

Using a peer-to-peer overlay network to protect SCADA traffic

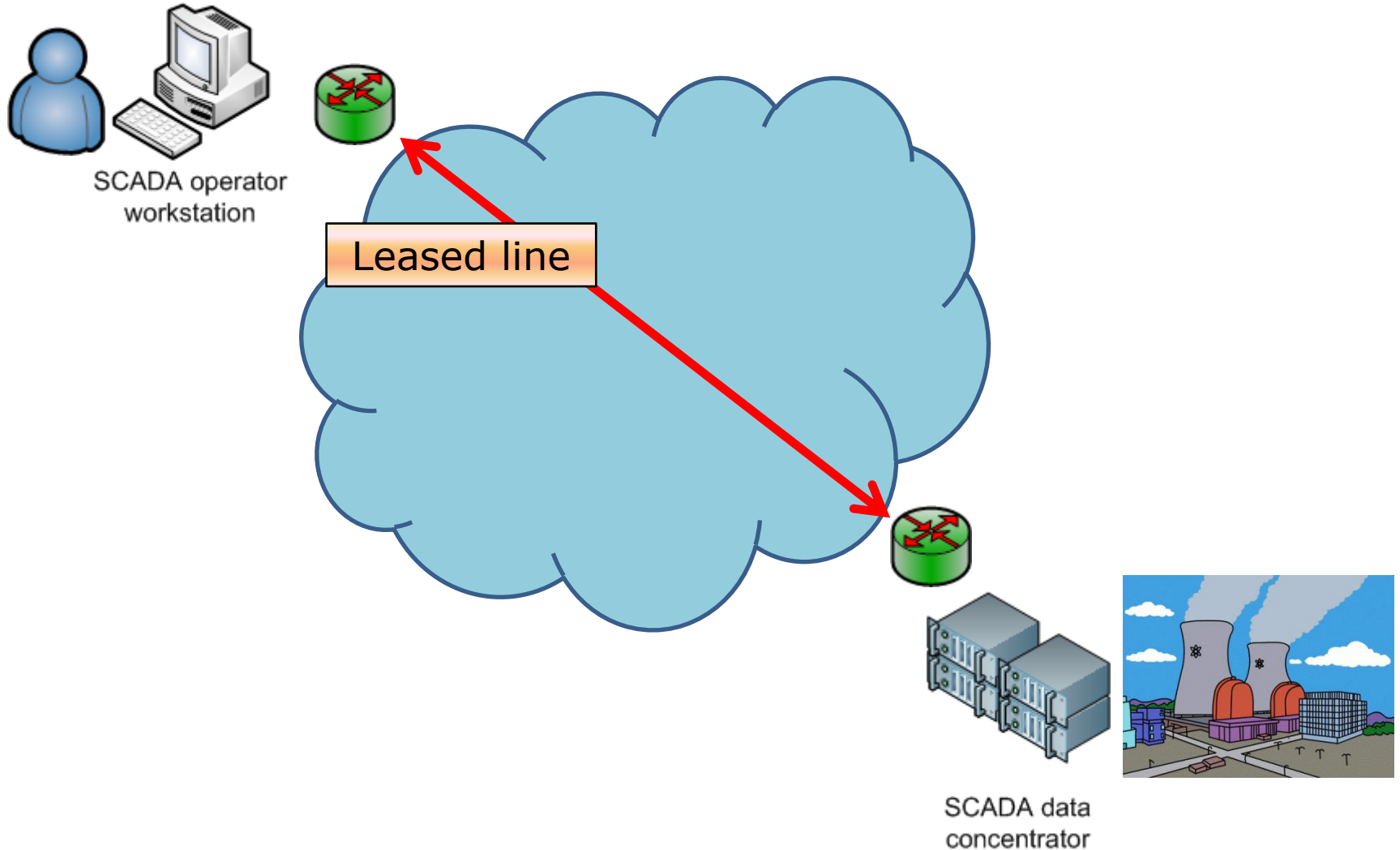
INSPIRE – 2nd Workshop
Rome, January 21, 2011

Marcello Antonucci - Selex Sistemi Integrati



Daniel Germanus - Technische Universität Darmstadt

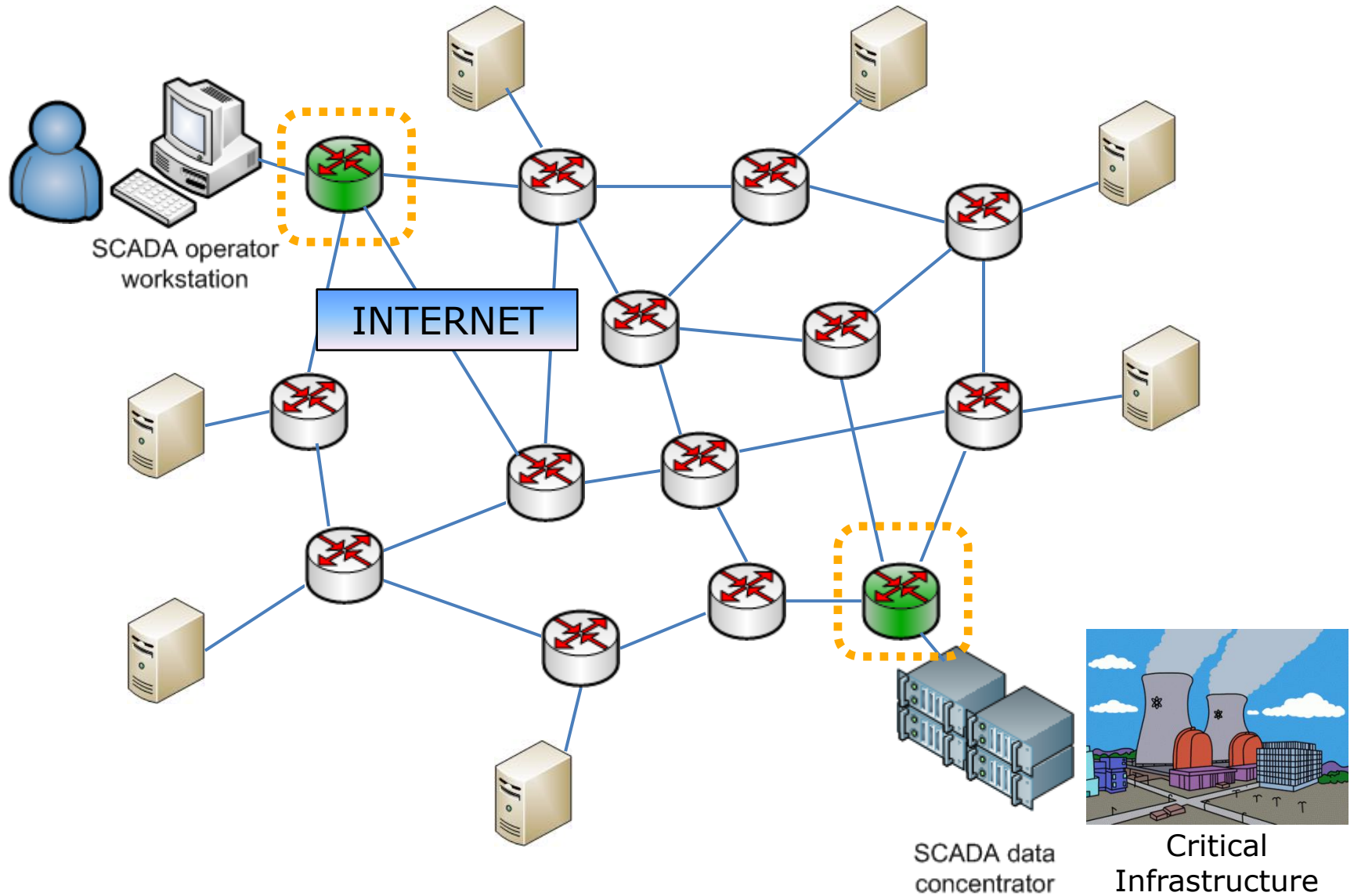
Wide Area connection



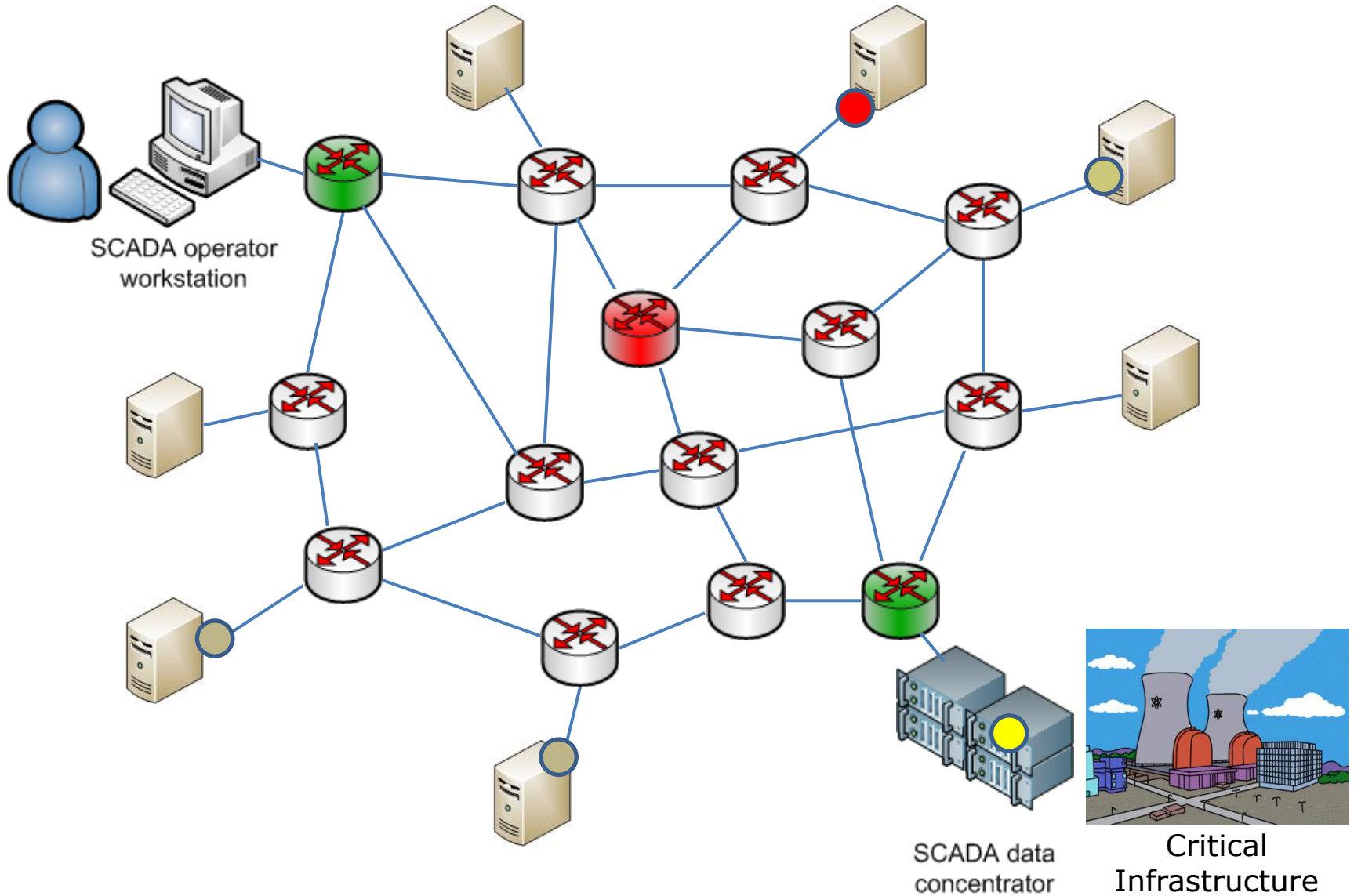
Wide Area connection

I N S P I R E

EC Grant Agreement n. 225553



Hacking a router



Untrusted routers

Pakistan and India do not trust much on each other.

Pakistan has a CI made by the Chinese, and to be monitored from China

They use an Internet connection provided by a world-leader ISP

The ISP signs a good contract with India, to get discount price connections in that area

Now Pakistani secrets pass through routers in India.



Risks at a router

Troubles that involve a router include:

1. Shut down of the router
2. Filtering out of the SCADA traffic
3. Wrong routing rules
4. Link saturation
5. SCADA traffic alteration

Getting control of a router, an attacker might:

1. Shut down the router
2. Filter out SCADA traffic
3. Set wrong routing rules
4. Saturate a link
5. Alter the SCADA traffic (change the content of the packets)

**No Internet
self-healing
for these**

Getting control of a router, an attacker might:

1. Shut down the router
2. Filter out SCADA traffic
3. Set wrong routing rules
4. Saturate a link
5. Alter the SCADA traffic (change the content of the packets)

**Do not
even require
an attacker**

Getting control of a router, an attacker might:

1. Shut down the router
2. Filter out SCADA traffic
3. Set wrong routing rules
4. Saturate a link
5. Alter the SCADA traffic (change the content of the packets)

**No automatic
activation
of backup link**



I N S P I R E

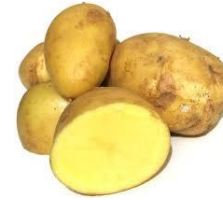
EC Grant Agreement n. 225553

THEN WHAT ?

a childish game

I N S P I R E

EC Grant Agreement n. 225553

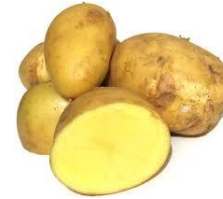


a childish game

I N S

EGGPLANT!

ONION!



ZUCCHINI!



POTATO!



CARROT!



a childish game

I N S P I R E

EC Grant Agreement n. 225553





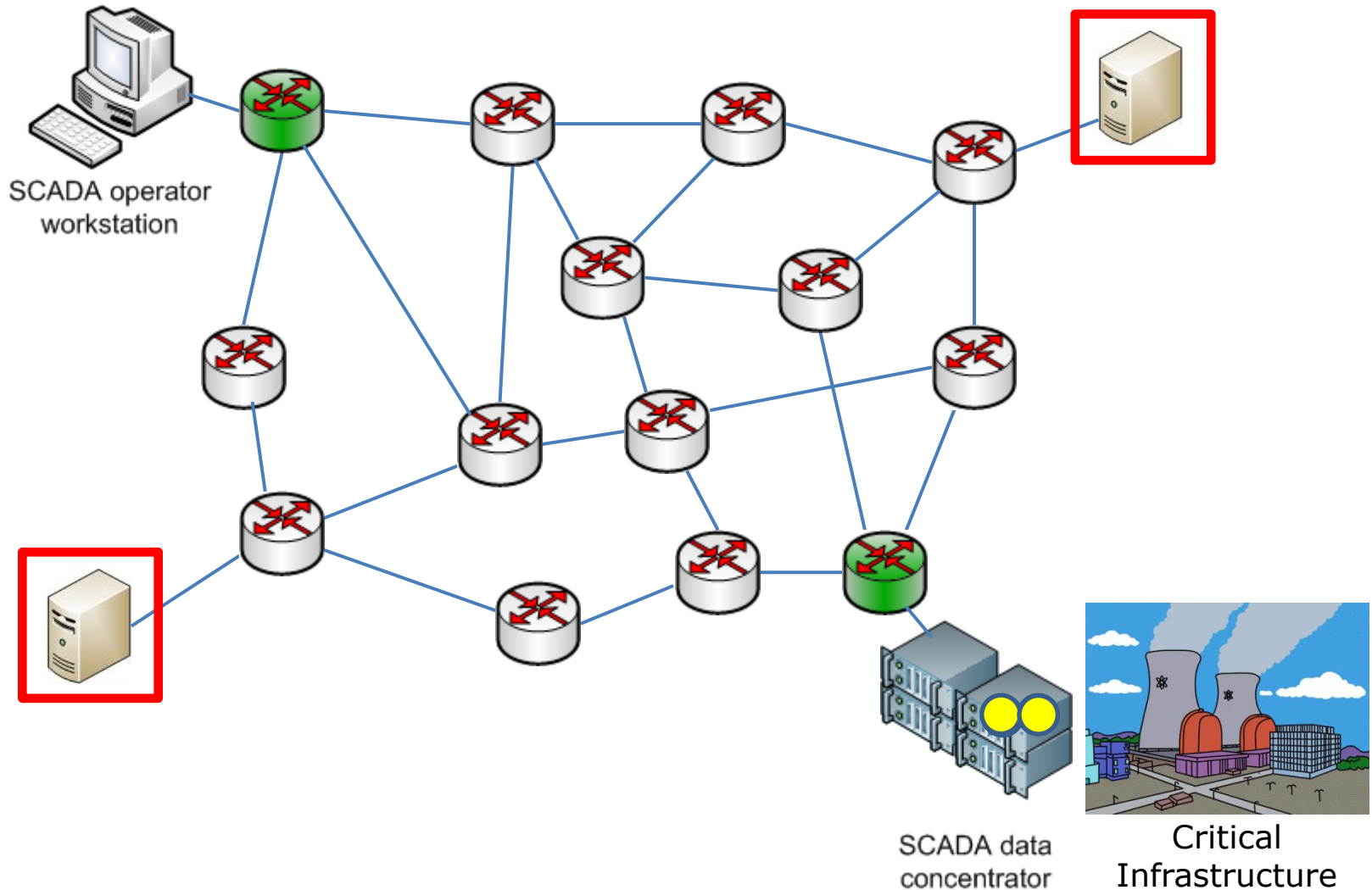
Application to the network

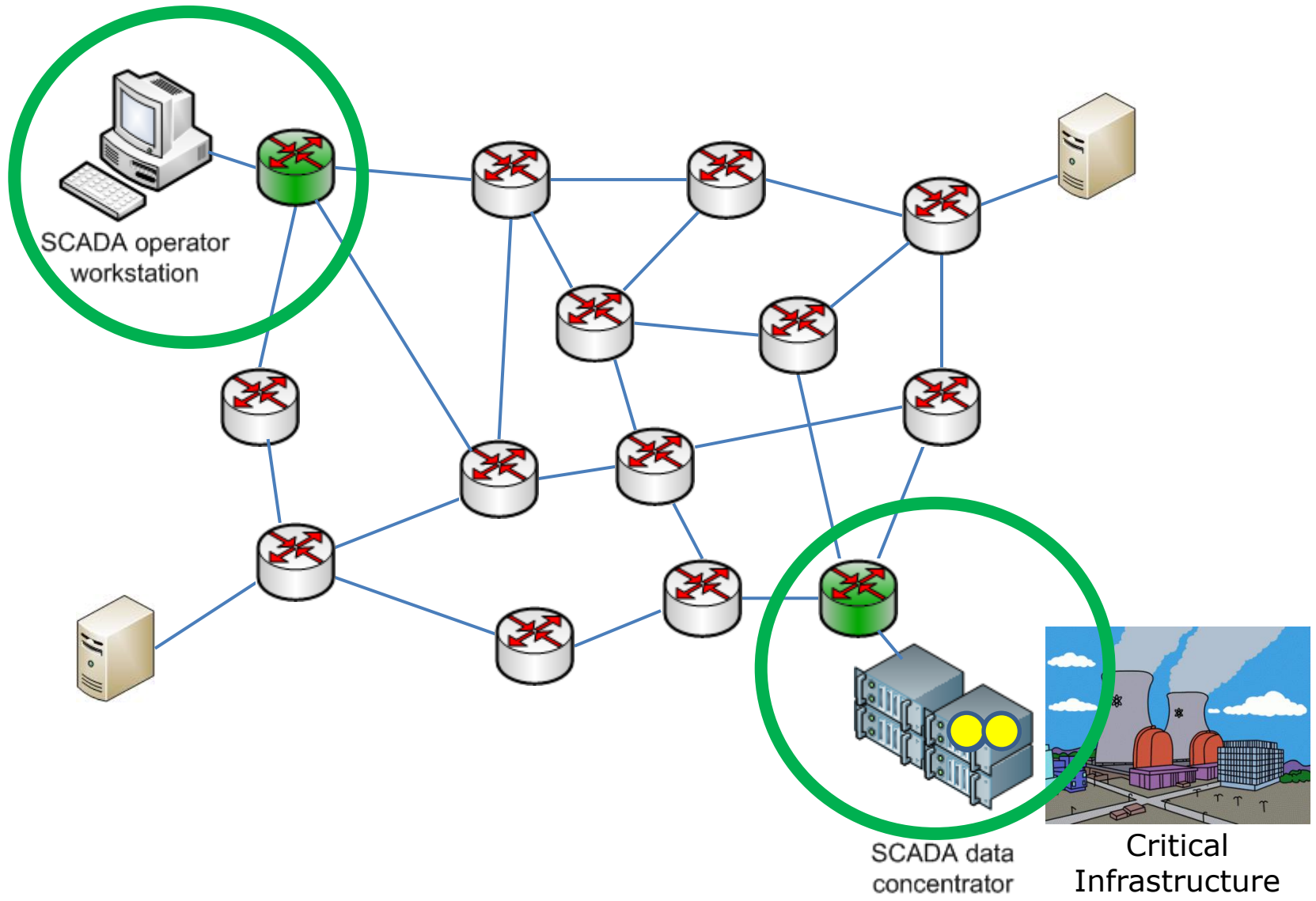


I N S P I R E

EC Grant Agreement n. 225553







P2P Technology zoom-in

- P2P Technology is complex
- Its use for SCADA has been a matter of research in INSPIRE
- Partner TUD will report about that in the next presentation

In summary

1. SCADA systems operating over the Internet are at risk
2. The risk is extremely high if those SCADA systems operate critical infrastructures
3. Besides well known issues for the endpoints (viruses, bad passwords), it is often neglected that troubles can come from intermediate routers
4. Peer to peer technology can help reduce this risk
5. We will see in the afternoon a demonstration of an example of the protection of a SCADA system using P2P.



End of the presentation



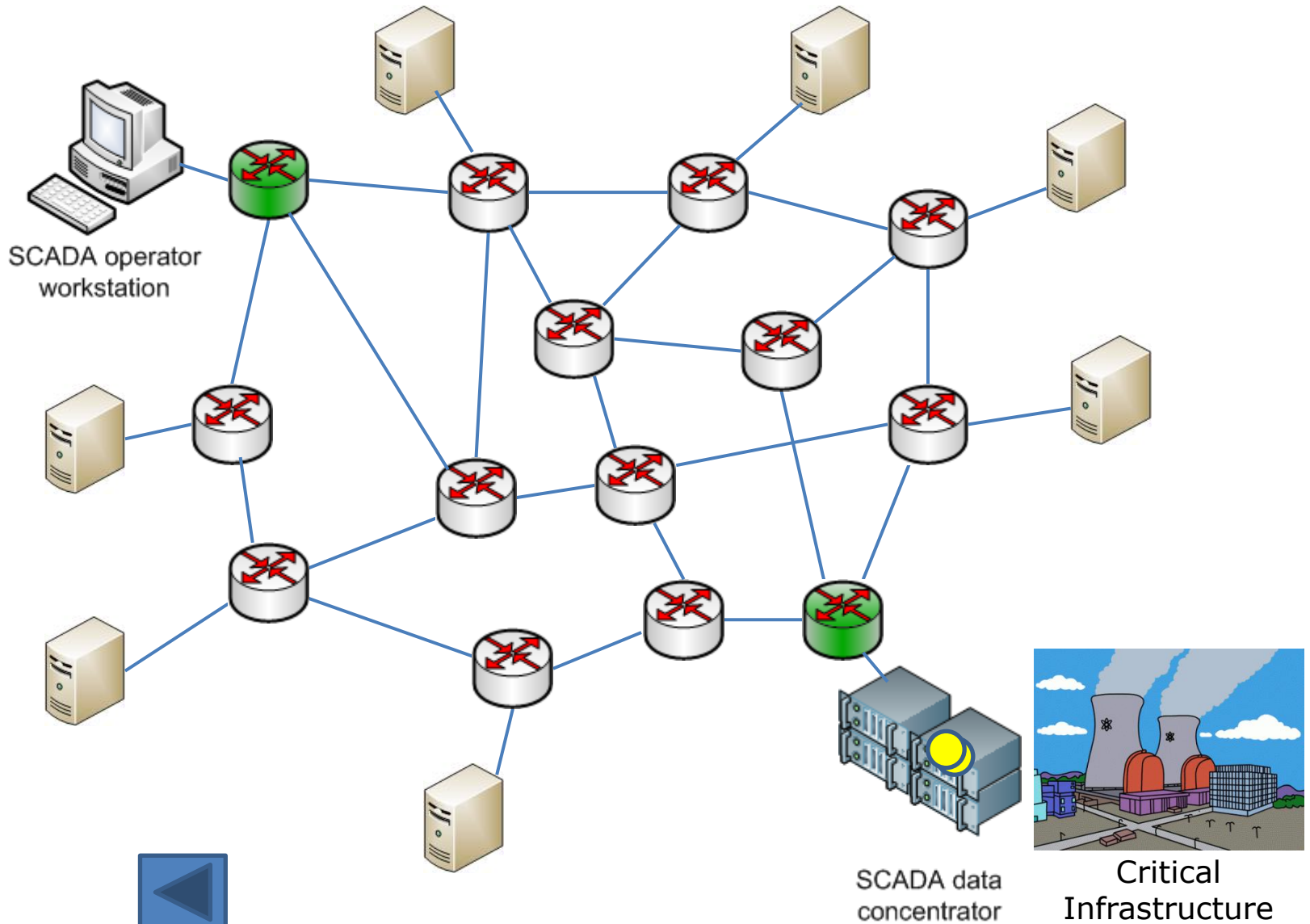
I N S P I R E

EC Grant Agreement n. 225553

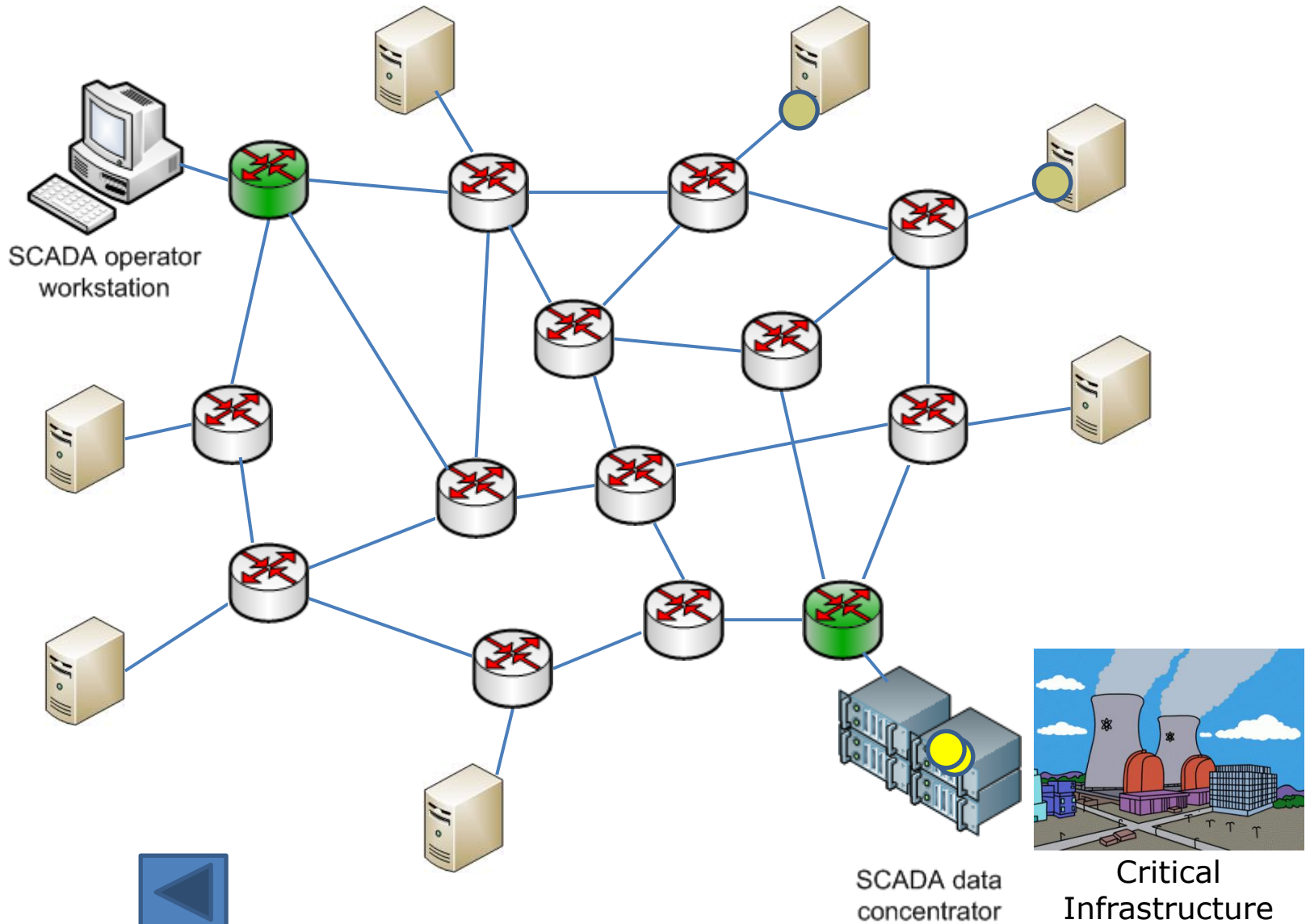
- Time for questions in the afternoon
- Post-event info:
 - fmargaresi@selex-si.com
 - germanus@cs.tu-darmstadt.de

Thank you for your attention

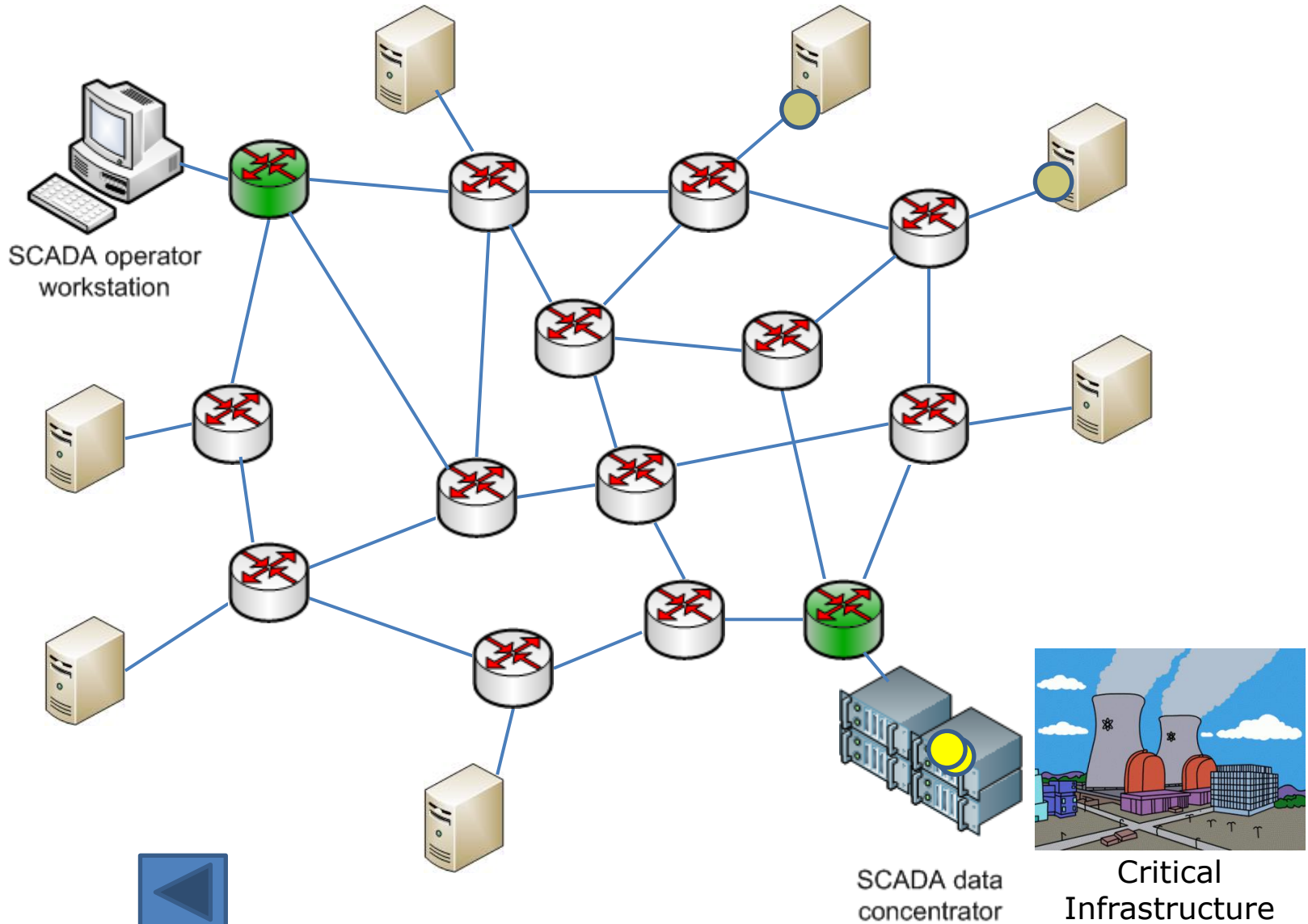
Shutdown of the router



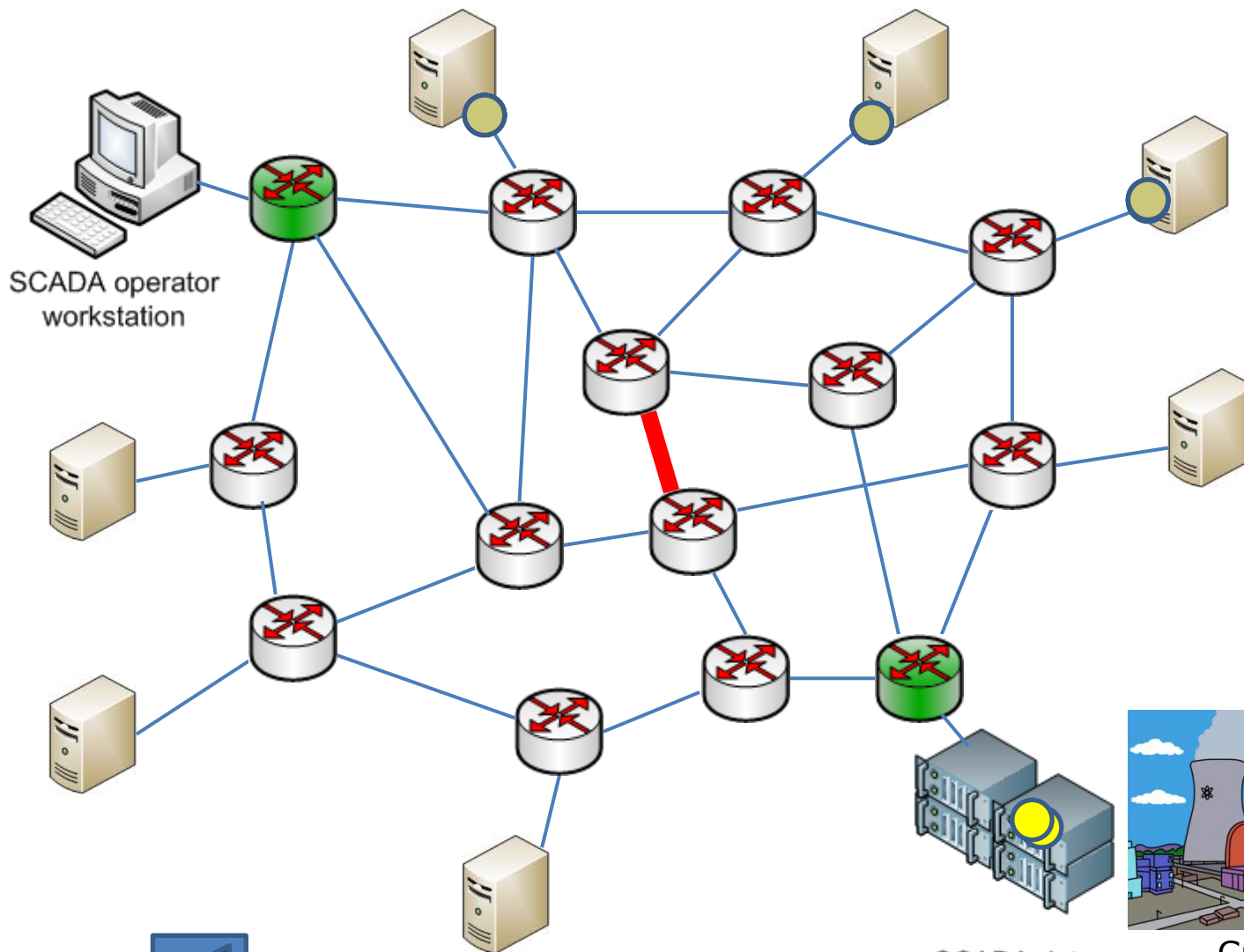
Filtering out SCADA packets



Wrong routing rules

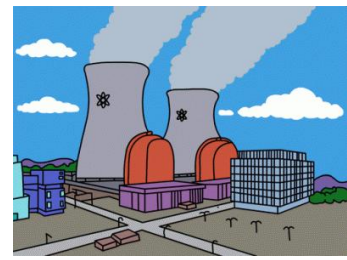


Link congestion



SCADA operator workstation

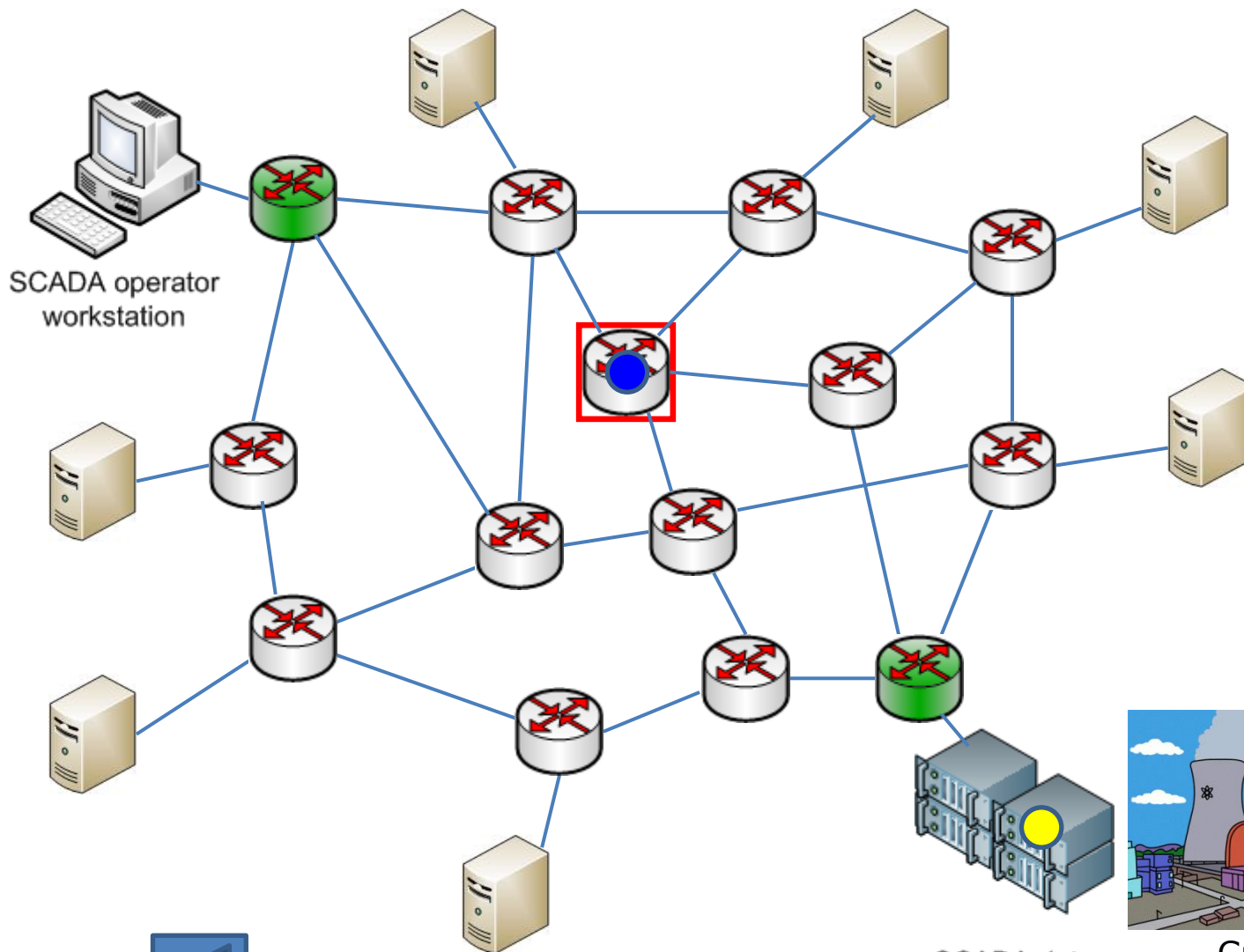
SCADA data concentrator



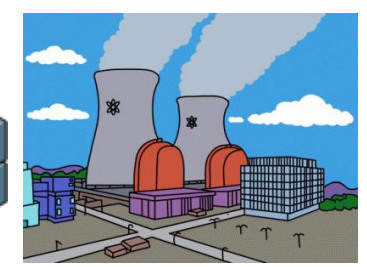
Critical Infrastructure



Data alteration



SCADA data concentrator



Critical Infrastructure

