble Telescope disaster

The mirror's manufacturer had finished the final polishing in 1981. As the telescopes 2.4 meter primary mirror was being polished, and unrecognised 1.308 millimetre error in the structure of a device used to monitor the process caused technicians to give the mirror an exquisitely smooth surface with a grossly inaccurate shape. The result is the "spherical aberration" that now bathes the stars in fuzz whenever Hubble tries to look at them. The culprit device was called the reflective null corrector.
The manufacturer could have corrected the error before it was too late, the optical team managed to dismiss the warning signs. The first indication of trouble appeared as the polishing team was assembling the null corrector. As they tried to move the errant lens into position, they found that the lens adjustment screws would not turn far enough. The report concludes that the opticians were probably taking incorrect readings from a high-precision measuring rod. But at the time, they did not try to find out what was wrong. Instead, they simply added some 1.3 millimetre thick spacers to extend the lens range of motion. Once they were done, they treated this null corrector as being "certified" correct.
Just these kinds of errors can be avoided by a systematic approach.

Example of a calibration unit

Step 1: What makes the client angry?

Figure 10 shows a calibrator which is used to calibrate optical elements for surgery. The important feature is the precise distance at the moment of measurement. The calibration of the optical element wrong when the distance is not correct read out (see story of the Hubble telescope on the right).

Step 2: Physical Reference:

"Absolute Zero" is the surface of the optical unit to be calibrated (Please note: The absolute zero is not part of the calibrator itself). The absolute zero is found during a initialisation procedure. It makes the calibration independent of any changes of the calibrator with time.

Step 4: Robust Design:

Oversized linear actuator with positioning precision 10 times higher than needed. USB interface instead of RS 232.

Step 5: Reduce Complexity:

Soldered case instead of screwed parts (one piece instead of about 30 pieces). Reducing amount of possible software commands to the absolute minimum.

Step 6: Watchdog & Redundancy:

All software related functions have timers to check for time-outs. A redundant optical ruler with reading capabilities 100 times better than demanded.

Step 7: Verification and Validation:

Scenario protocols for function checking.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

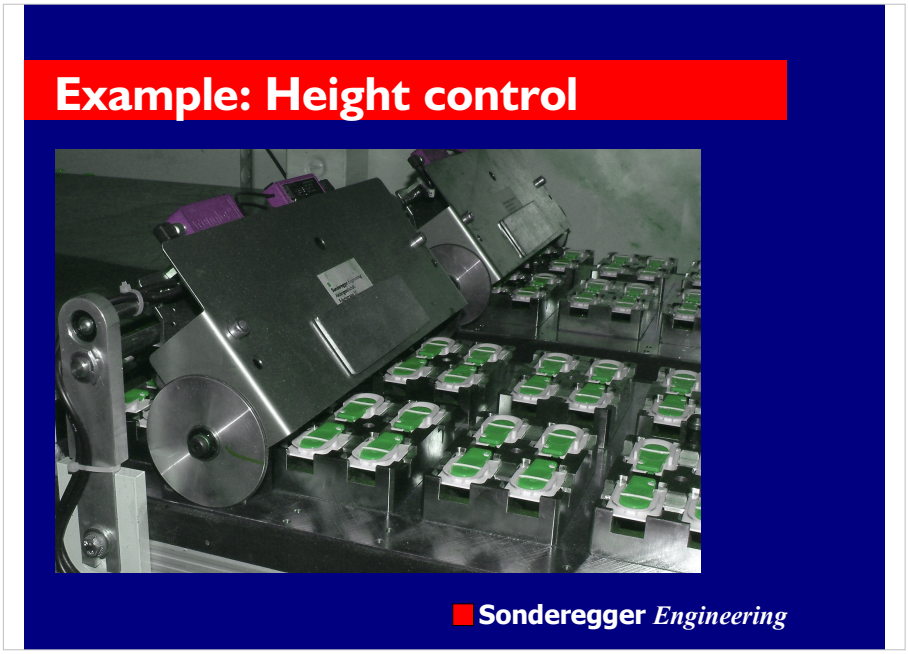


Figure 10

Example of hight control of an IN-LINE quality control device

Step 1: What makes the client angry?

Figure 11 shows parts which are used for drink blisters. If one of them is 1/10mm too high, it blocks the filling machine.

Step 2: Physical Reference:

Definition of an "absolute height" which is the centre of the wheels.

Step 3: Phyiscal Security:

A laser beam to measure height with a receiver on the opposite side. Interrupted laser beam means faulty part. Therefore 100% reject in case of system failure (shift, broken laser etc.).

Step 4: Robust Design:

Vibration were a major problem: Making the quality control device heavier suppressed parts of the vibration.

Step 5: Reduce complexity:

Reducing the amount of parts.

Step 6: Watchdog & Redundancy:

Two control pins are integrated in the carrier creating two redundant errors per carrier.

Step 7: Verification and Validation:

Scenario protocols (Design of Experiment) for function checking.

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

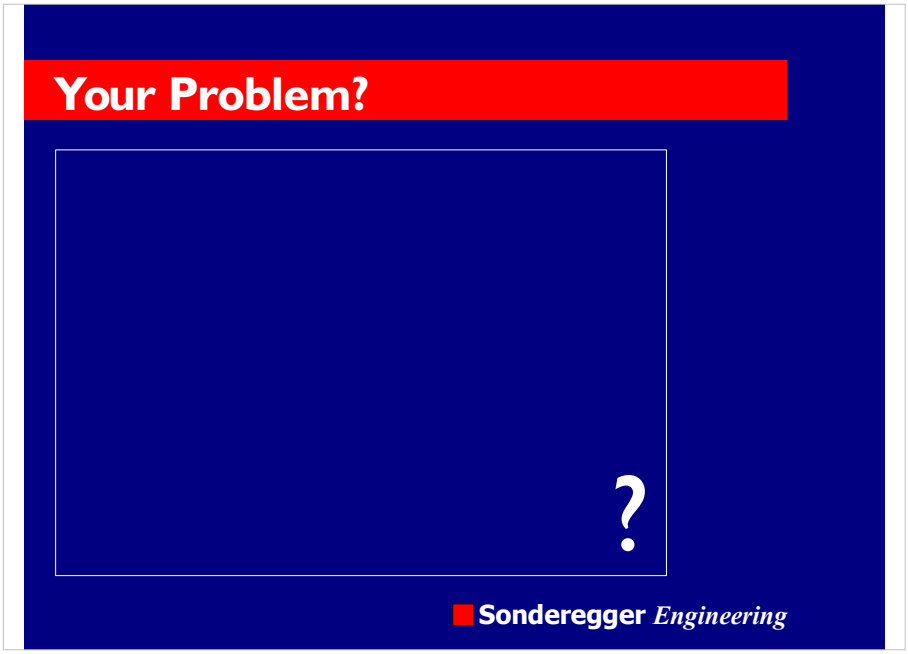


Figure 11

Solution:

Step 1: What makes clients angry?

Step 2: Physical Reference:

Step 3: Physical Security:

Step 4: Robust Design:

Step 5: Reduce complexity:

Step 6: Watchdog:

Step 7: Validation:

if it needs to be safer

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch

Figure 12

Conclusion

- We thoroughly believe you need to use the presented approach, if you really need to reach the goals of 6 Sigma, i.e. 99.99966% defect-free parts.

Feel free to call us:
Dr. eng. Marcel Sonderegger
+41 (52) 622 22 55

Sonderegger *Engineering*
Aktiengesellschaft
Fulachstrasse 30
8200 Schaffhausen
Switzerland
Tel: +41 (52) 622 22 55
Fax: +41 (52) 622 22 56
info@sonderegger-engineering.ch
www.sonderegger-engineering.ch