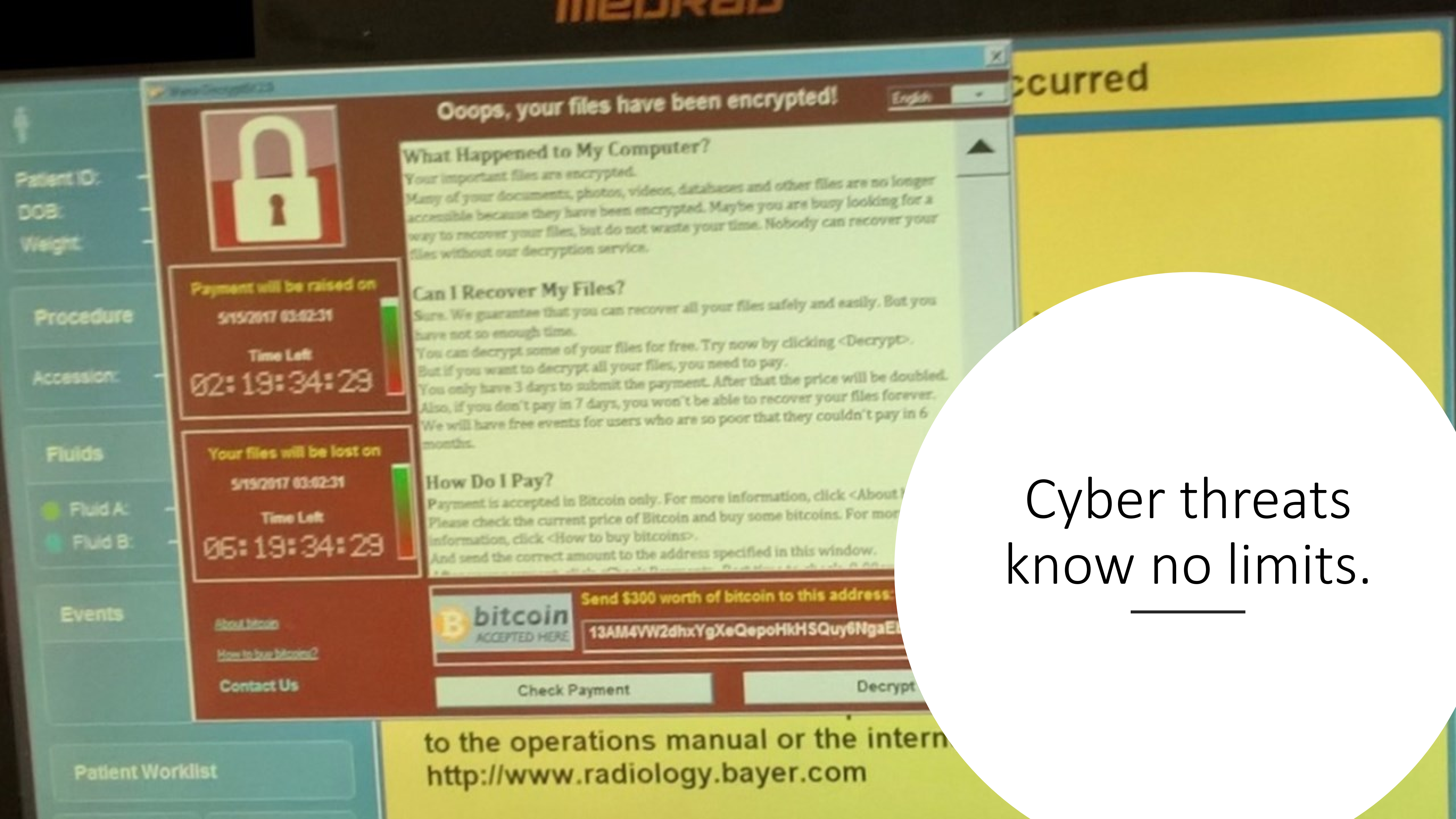
Assurance of Biomedical Systems

Dr. Roberto Gallo

August 2022

How much risk is acceptable when lives are in the balance?



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29

Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer
accessible because they have been encrypted. Maybe you are busy looking for a
way to recover your files, but do not waste your time. Nobody can recover your
files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you
have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6
months.

How Do I Pay?

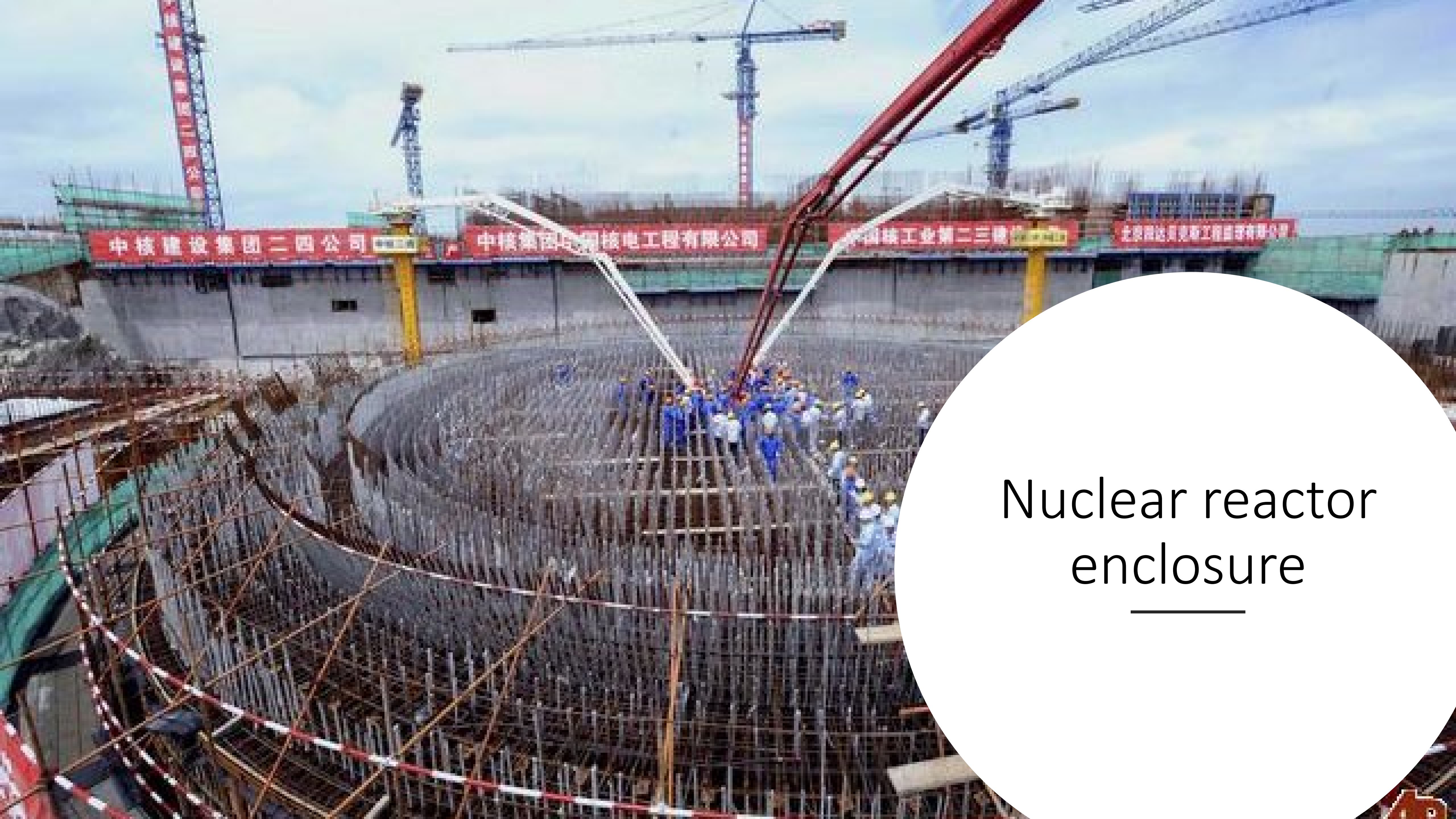
Payment is accepted in Bitcoin only. For more information, click <About
Please check the current price of Bitcoin and buy some bitcoins. For mor
information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaE

to the operations manual or the intern
http://www.radiology.bayer.com

Cyber threats know no limits.

We better rethink!



Nuclear reactor enclosure

Popular homes

The greatest difference between the final build results is trustworthiness.

The collapse of a house is acceptable under many circumstances – a violent tornado (EF5), for instance.

In the other hand, a collapsing nuclear reactor must resist not only heavy “acts of God”, but also acts of adversaries!

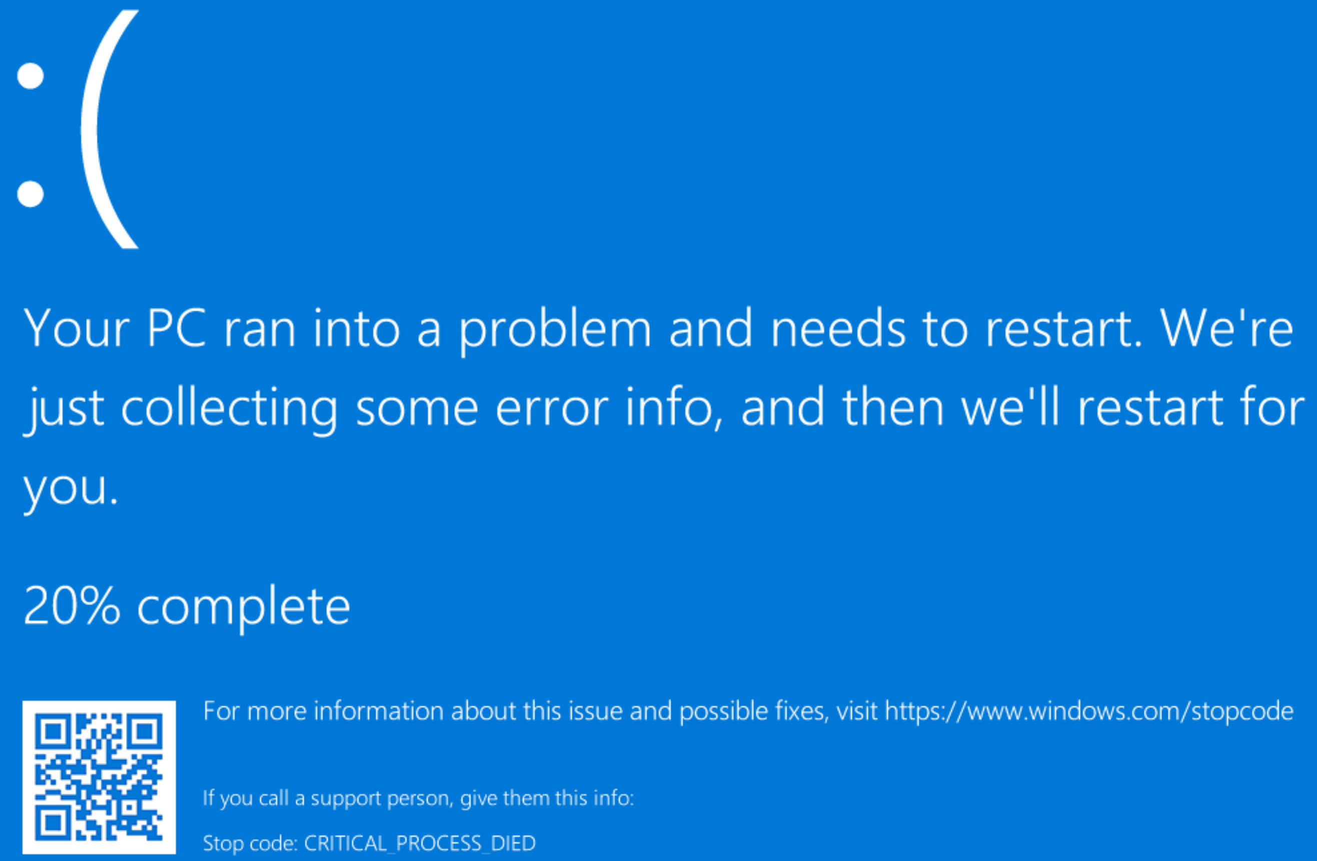
Essentially using the same types of resources…

But what happens when unknown unknows are in the play?

Engineering objectives changes it all.

ICT, ICS, MIL, Med?

Item	ICT (TIC)	ICS (SCADA)	MIL, Avionics	Biomedical
Operation time	1 to 5 years	10 a 20 years	35+	1 to 10
Attack impact	Information assets	Physical sites, limited kinetic damage, life threat.	Lethal, destruction of critical infrastructure	Life threat, lethal
Reversibility, contention	High	Variable	None	None
Risk management strategy	Economic impact	Economic impact, environmental, regulatory	Unacceptable risks, unknown unknowns	Economic impact, regulatory
Renew cycles	Months, years	Years, decades	Months to multiple decades	Years
Development strategy	TTM, features	Resilience	Survival, degraded operation	Resilience, survival



:(

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

Still…

Biomedical systems are developed with ICT methodologies

Quality cannot be added after a device is made

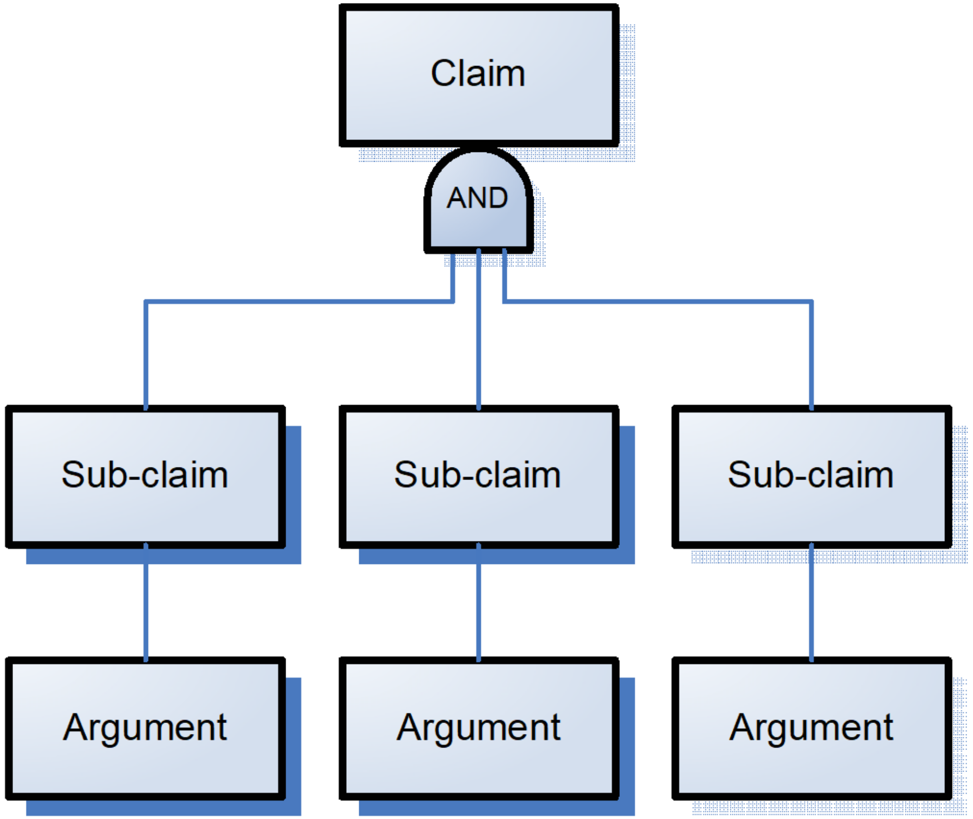
Must be there at the conception

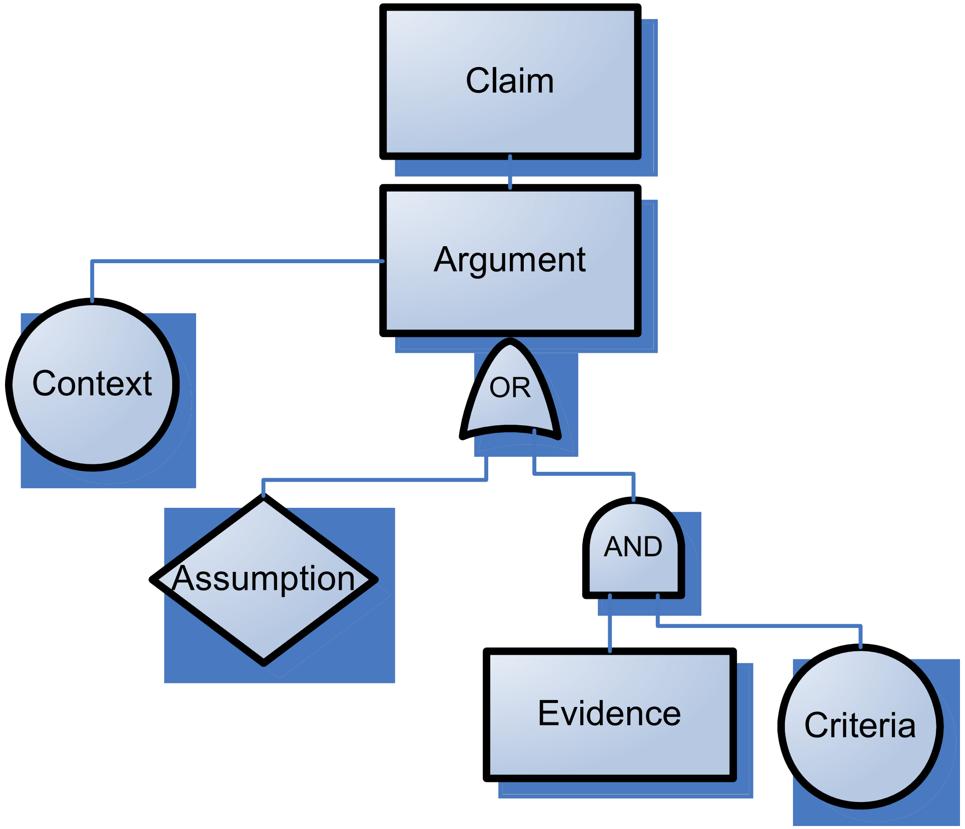
Common medical device standards

Standard	Name
ISO 13485	Medical devices — Quality management systems — Requirements for regulatory purposes
ISO 14791	Medical devices — Application of risk management to medical devices
IEC 62304	Medical device software — Software life cycle processes
IEC 80001-1	Safety, effectiveness and security in the implementation and use for connected medical devices or connected health software — Part 1: Application of risk management

© AP

Assurace Cases: Trustwortyness Enablers





Assurance case benefits

Makes clear to the R&D team what business logic and cyber security properties to be achieved, to what degree of certainty

Allows for degraded operation of non vital features

Handle unknow unknowns naturally – just revaluate the assurance three

Can handle both stochastic (“acts of God”) and adversarial events

Risk analysis and Assurance Cases are different sides of the same coin. Risk analysis allows for concentrating efforts in know issues. Assurance Case helps designing the solution.

QA

Dr. Roberto Gallo

<gallo@kryptus.com>