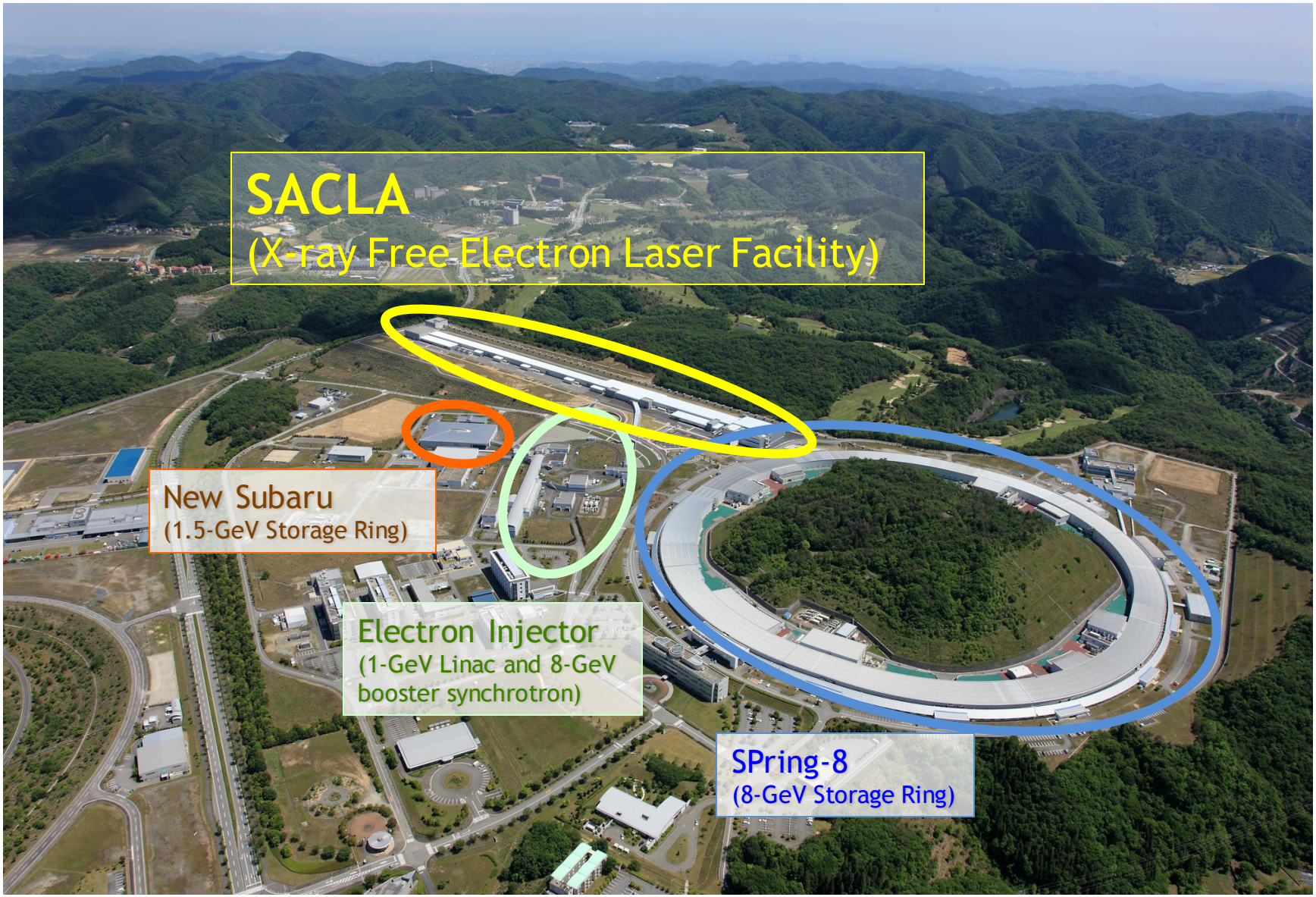
DAQ control system for multi-beamline simultaneous experiments at SACLA

Takashi SUGIMOTO

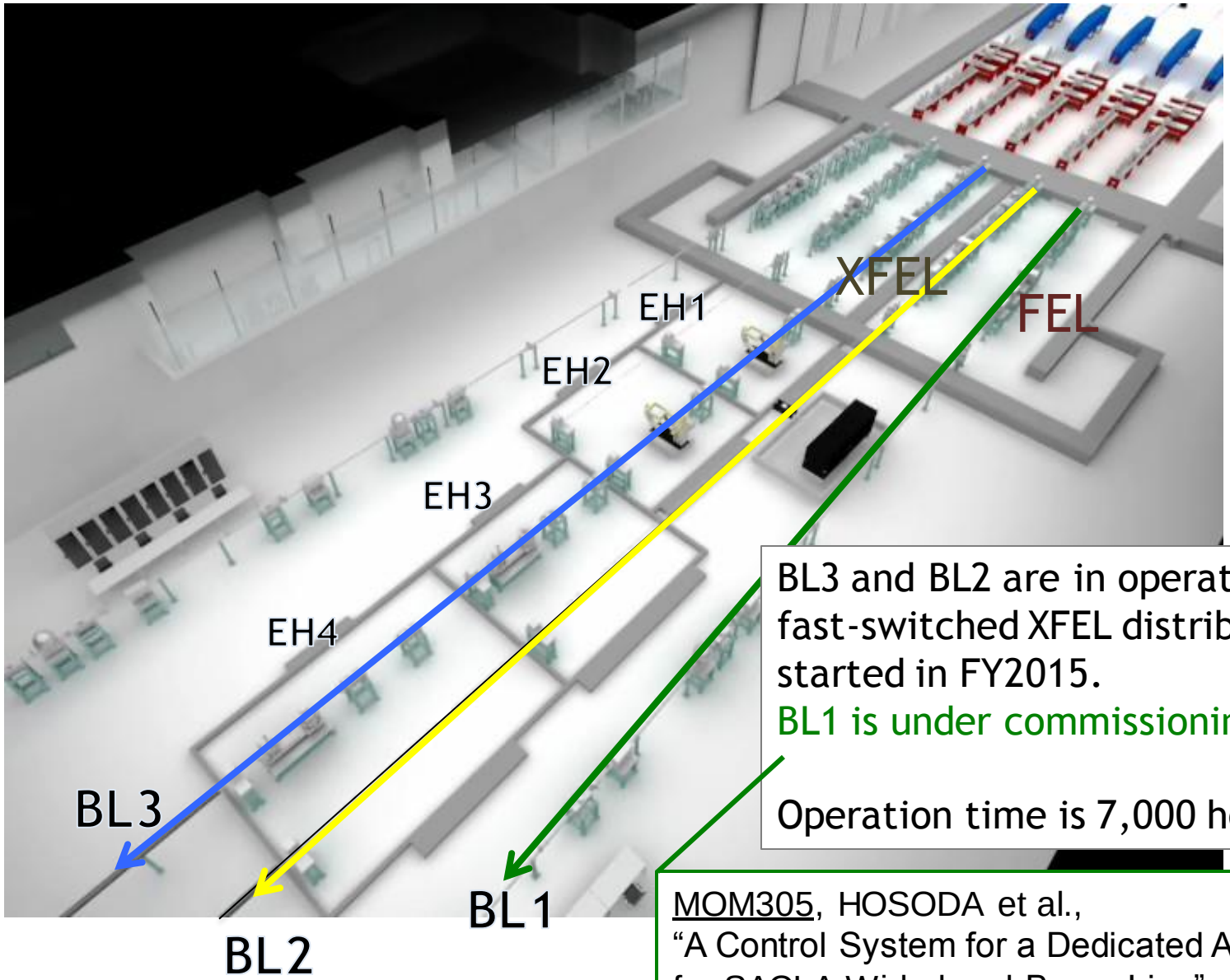
Japan Synchrotron Radiation Research Institute
(JASRI/SPring-8)

SPring-8 and SACLA

SPring-8: Light source complex



SACLA Beamlines



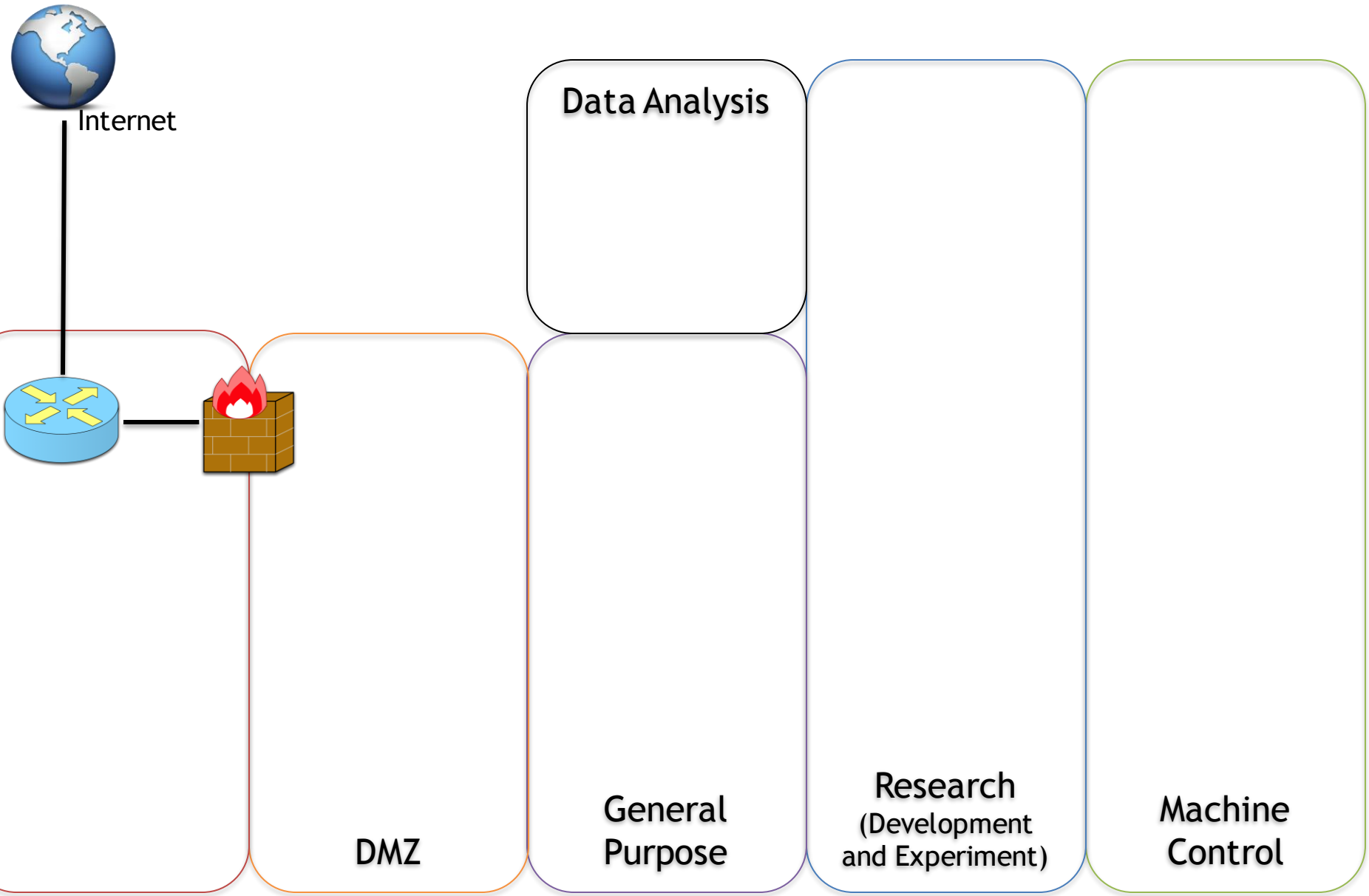
BL3 and BL2 are in operation. BL3/BL2 fast-switched XFEL distribution has just started in FY2015.
BL1 is under commissioning.

Operation time is 7,000 hour/year.

MOM305, HOSODA et al.,
"A Control System for a Dedicated Accelerator for SACLA Wide-band Beam Line"

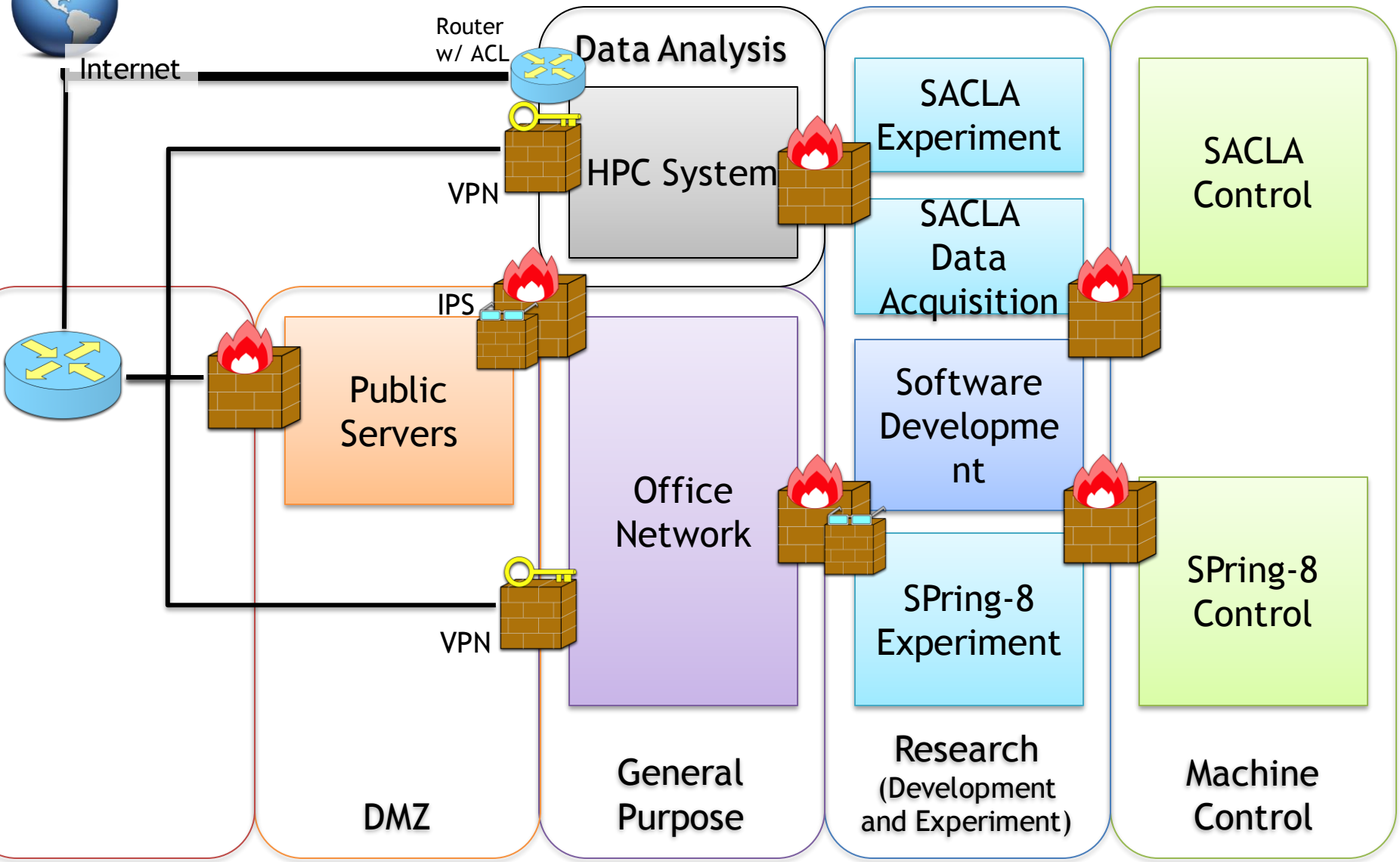
Overview of SPring-8 Campus Network

SPring-8 Campus Network



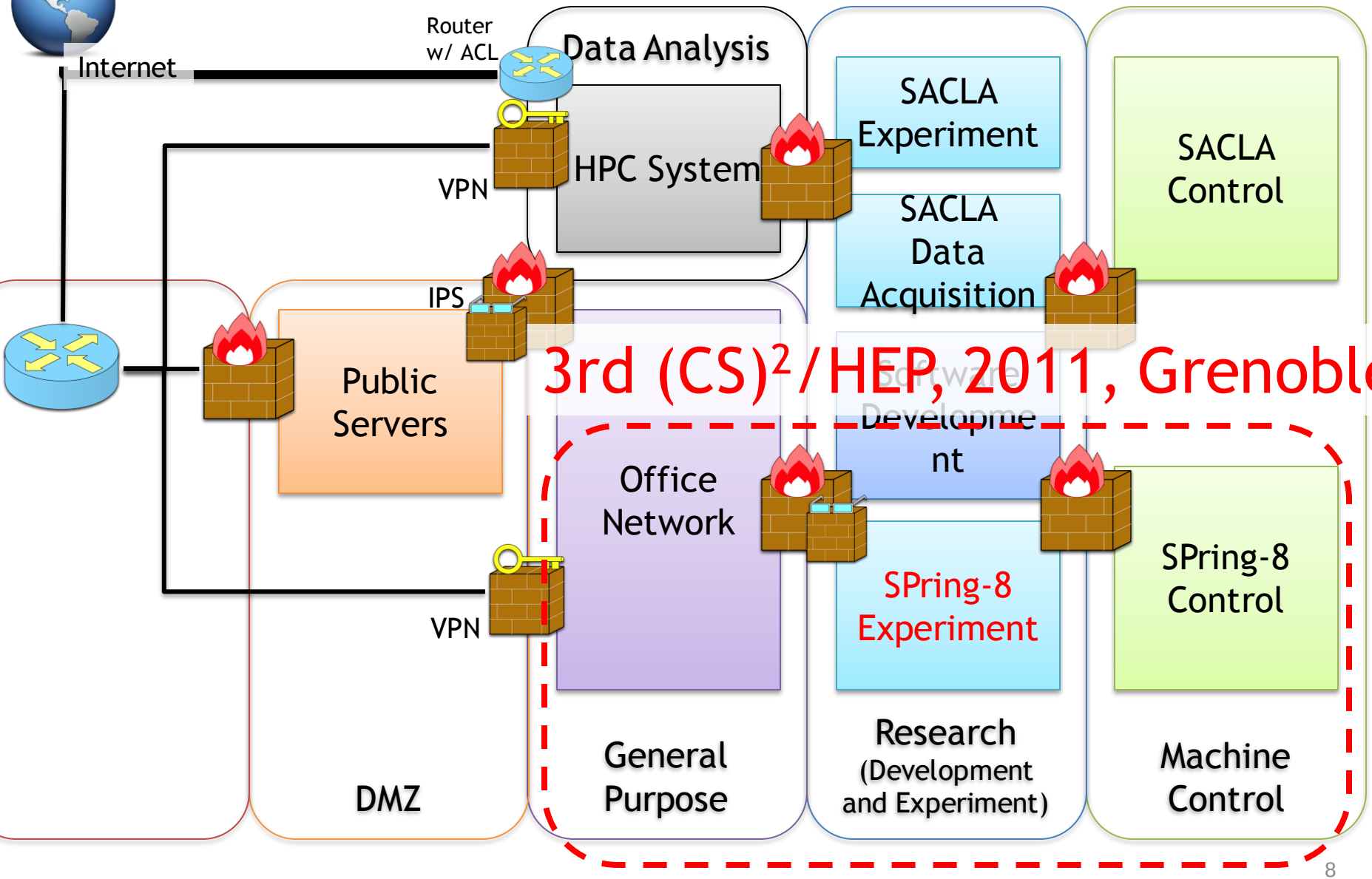
SPring-8 Campus Network

Defense-in-depth oriented network system (2010-)



SPring-8 Campus Network

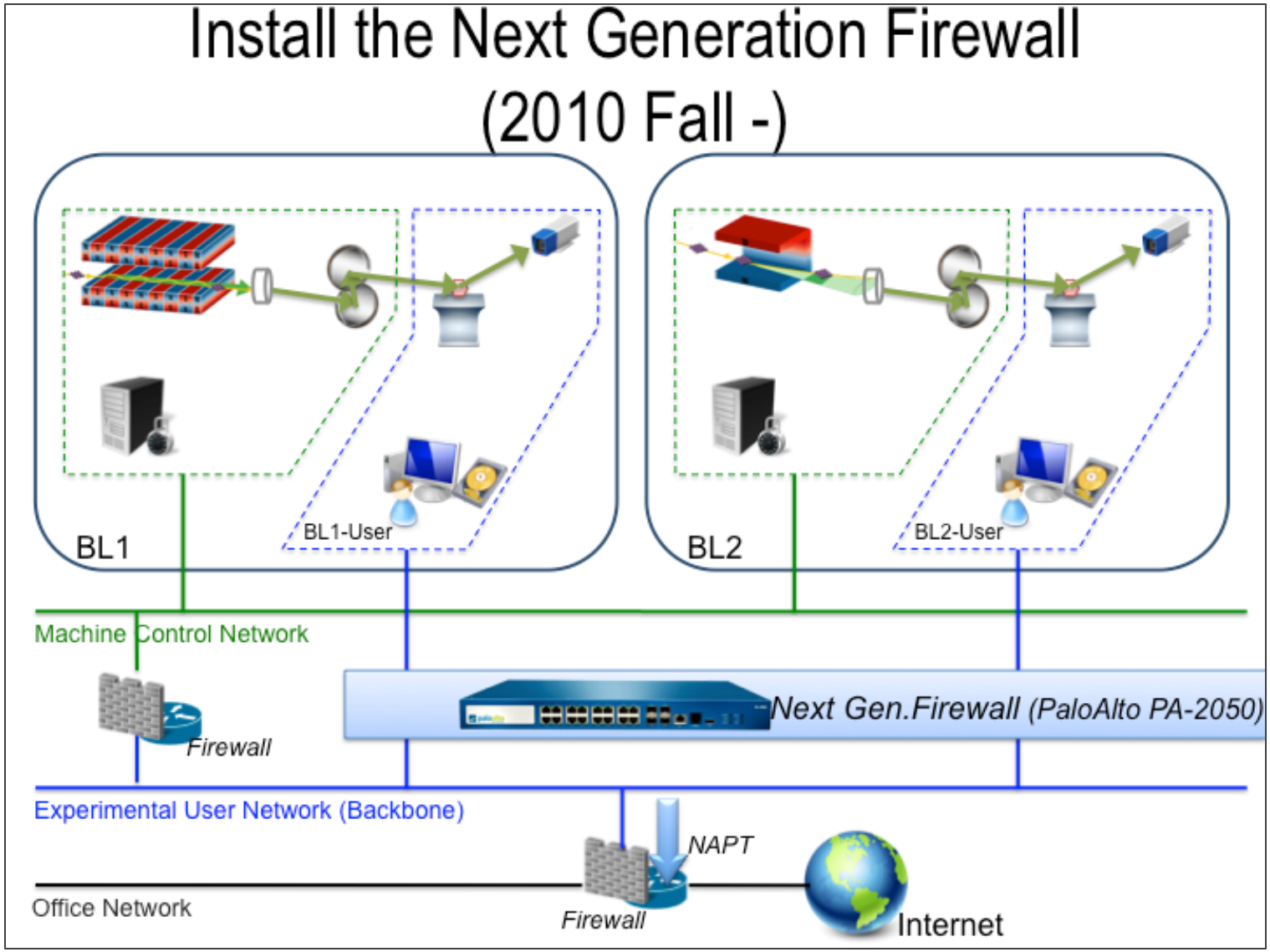
Defense-in-depth oriented network system (2010-)



3rd (CS)²/HEP, 2011, Grenoble

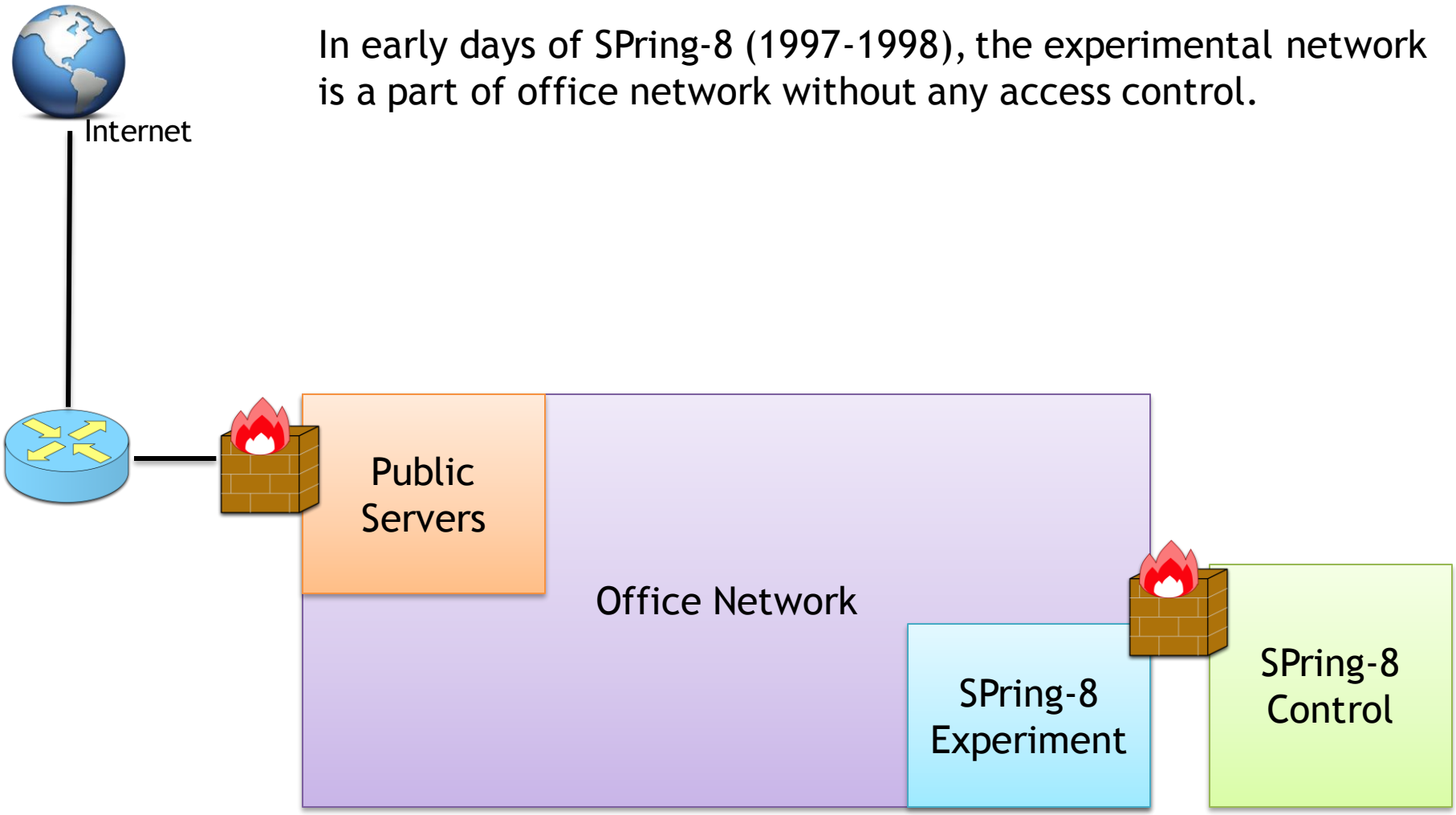
SPring-8 Experiment Network

Presented on 3rd (CS)2/HEP Workshop, 2011



History of SPring-8 Experiment Network (1of3)

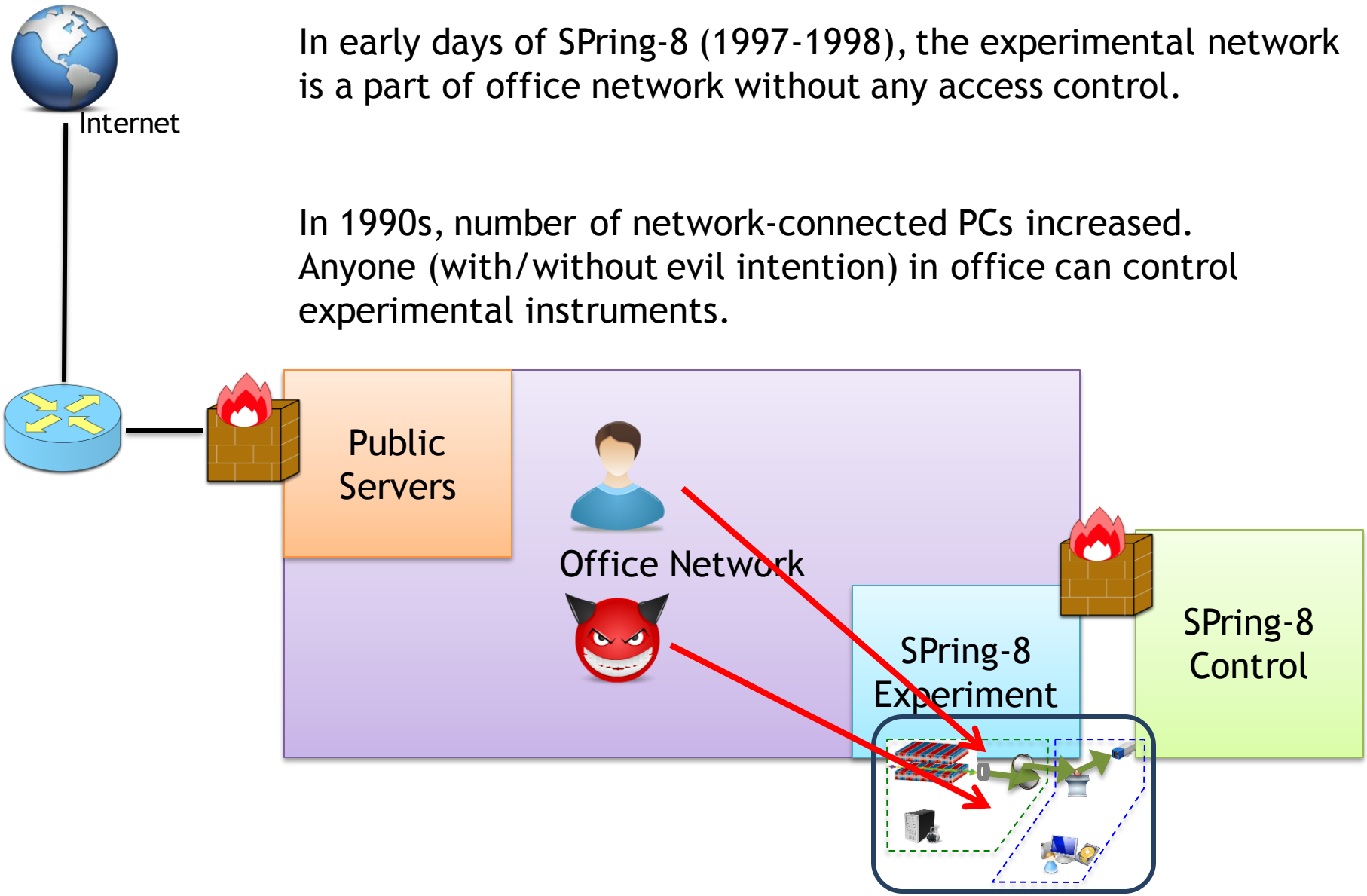
In early days of SPring-8 (1997-1998), the experimental network is a part of office network without any access control.



History of SPring-8 Experiment Network (1of3)

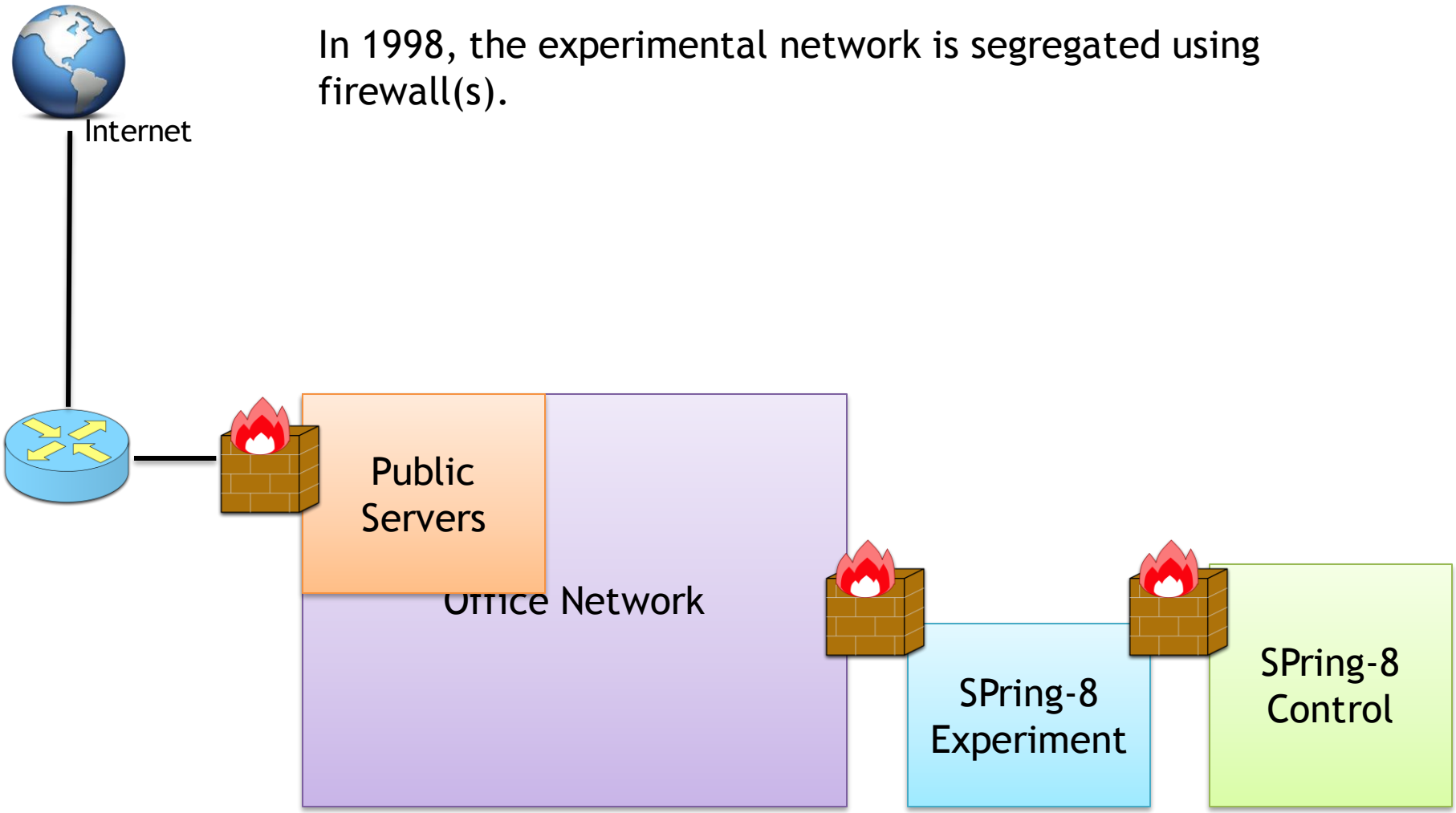
In early days of SPring-8 (1997-1998), the experimental network is a part of office network without any access control.

In 1990s, number of network-connected PCs increased. Anyone (with/without evil intention) in office can control experimental instruments.



History of SPring-8 Experiment Network (2of3)

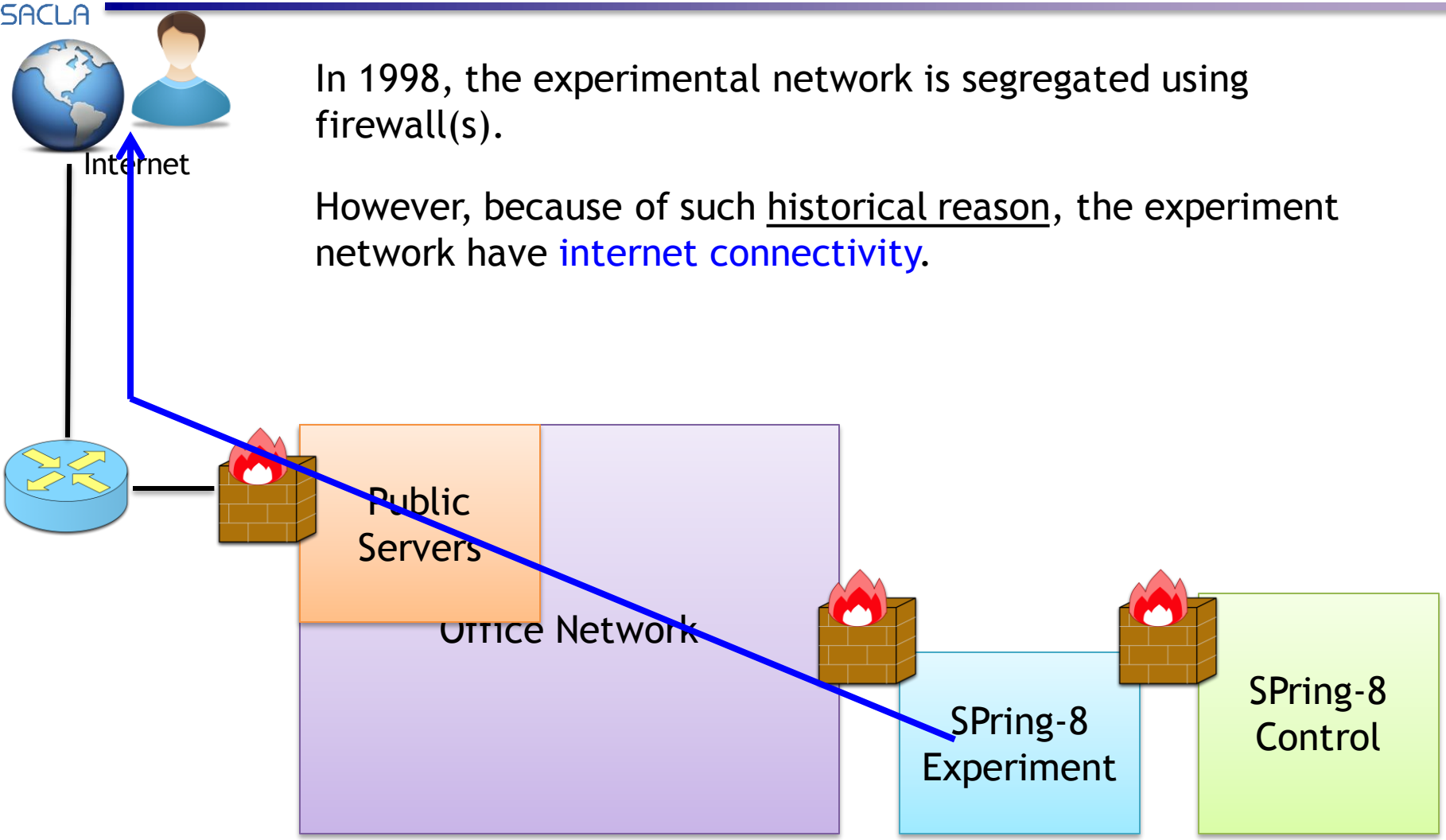
In 1998, the experimental network is segregated using firewall(s).



History of SPring-8 Experiment Network (2of3)

In 1998, the experimental network is segregated using firewall(s).

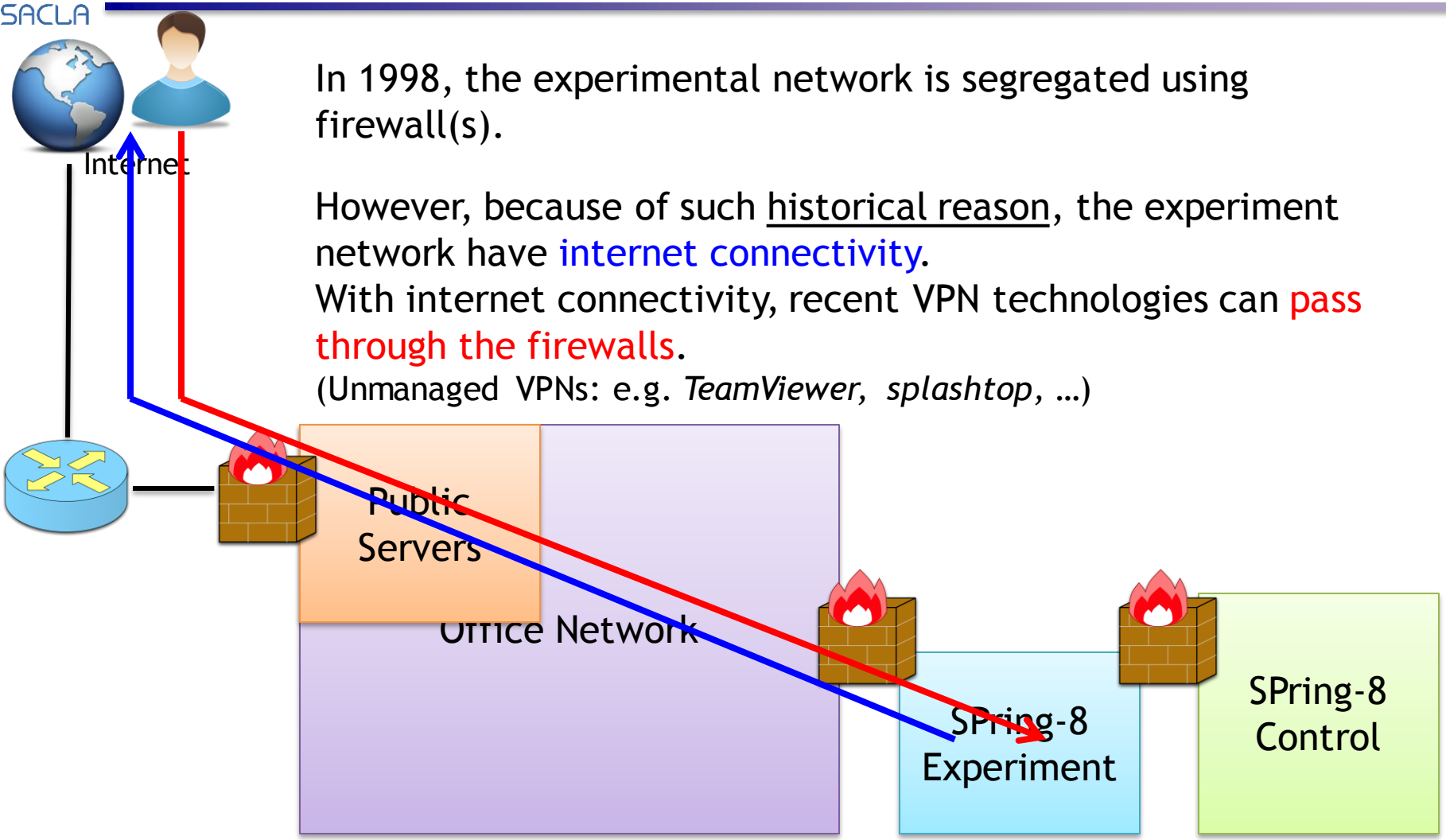
However, because of such historical reason, the experiment network have internet connectivity.



History of SPring-8 Experiment Network (2of3)

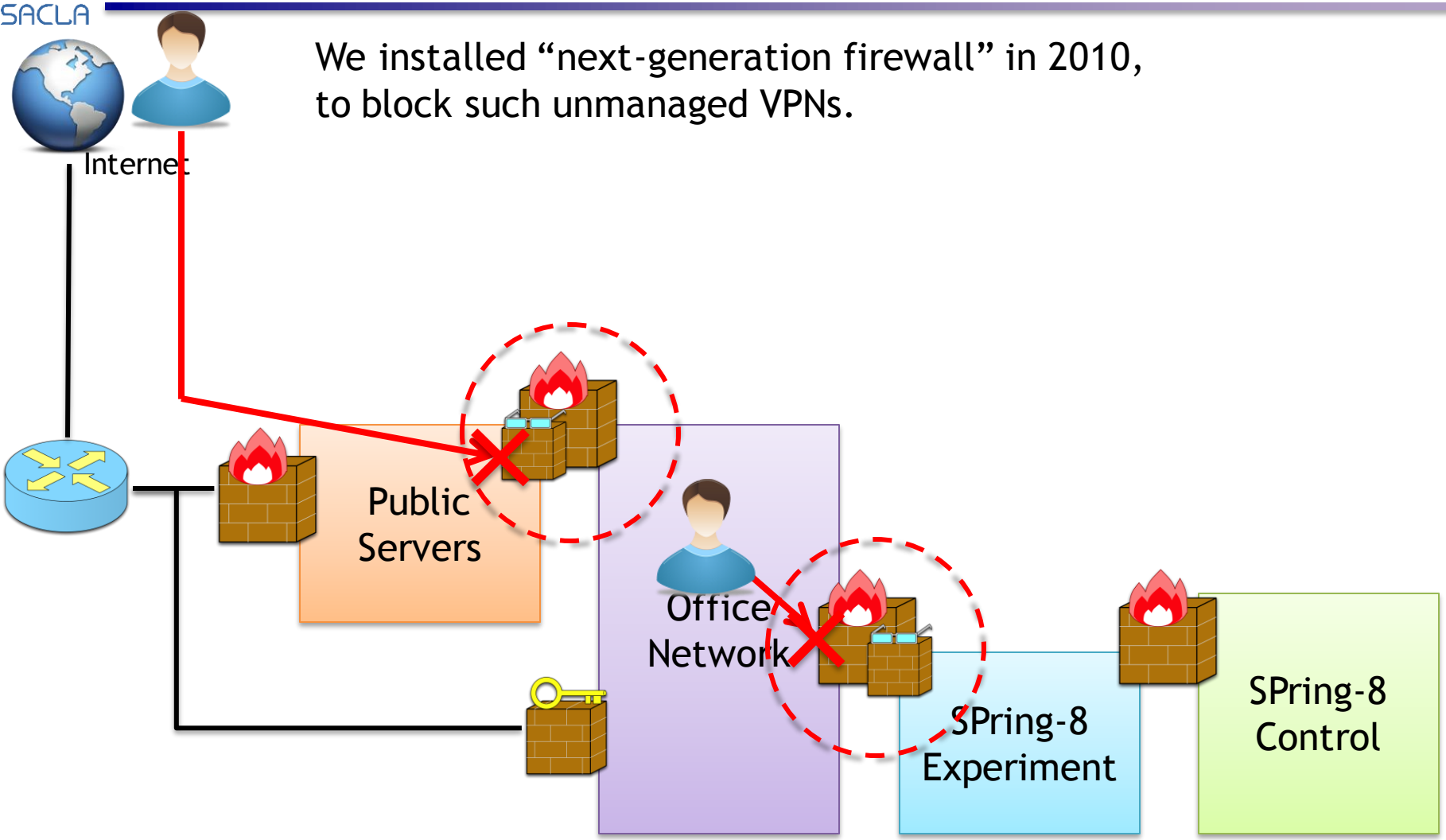
In 1998, the experimental network is segregated using firewall(s).

However, because of such historical reason, the experiment network have internet connectivity.
With internet connectivity, recent VPN technologies can pass through the firewalls.
(Unmanaged VPNs: e.g. *TeamViewer*, *splashtop*, …)



History of SPring-8 Experiment Network (3of3)

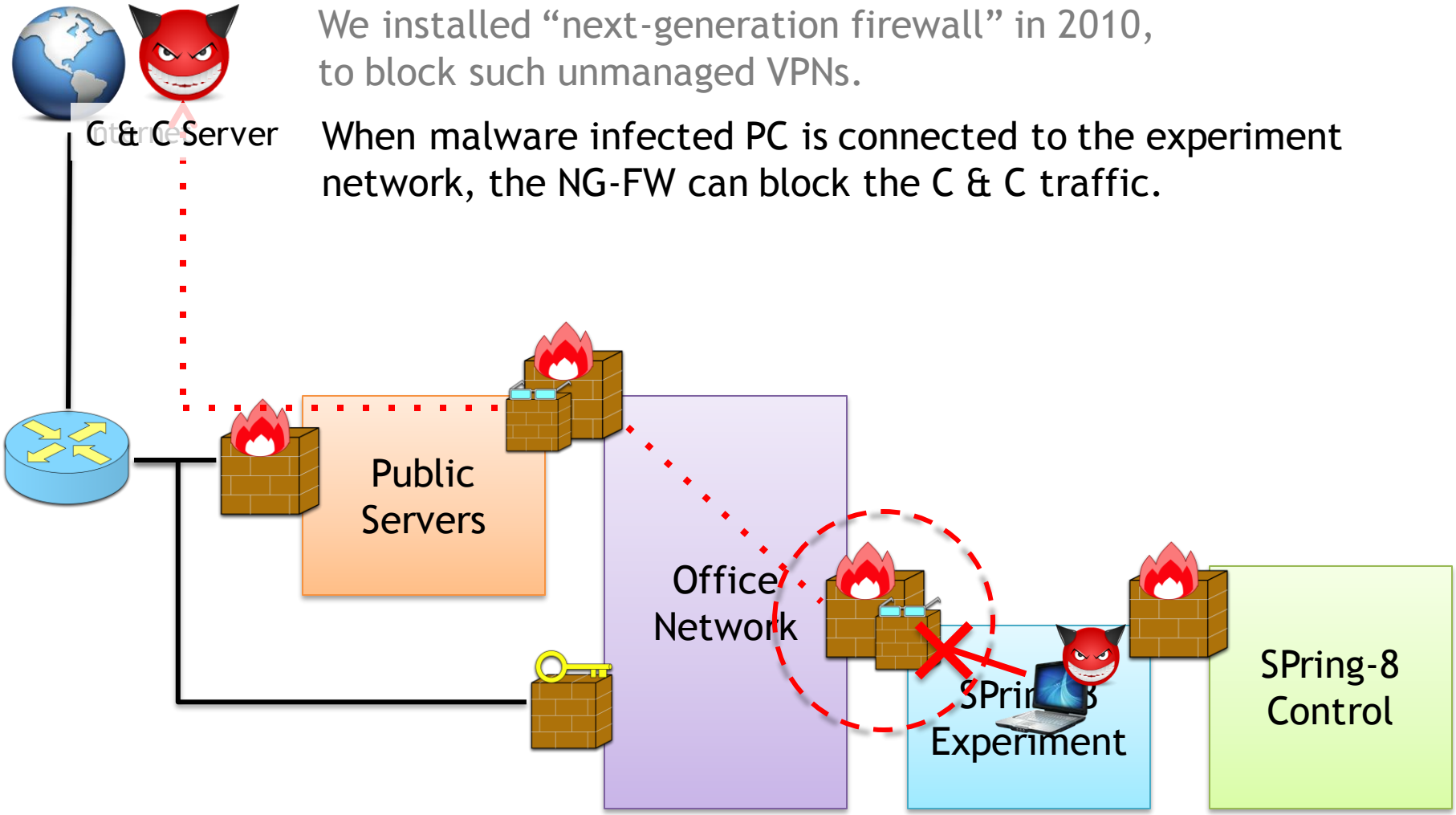
We installed “next-generation firewall” in 2010,
to block such unmanaged VPNs.



History of SPring-8 Experiment Network (3of3)

We installed “next-generation firewall” in 2010,
to block such unmanaged VPNs.

When malware infected PC is connected to the experiment network, the NG-FW can block the C & C traffic.



名前: Suspicious.Gen Command And Control Traffic

ID: 13716

内容: This signature detects Suspicious.Gen command and control traffic.

重大度: CRITICAL

上位攻撃者

	攻撃者の IP	攻撃者のホスト名	攻撃者	セッション
1	54.230.124.83	server-54-230-124-83.nrt52.r.cloudfront.net		11
2	54.230.124.50	server-54-230-124-50.nrt52.r.cloudfront.net		10
3	54.230.124.12	server-54-230-124-12.nrt52.r.cloudfront.net		8
4	54.230.124.87	server-54-230-124-87.nrt52.r.cloudfront.net		7
5	54.230.124.80	server-54-230-124-80.nrt52.r.cloudfront.net		6
6	54.230.124.41	server-54-230-124-41.nrt52.r.cloudfront.net		5
7	54.230.124.38	server-54-230-124-38.nrt52.r.cloudfront.net		5
8	54.230.124.32	server-54-230-124-32.nrt52.r.cloudfront.net		3
9	54.192.235.210	server-54-192-235-210.nrt12.r.cloudfront.net		1

上位の被害者

	被害者 IP	被害者ホスト名	被害者	セッション
1	[redacted]	[redacted].spring8.or.jp		56

上位攻撃国

	攻撃者の国	セッション
1	United States	56

上位の被害者国

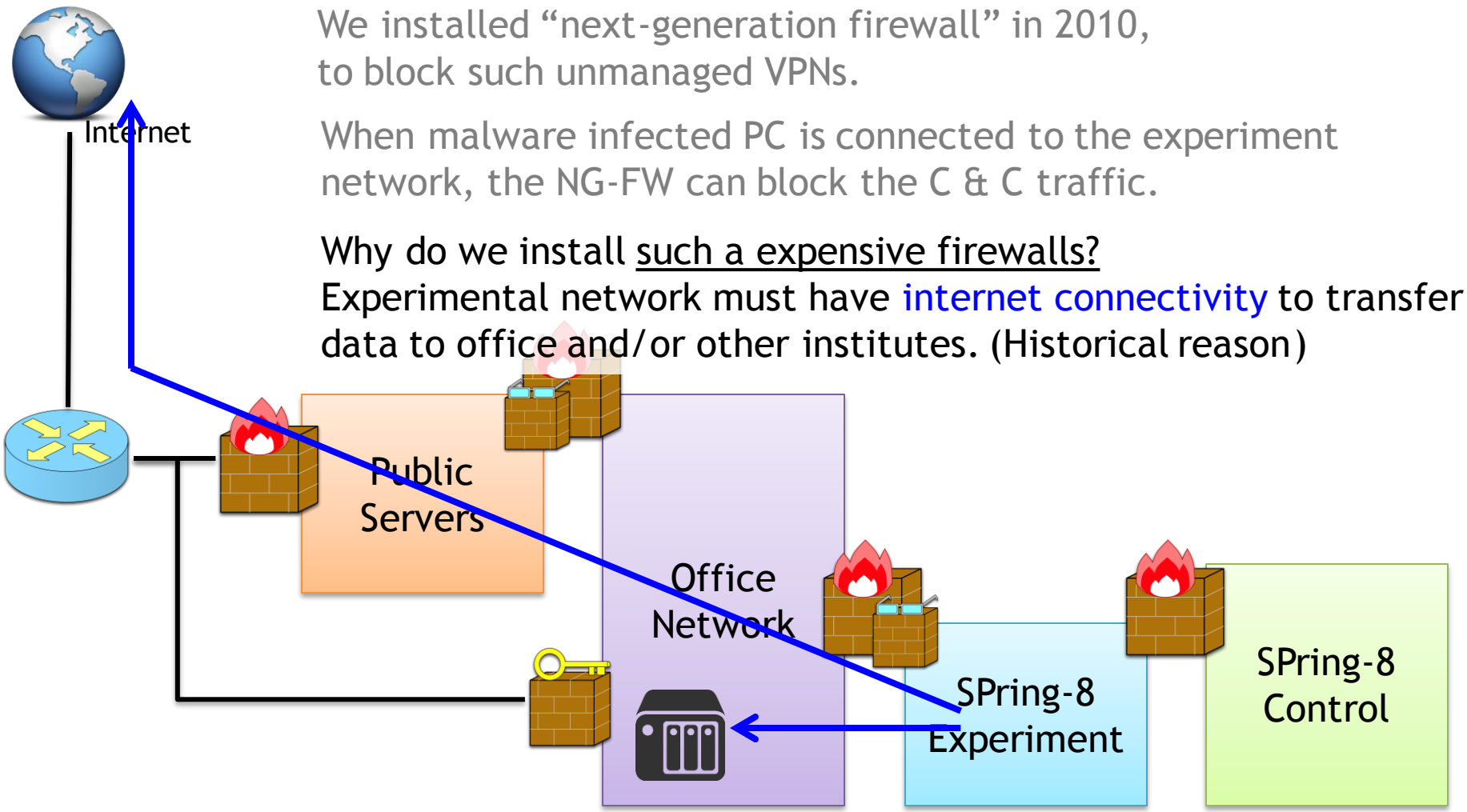
	被害者国	セッション
1	JP_SP8_OA-LAN	56

History of SPring-8 Experiment Network (3of3)

We installed "next-generation firewall" in 2010, to block such unmanaged VPNs.

When malware infected PC is connected to the experiment network, the NG-FW can block the C & C traffic.

Why do we install <u>such a expensive firewalls?</u>
Experimental network must have internet connectivity to transfer data to office and/or other institutes. (Historical reason)



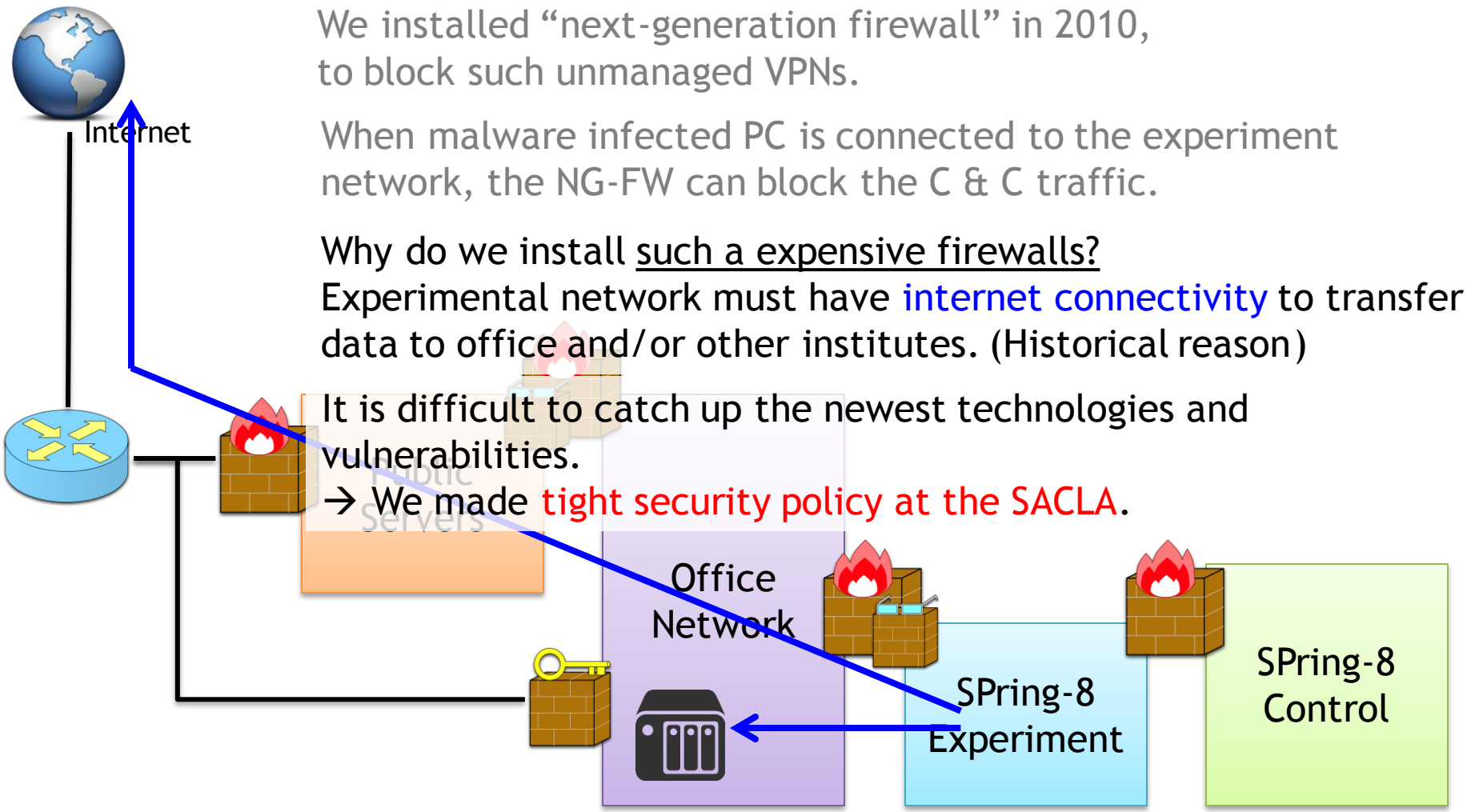
History of SPring-8 Experiment Network (3of3)

We installed "next-generation firewall" in 2010, to block such unmanaged VPNs.

When malware infected PC is connected to the experiment network, the NG-FW can block the C & C traffic.

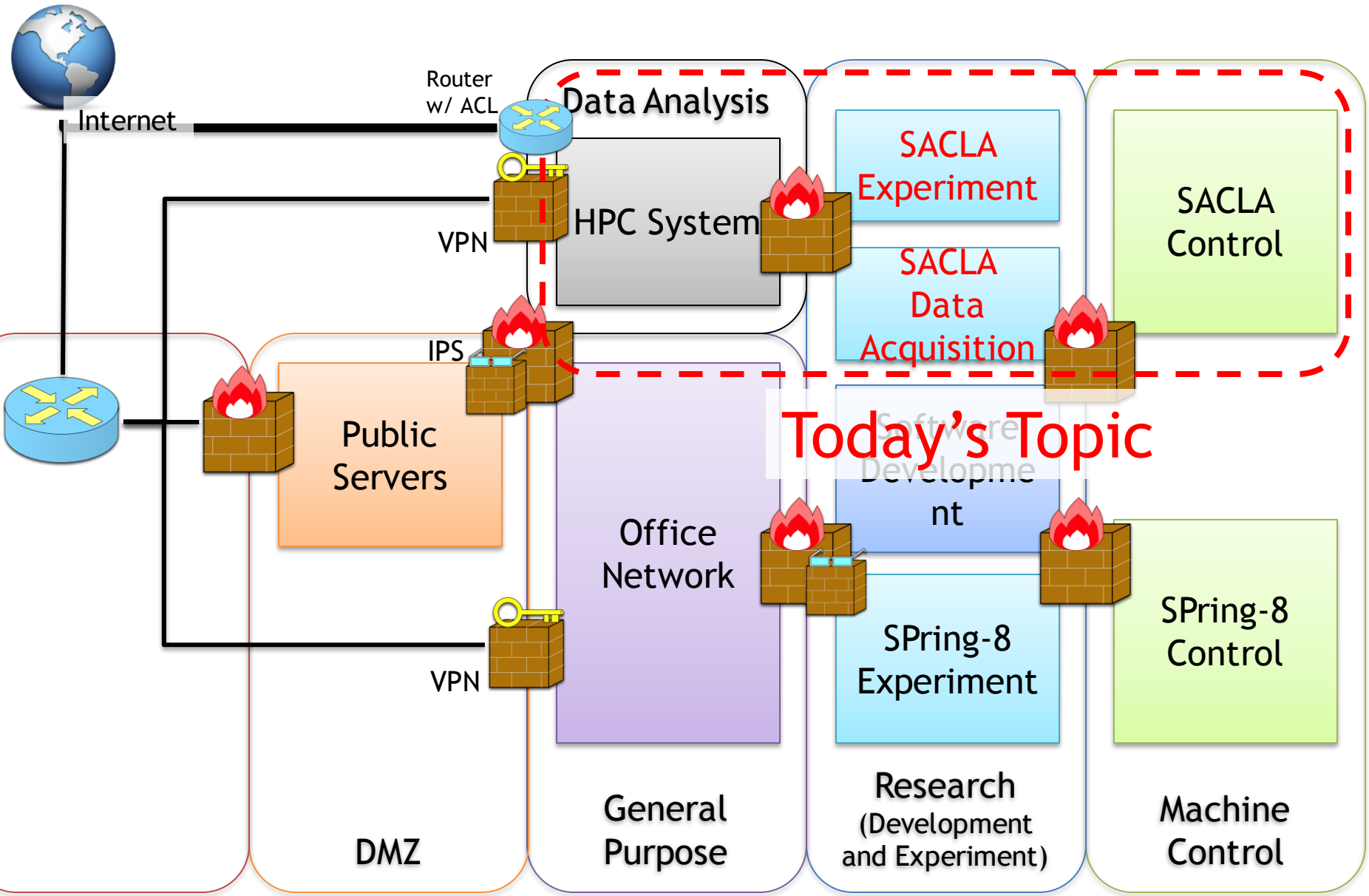
Why do we install <u>such a expensive firewalls?</u>
Experimental network must have internet connectivity to transfer data to office and/or other institutes. (Historical reason)

It is difficult to catch up the newest technologies and vulnerabilities.
→ We made tight security policy at the SACLA.



SACLA Network System

SPring-8 Campus Network

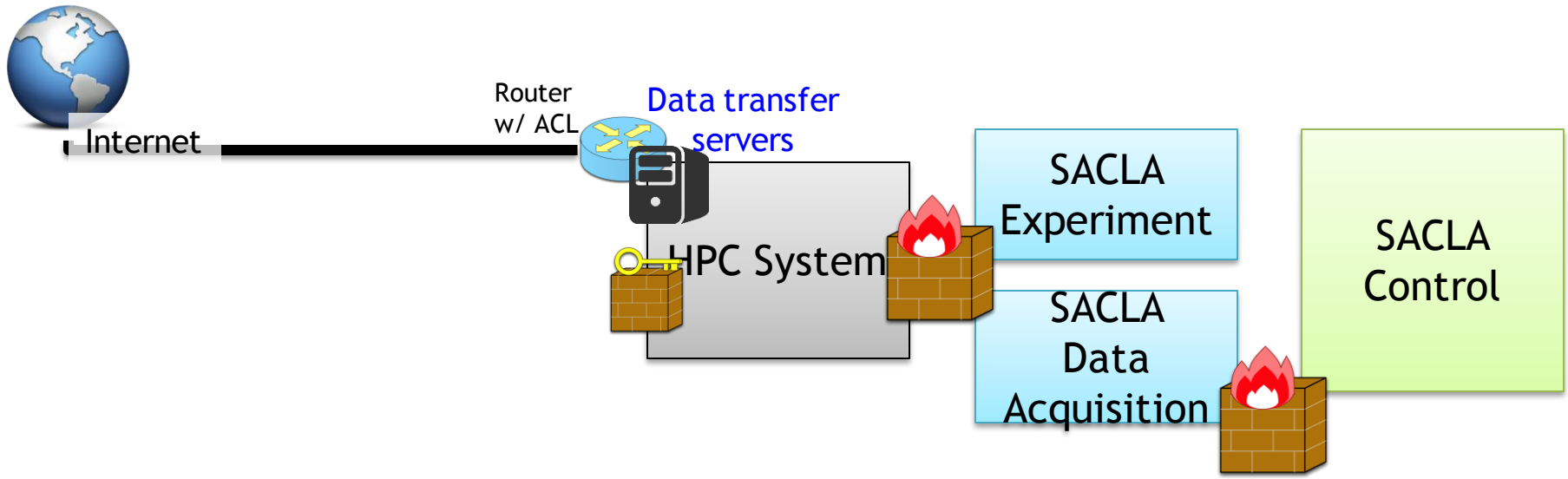


Summary

SACLA Experimental Network Policy

1. No internet connectivity
2. Segregate LANs based on purpose
3. Logically segmented by experimental area/unit, to perform multi-beamline experiments
4. Physically segmented by beamlines to guaranty DAQ performance

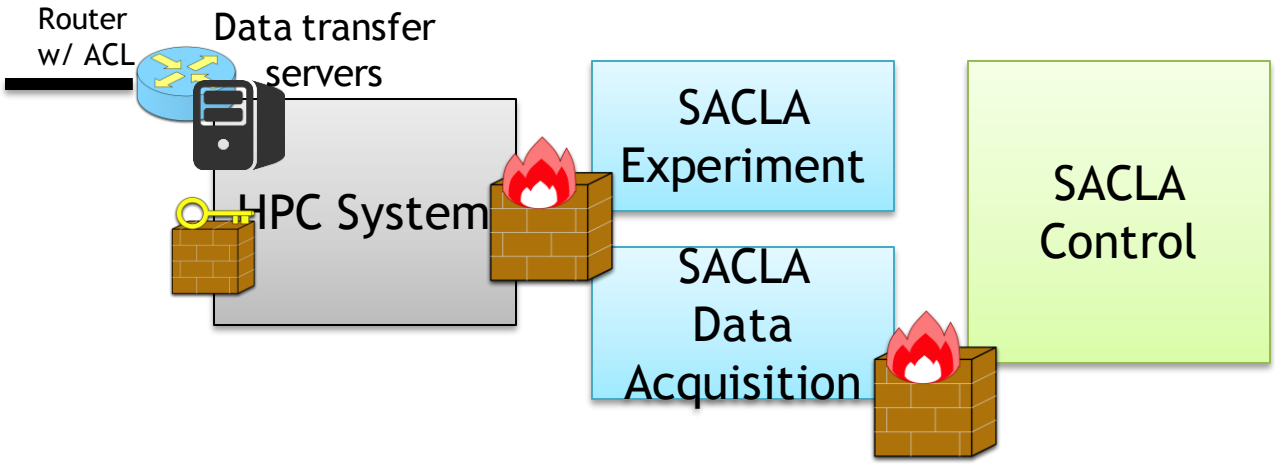
1. No Internet Connectivity



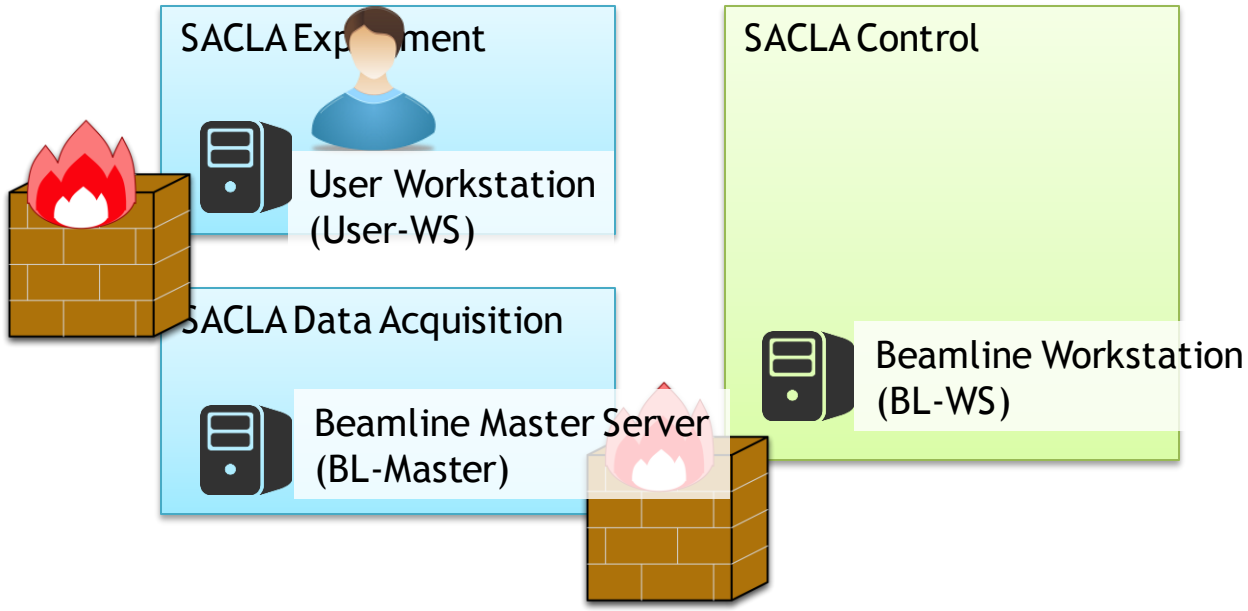
At first, we decided to have no internet connectivity at the SACLA network systems. Dedicate servers take charge of data transfer to other institutes.

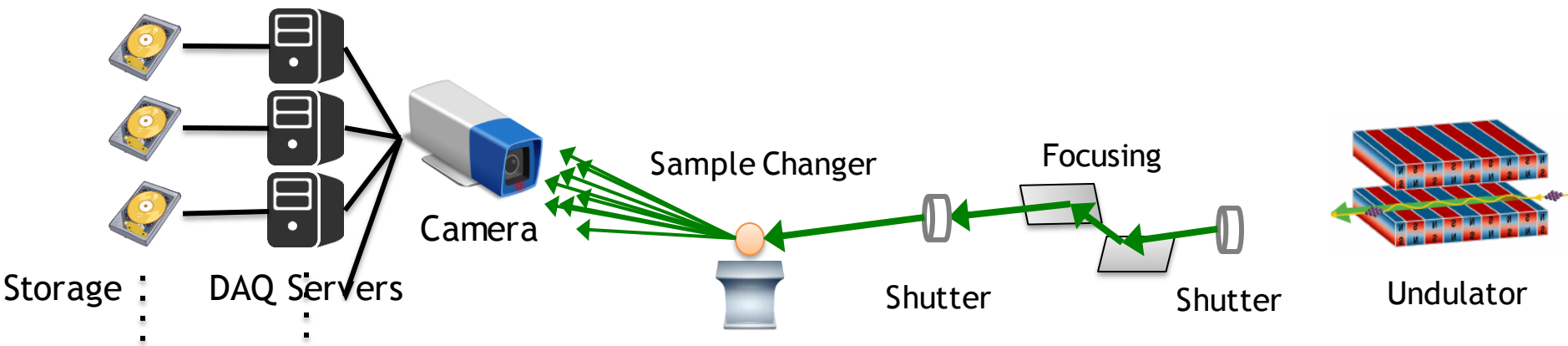
By segregating network systems from the Internet, experimental systems are prevented from recent vulnerabilities which utilize the internet.

1. No Internet Connectivity

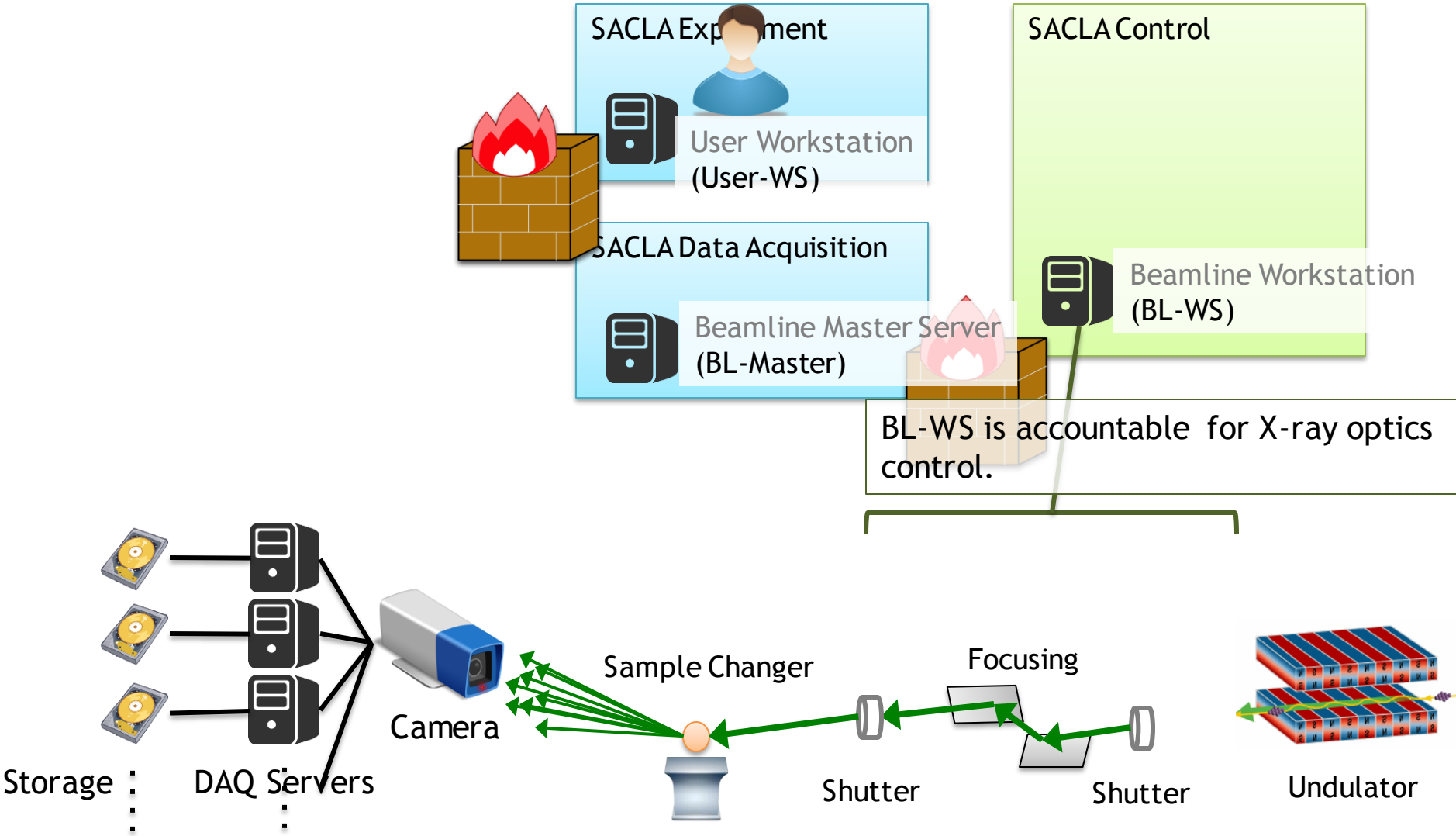


2. Segregate LANs based on purpose

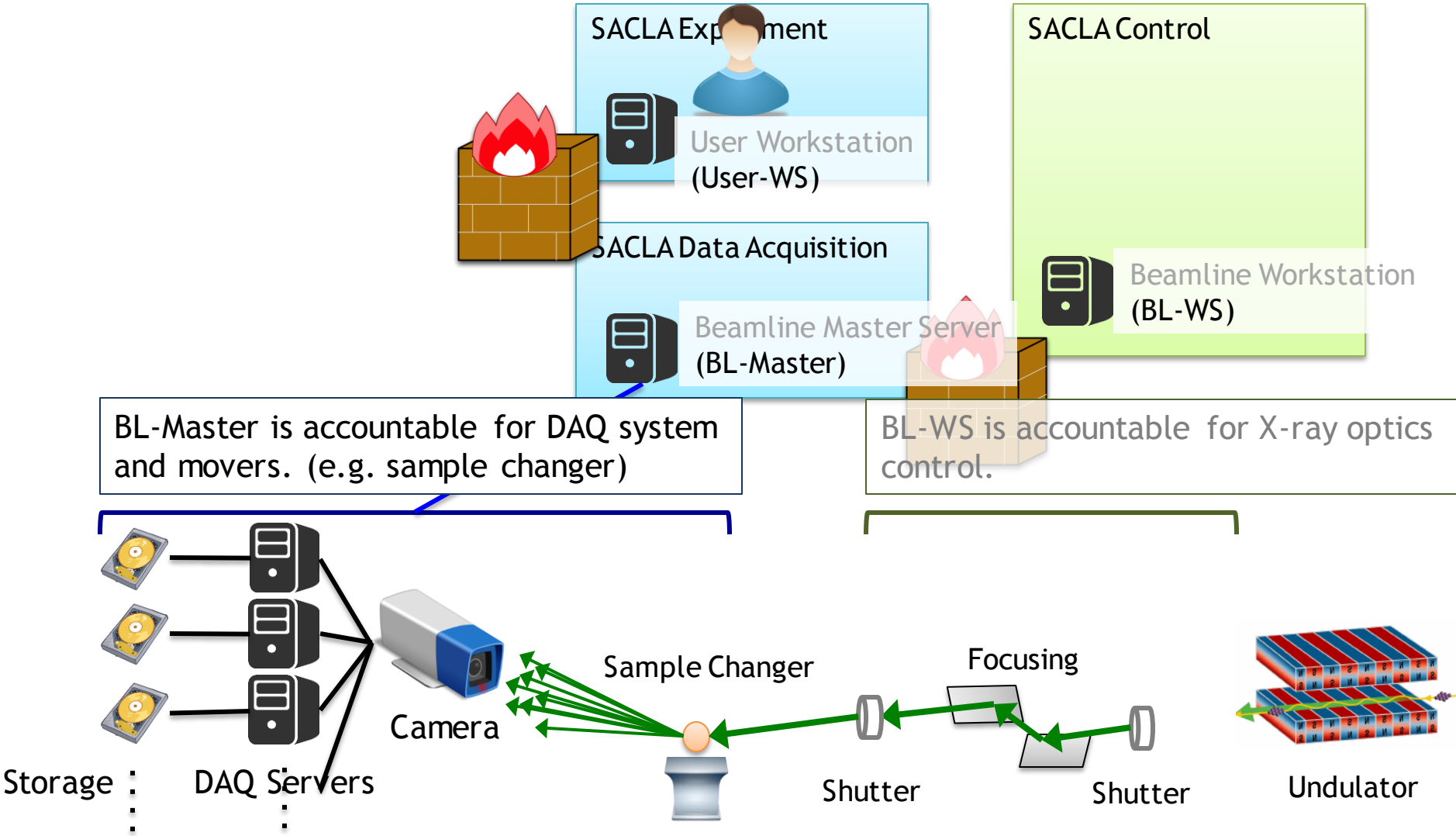




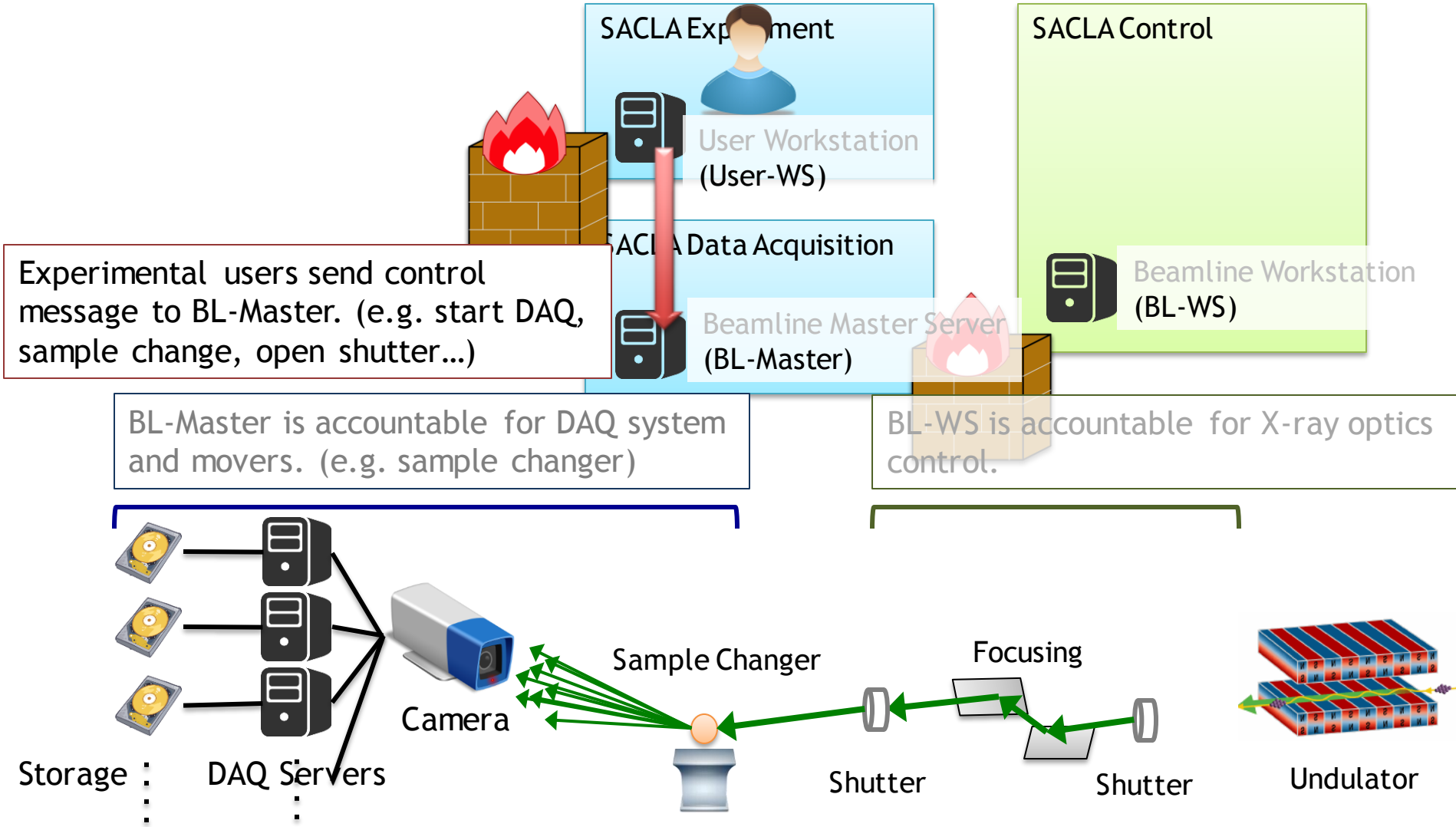
2. Segregate LANs based on purpose



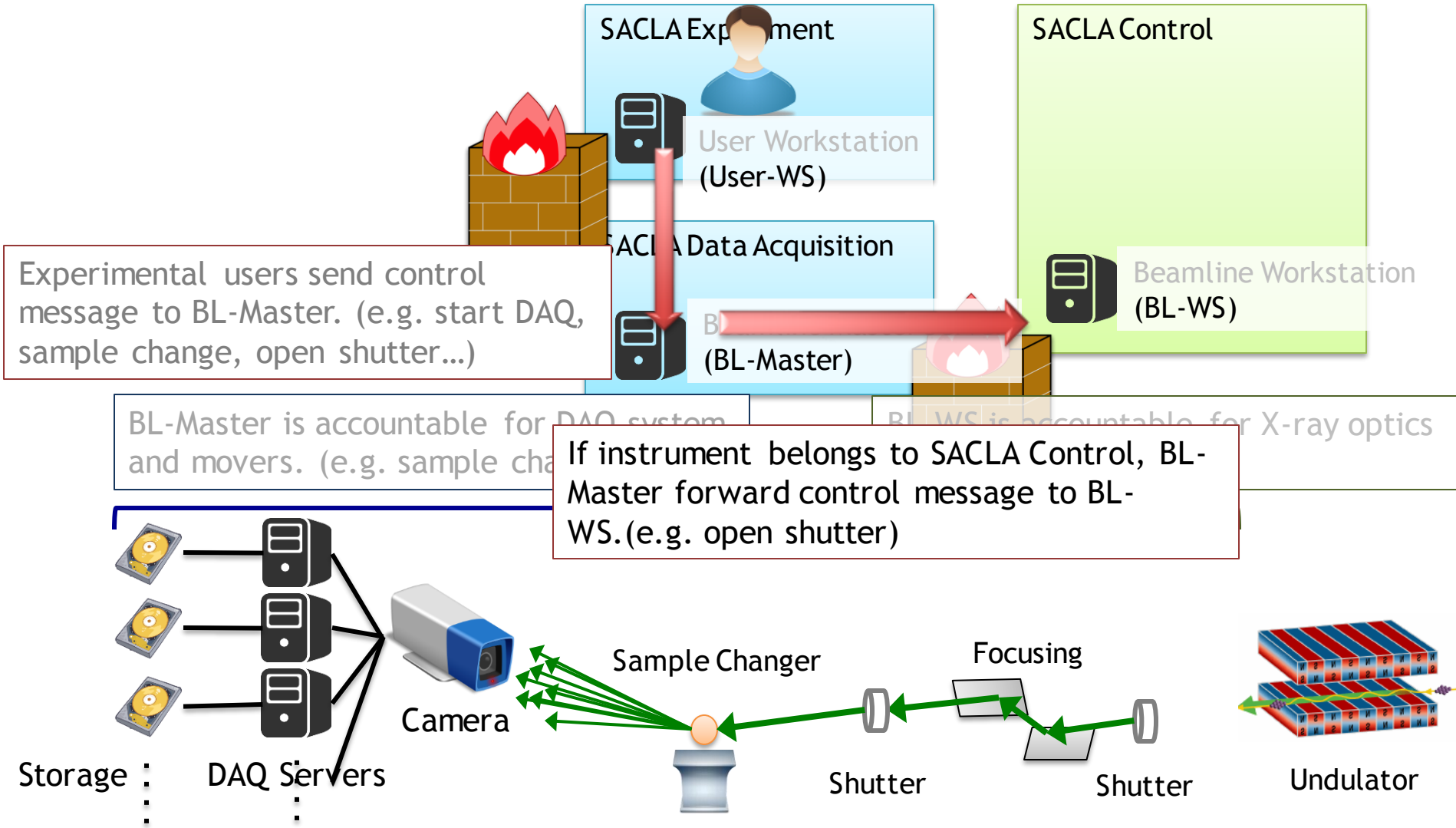
2. Segregate LANs based on purpose



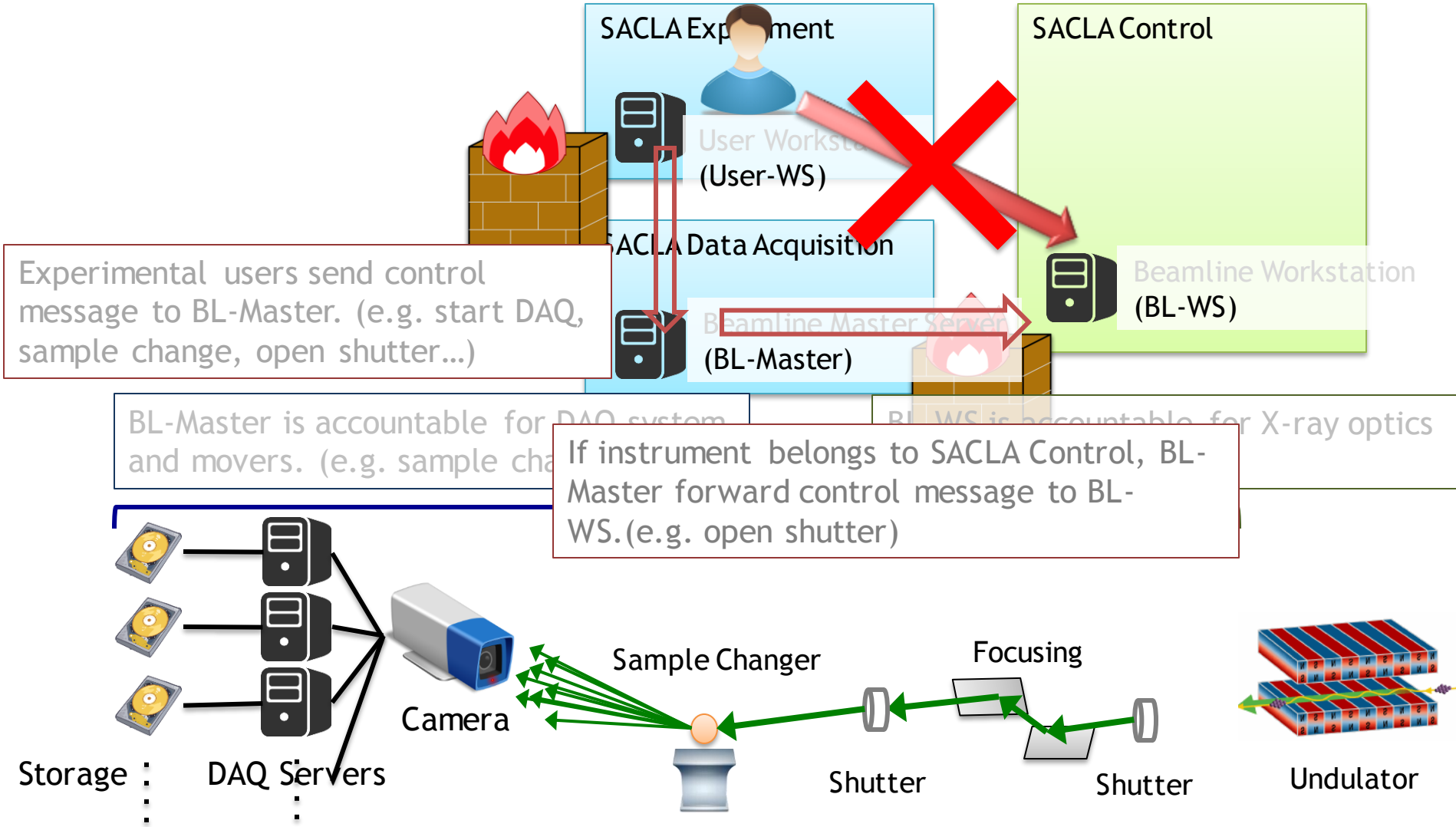
2. Segregate LANs based on purpose



2. Segregate LANs based on purpose

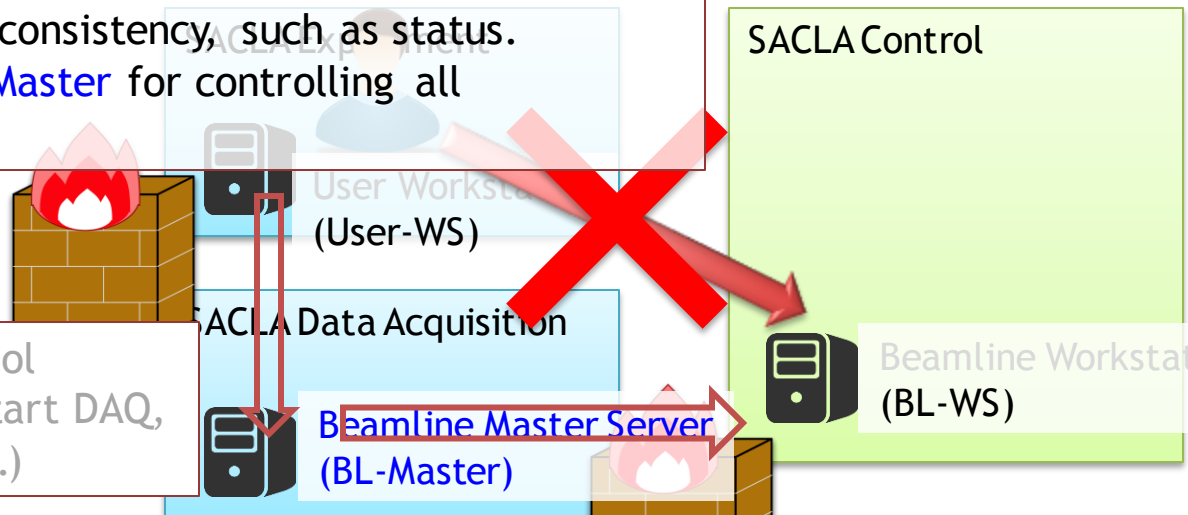


2. Segregate LANs based on purpose



2. Segregate LANs based on purpose

Direct access from User-WS to BL-WS is forbidden.
The reason are
1. To ensure control system consistency, such as status.
2. Single UI provided by BL-Master for controlling all experimental instruments.

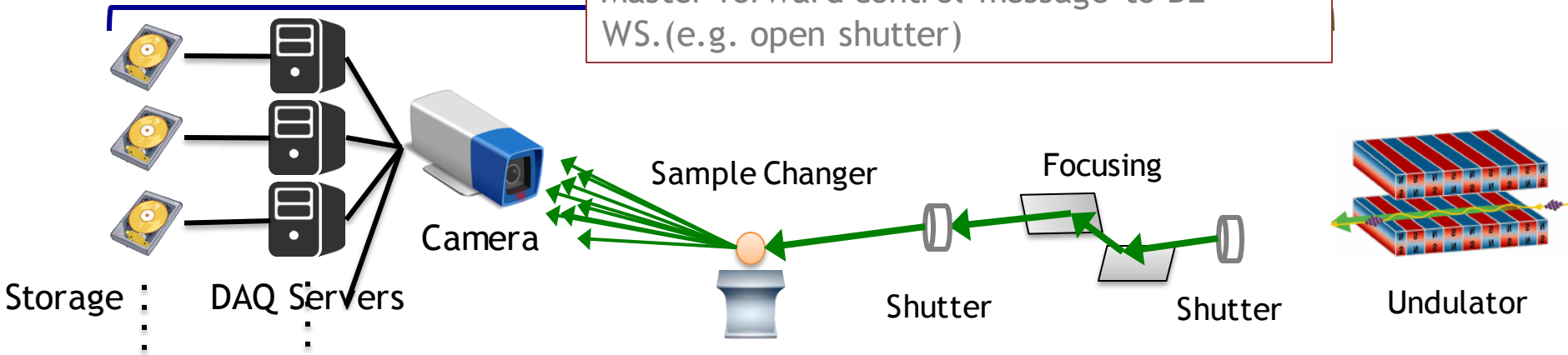


Experimental users send control message to BL-Master. (e.g. start DAQ, sample change, open shutter…)

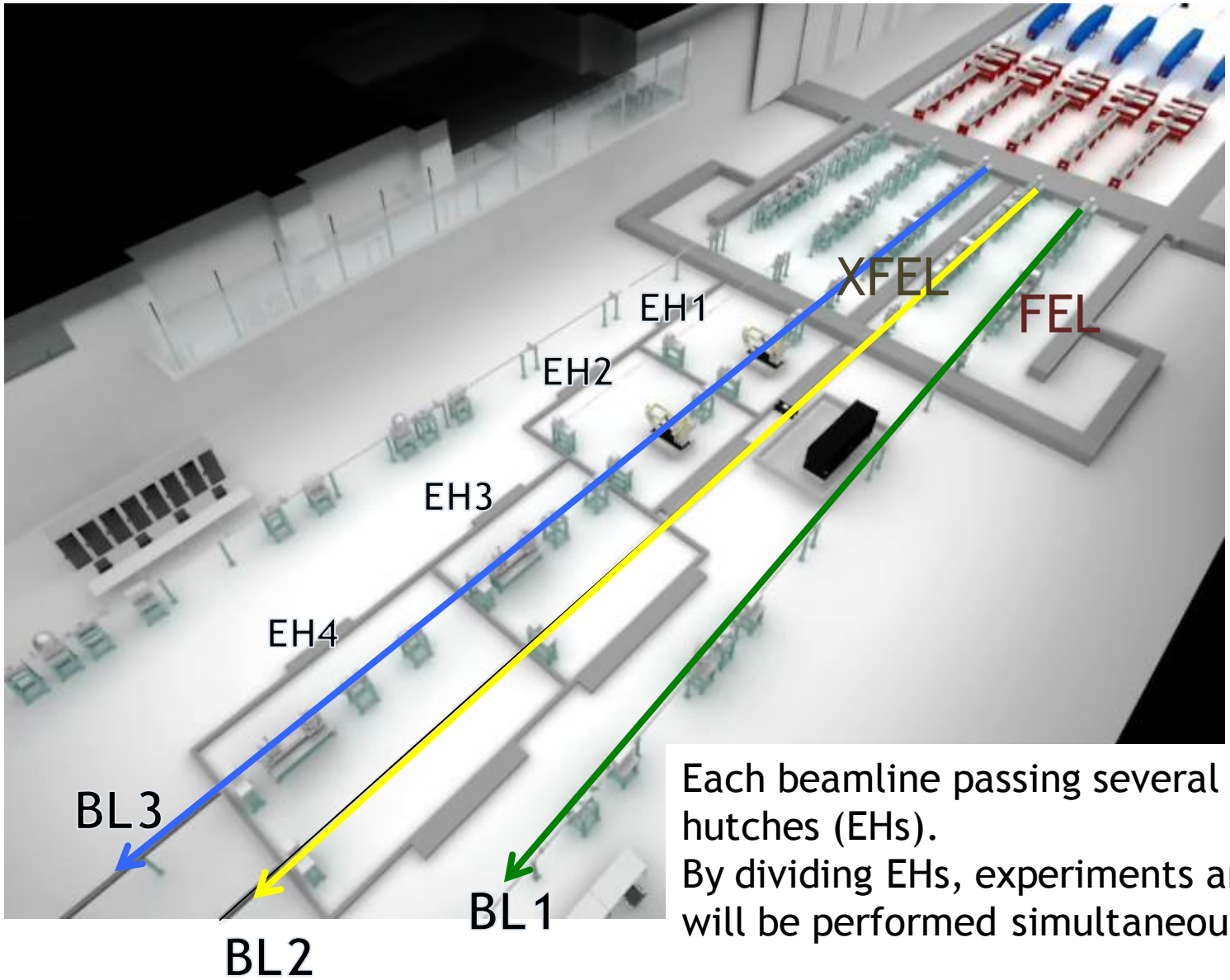
BL-Master is accountable for DAQ system and movers. (e.g. sample cha

BL-WS is accountable for X-ray optics

If instrument belongs to SACLA Control, BL-Master forward control message to BL-WS.(e.g. open shutter)



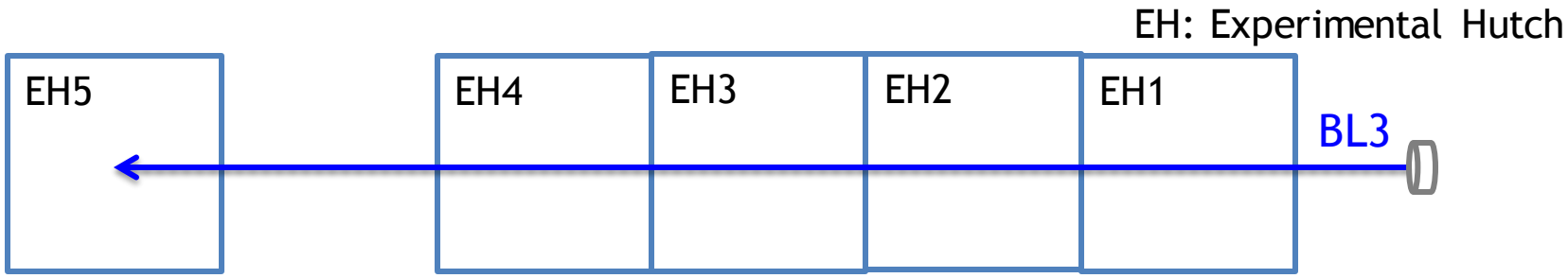
SACLA Experimental Hall



Each beamline passing several experimental hutches (EHs).
By dividing EHs, experiments and preparation will be performed simultaneously.

History and Current Status of SACLA Beamlines

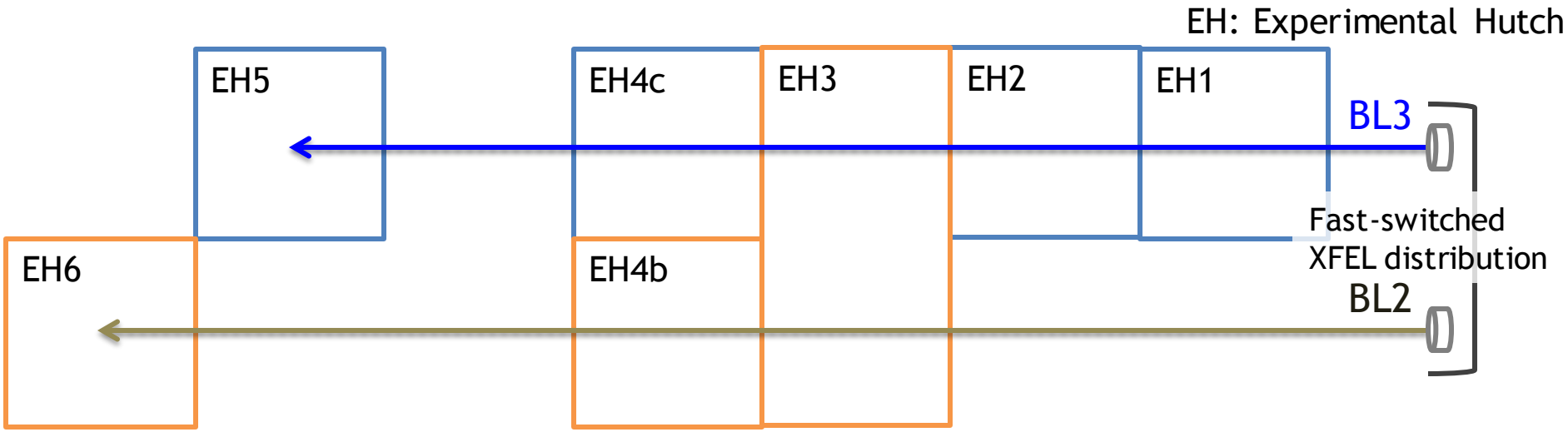
BL3 is the first beamline, which delivers XFEL to users. (2011)



History and Current Status of SACLA Beamlines

BL3 is the first beamline, which delivers XFEL to users. (2011)

BL2 is in operation. (2014)
Fast-switched XFEL distribution to BL2/BL3 is started. (2015)

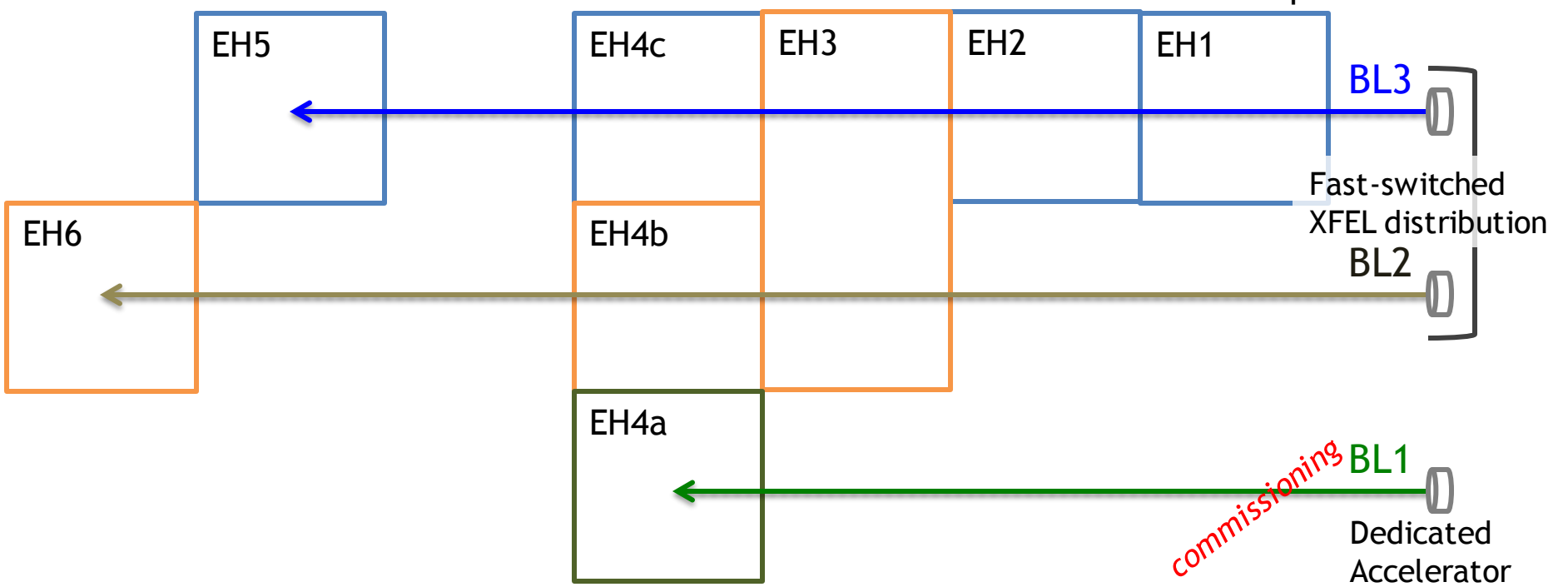


History and Current Status of SACLA Beamlines

BL3 is the first beamline, which delivers XFEL to users. (2011)

BL2 is in operation. (2014)
Fast-switched XFEL distribution to BL2/BL3 is started. (2015)

BL1 offers more experimental opportunity to users, especially from EUV to soft X-ray FEL. (2016)

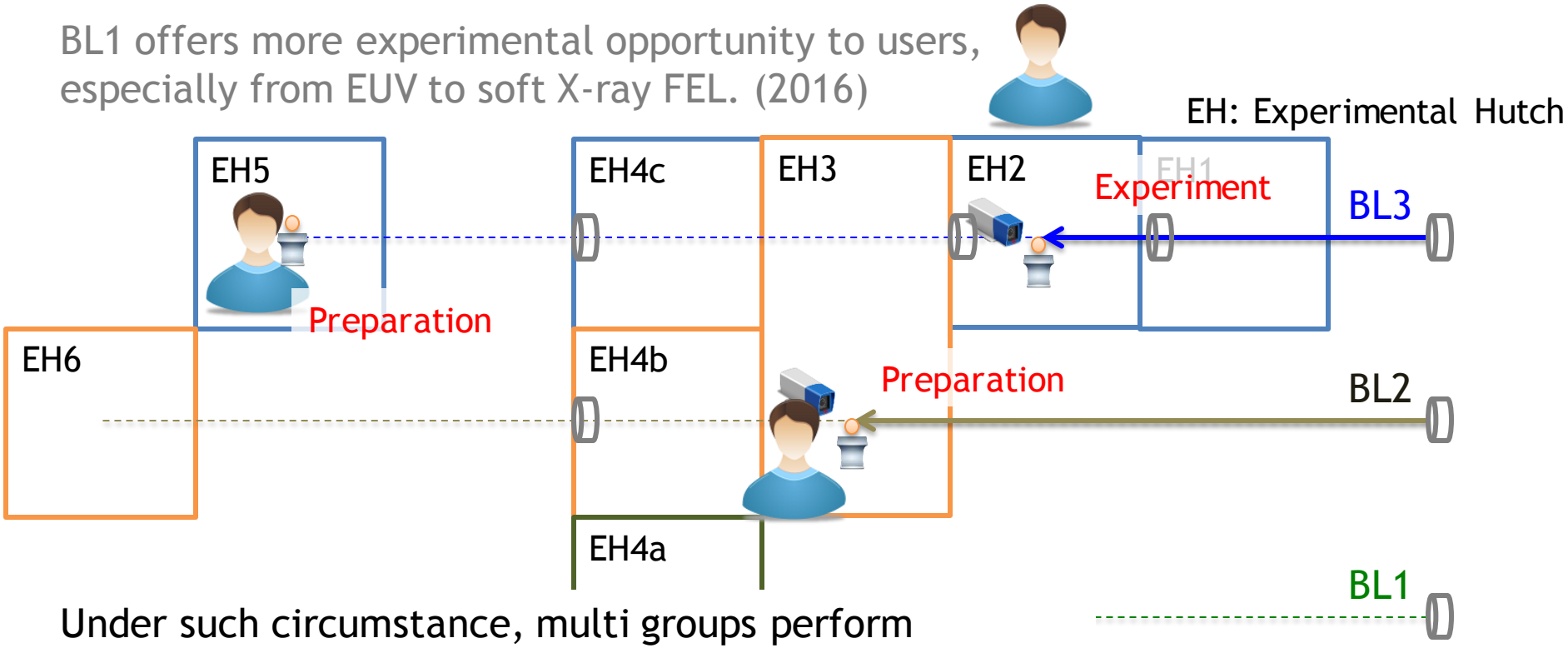


History and Current Status of SACLA Beamlines

BL3 is the first beamline, which delivers XFEL to users. (2011)

BL2 is in operation. (2014)
Fast-switched XFEL distribution to BL2/BL3 is started. (2015)

BL1 offers more experimental opportunity to users, especially from EUV to soft X-ray FEL. (2016)



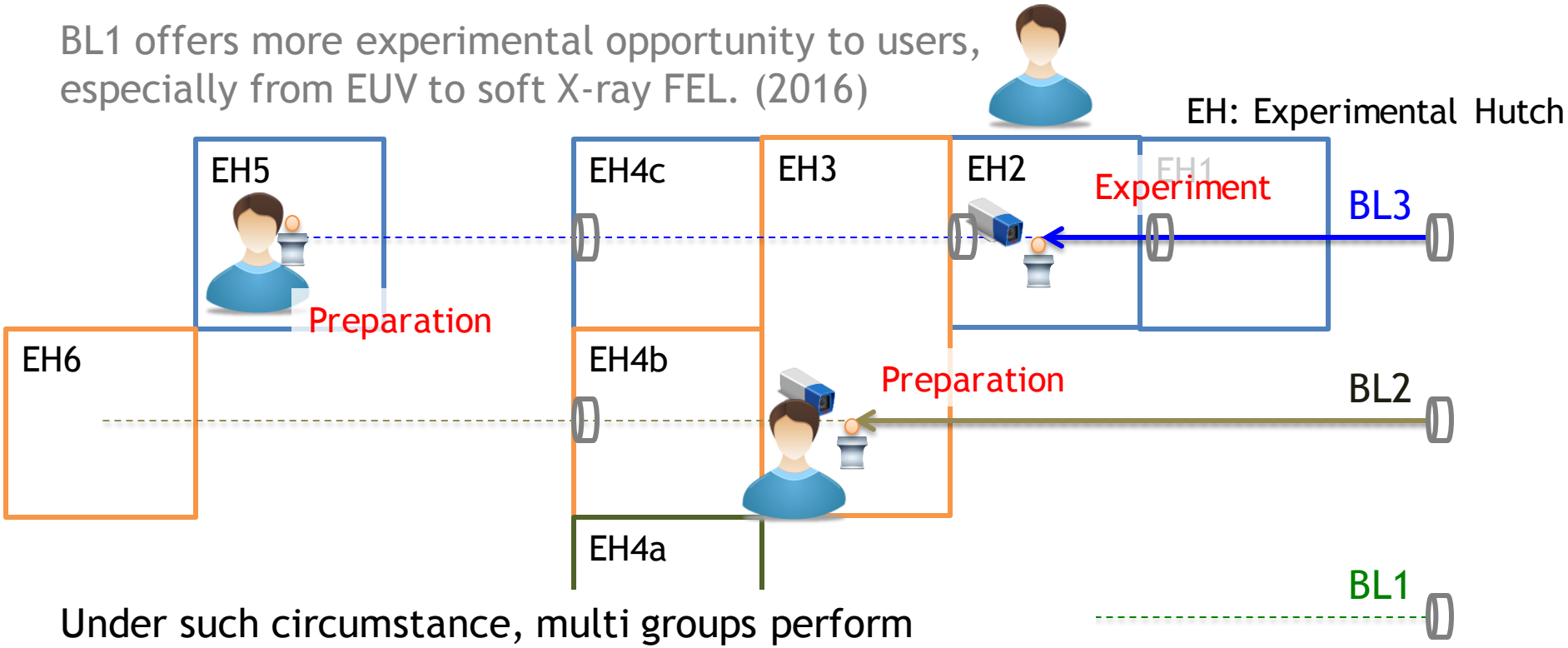
Under such circumstance, multi groups perform experiments and preparations, simultaneously.

History and Current Status of SACLA Beamlines

BL3 is the first beamline, which delivers XFEL to users. (2011)

BL2 is in operation. (2014)
Fast-switched XFEL distribution to BL2/BL3 is started. (2015)

BL1 offers more experimental opportunity to users, especially from EUV to soft X-ray FEL. (2016)

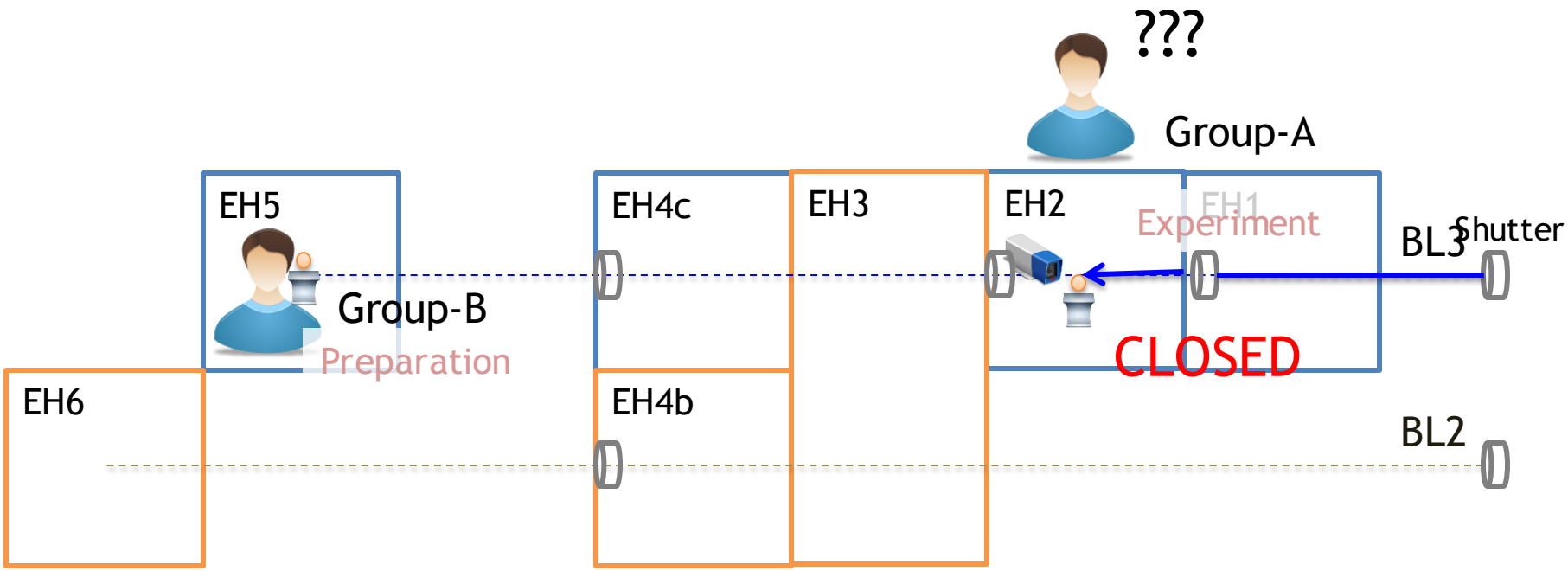


Under such circumstance, multi groups perform experiments and preparations, simultaneously.

→ Security issue occurred

Security Issue: wrong shutter operation

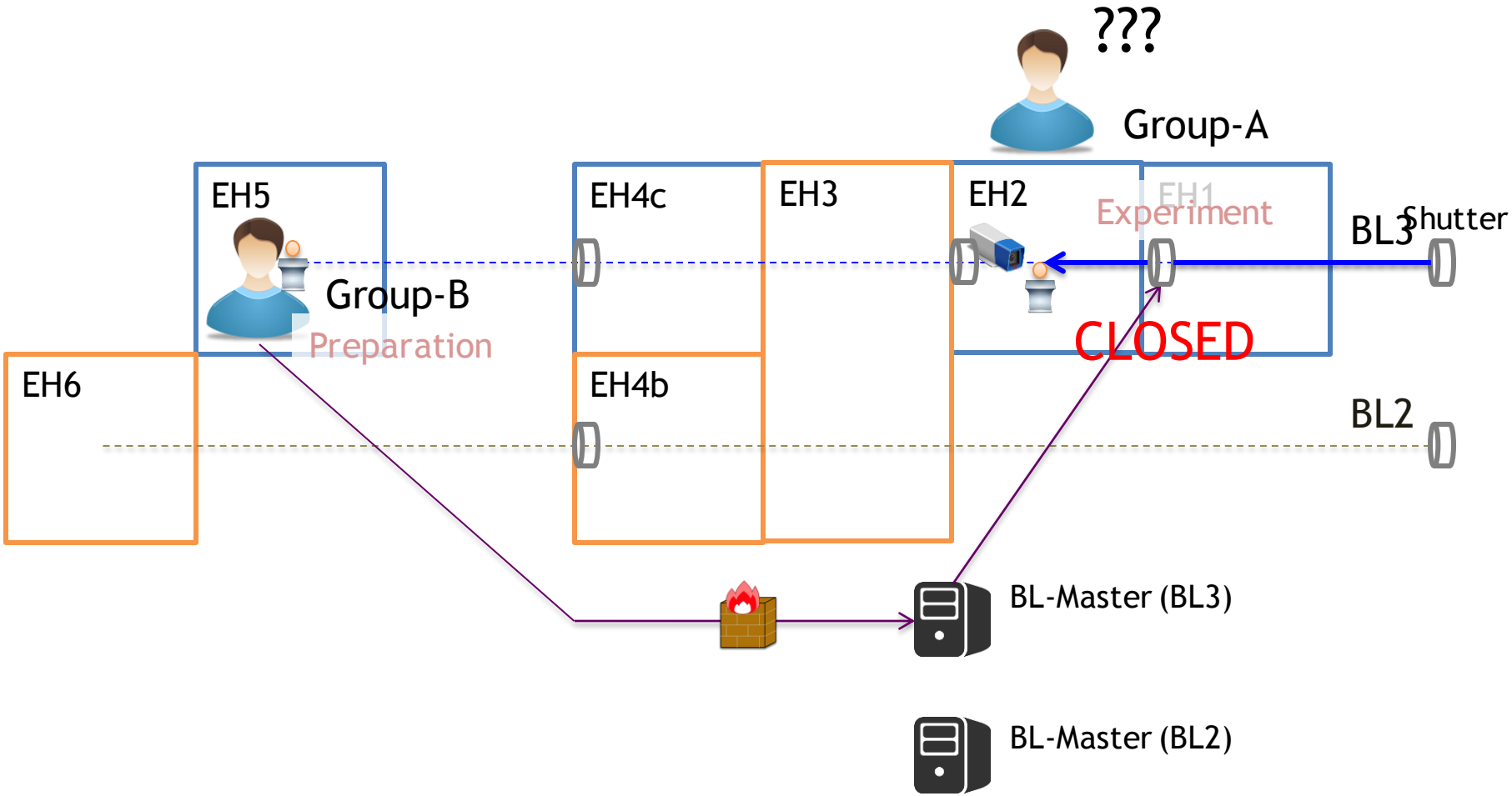
During machine time of group-A, shutter closed suddenly.



Security Issue: wrong shutter operation

During machine time of group-A, shutter closed suddenly.

Trouble source is control message from EH5 to BL-Master.



Security Issue: wrong shutter operation

During machine time of group-A, shutter closed suddenly.

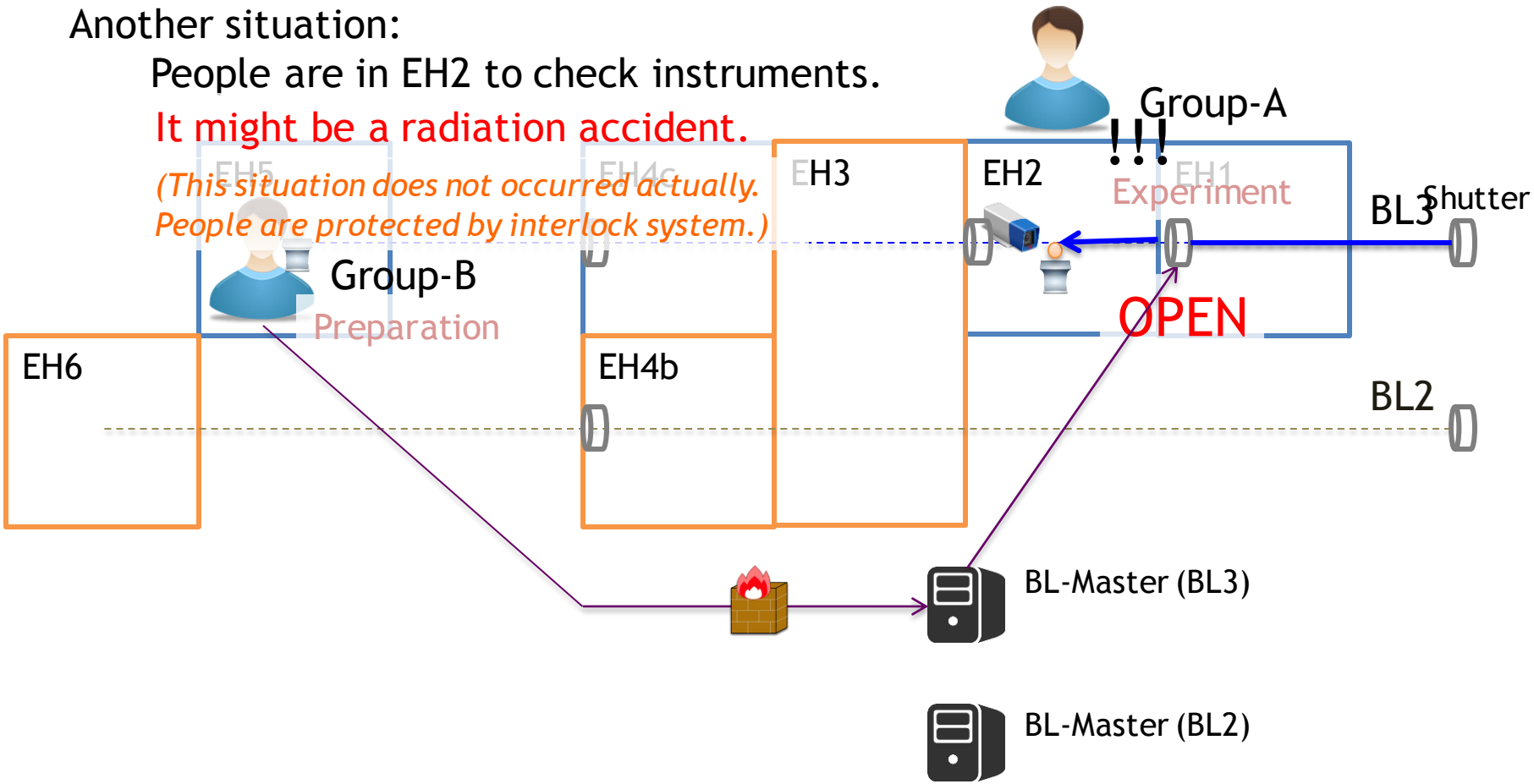
Trouble source is control message from EH5 to BL-Master.

Another situation:

People are in EH2 to check instruments.

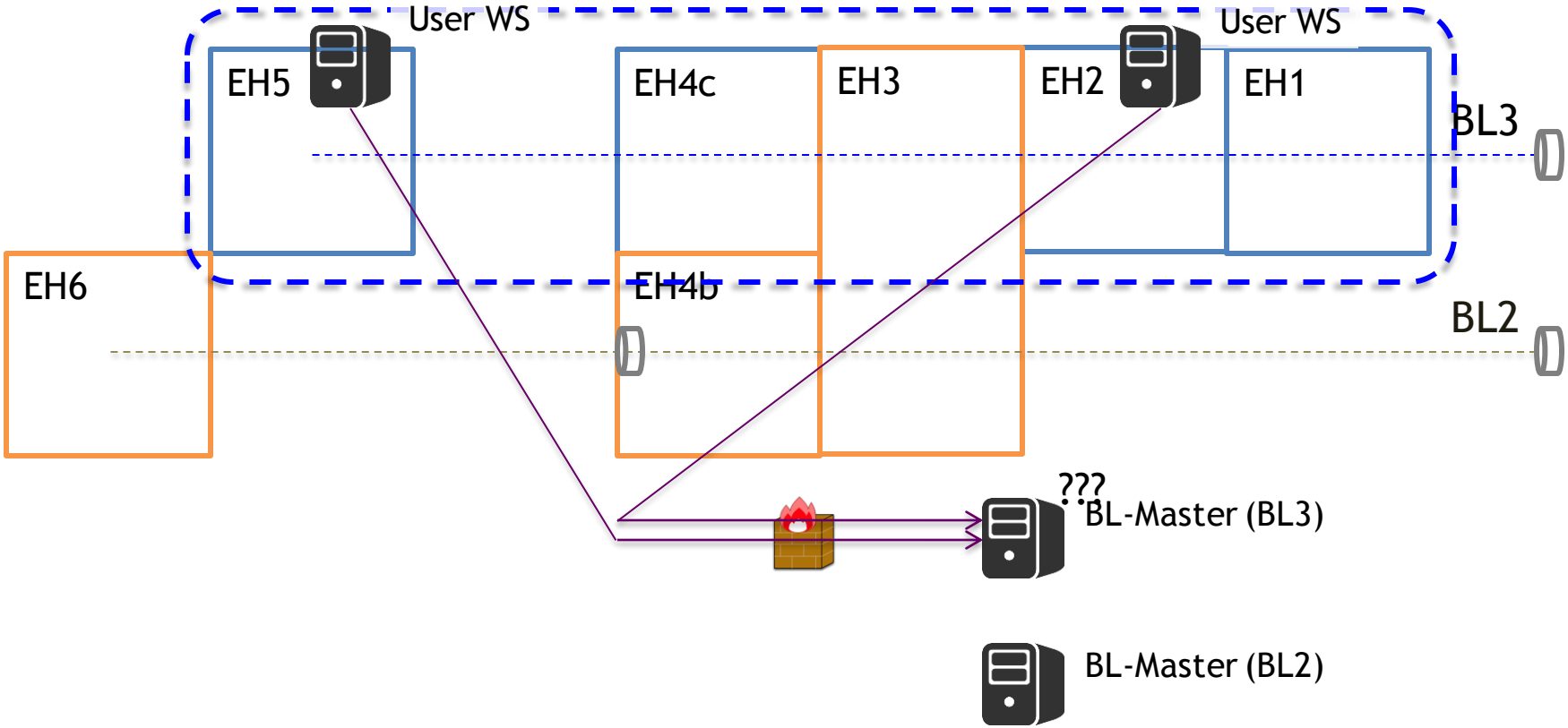
It might be a radiation accident.

(This situation does not occurred actually. People are protected by interlock system.)



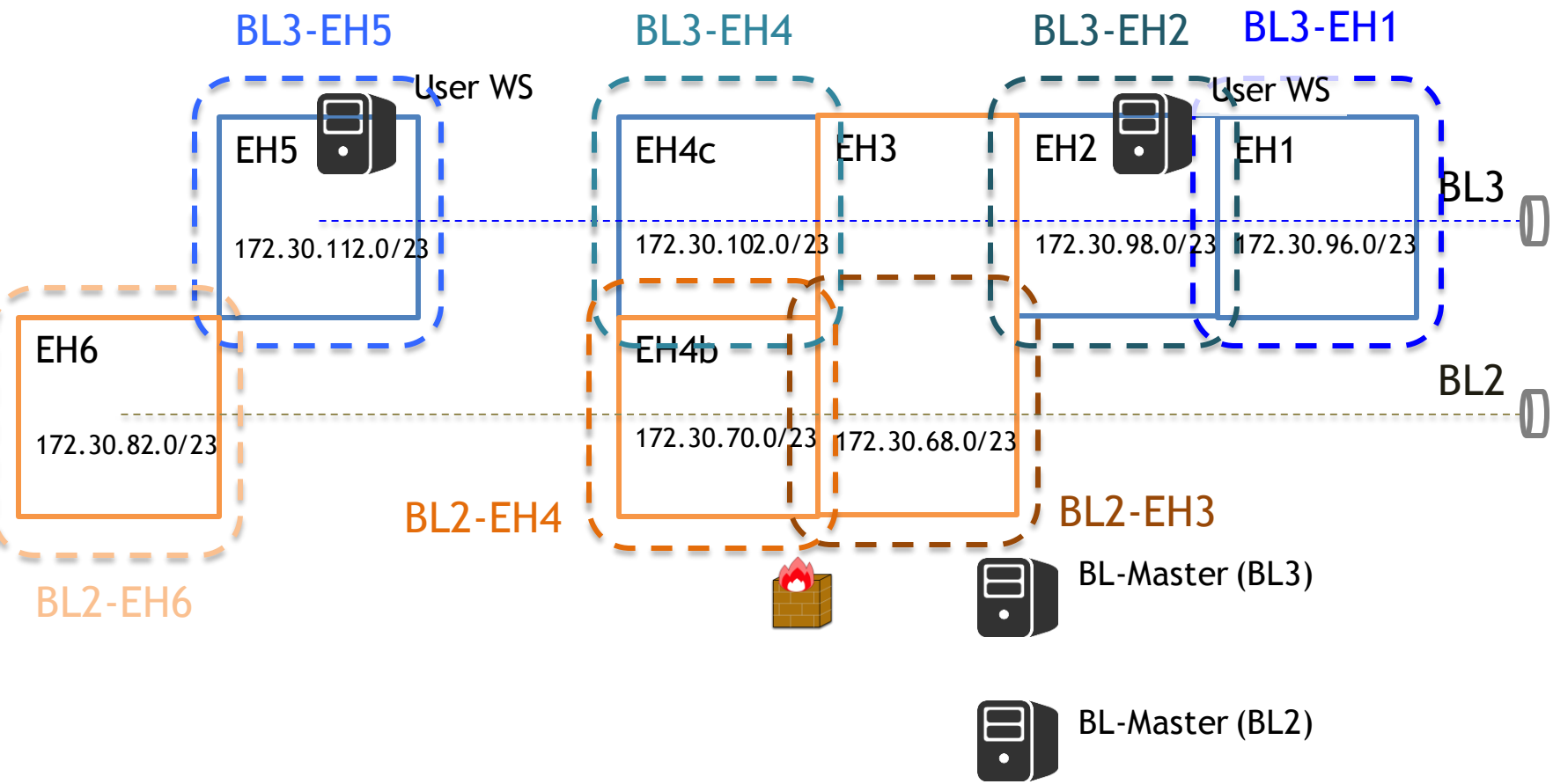
Problem: Network Segment

All of EHs shared one network segment. (This design is same as SPring-8 experiment network)
Since IP address of User-WS/carry-in PCs was arbitrary, the BL-Master can not distinguish message authority: “where this message come from?”



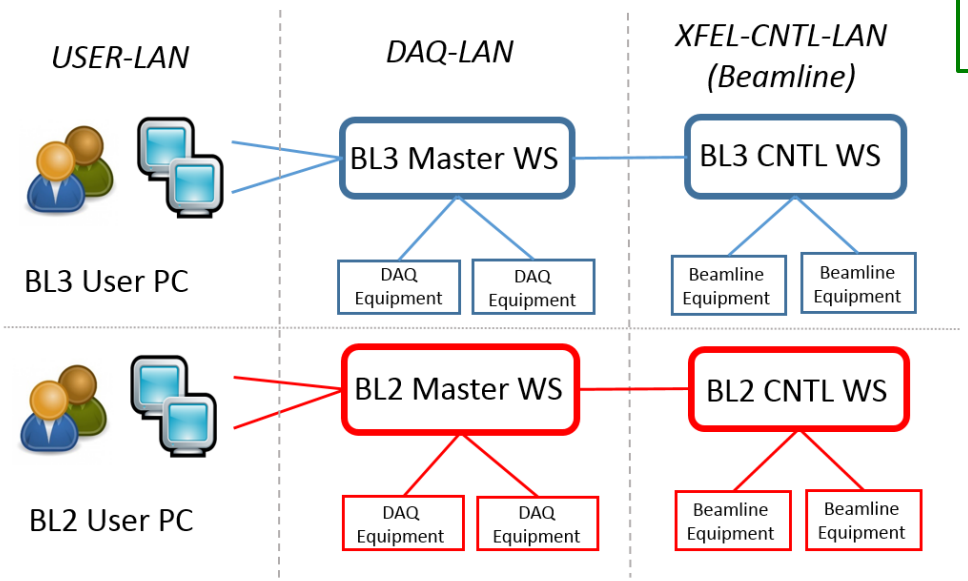
3. Logically segmented by experimental area/unit

In 2014, we divided network segments corresponding to each EHs.



MADOCA2 Message Routing with ACL

WEPGF107, MATSUMOTO et al.,
"Multi-host Message Routing in MADOCA II"



object name	management method	account@hostname
sr_ms_serve	MS	*@*
sr_ms_manage	MS	control@localhost
object_fwd1	MS:host-1	*@*
object_fwd2	MS:host-1,host-2	*@*
object_ip1	MS	*@172.24.12.15
object_ip2	MS	*@172.24.12.0/24

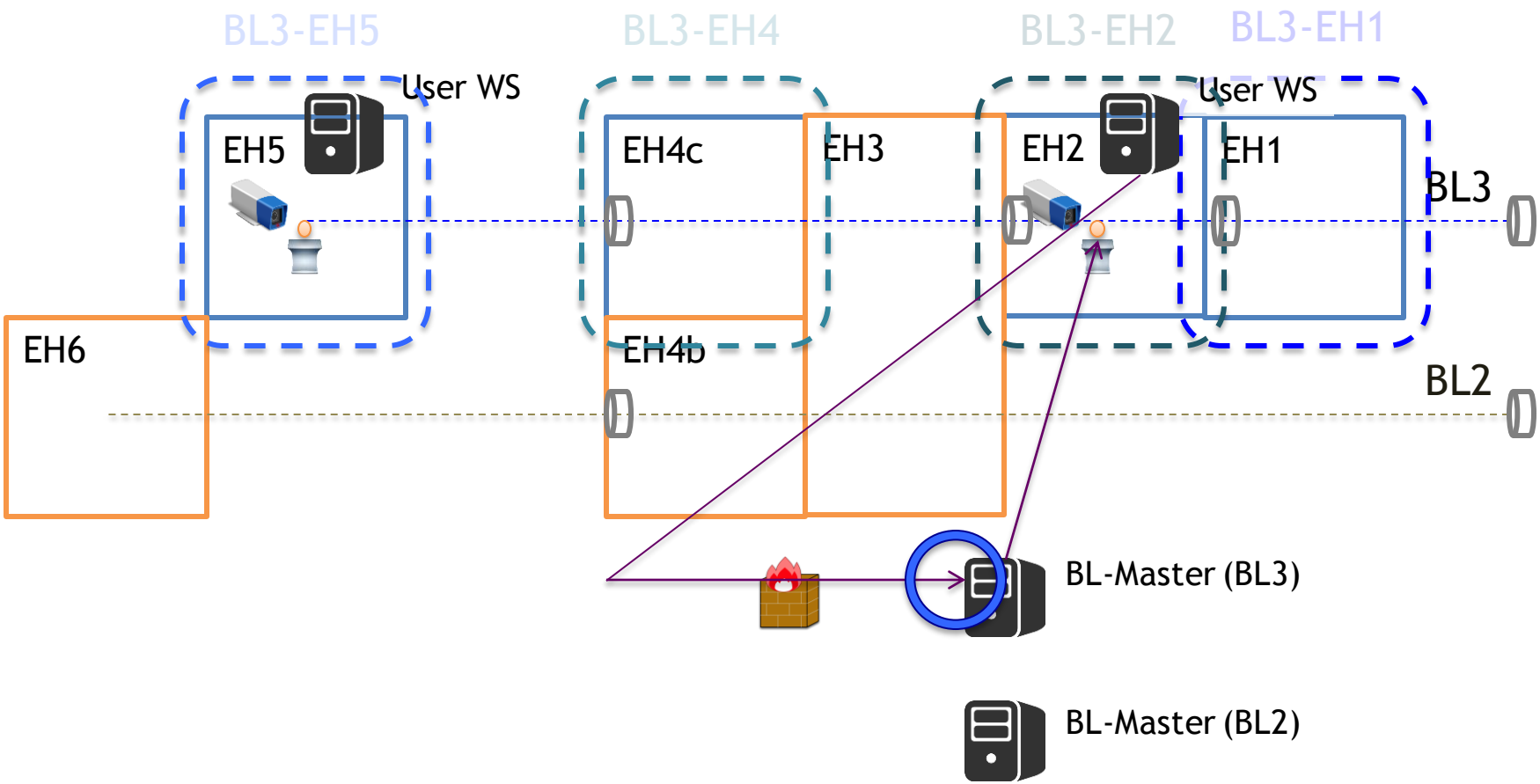
We can use IP/subnet as ACL keys

3. Logically segmented by experimental area/unit

In 2014, we divided network segments corresponding to each EHs.

Using MADOCA2, the BL-Master distinguish message authority, like these:

BL3-Master: Accept message from BL3-EH2 “drives motor in BL3-EH2”



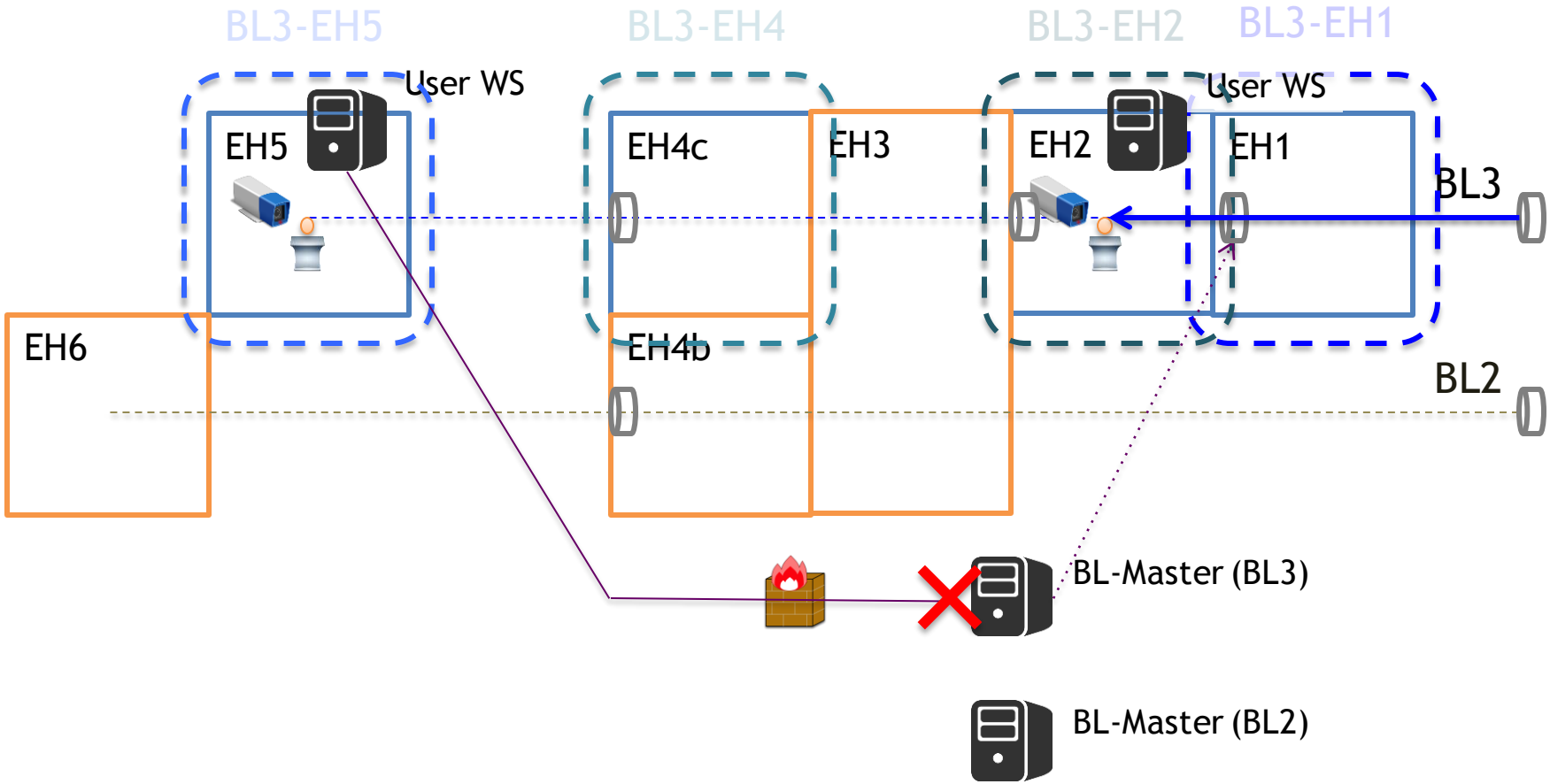
3. Logically segmented by experimental area/unit

In 2014, we divided network segments corresponding to each EHs.

Using MADOCA2, the BL-Master distinguish message authority, like these:

BL3-Master: Accept message from BL3-EH2 “drives motor in BL3-EH2”

BL3-Master: Discard message from BL3-EH5 “open shutter of BL3-EH1”

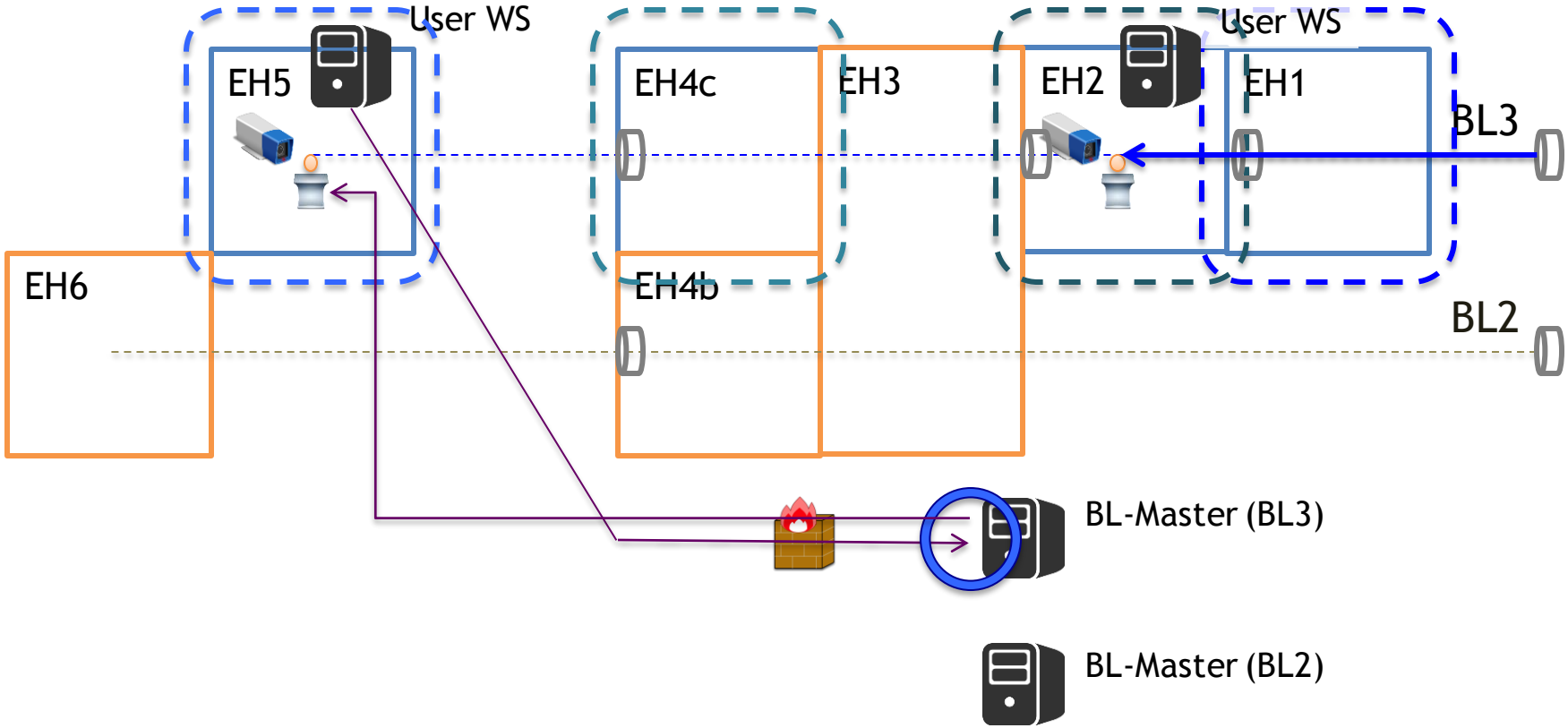


3. Logically segmented by experimental area/unit

In 2014, we divided network segments corresponding to each EHs.

Using MADOCA2, the BL-Master distinguish message authority, like these:

- BL3-Master: Accept message from BL3-EH2 “drives motor in BL3-EH2”
- BL3-Master: Discard message from BL3-EH5 “open shutter of BL3-EH1”
- BL3-Master: Accept message from BL3-EH5 “drives motor in BL3-EH5”

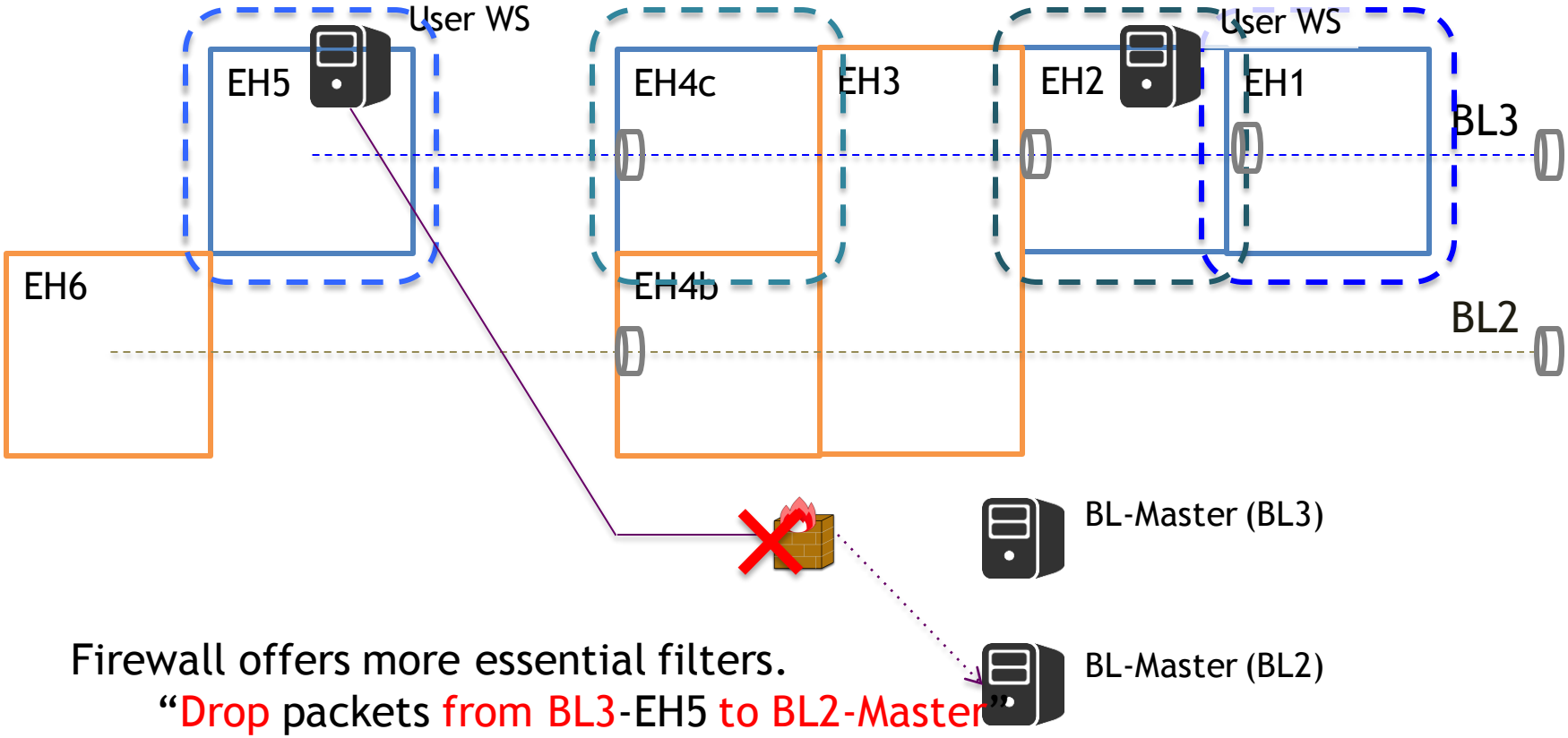


3. Logically segmented by experimental area/unit

In 2014, we divided network segments corresponding to each EHs.

Using MADOCA2, the BL-Master distinguish message authority, like these:

- BL3-Master: Accept message from BL3-EH2 “drives motor in BL3-EH2”
- BL3-Master: Discard message from BL3-EH5 “open shutter of BL3”
- BL3-Master: Accept message from BL3-EH5 “drives motor in BL3-EH5”

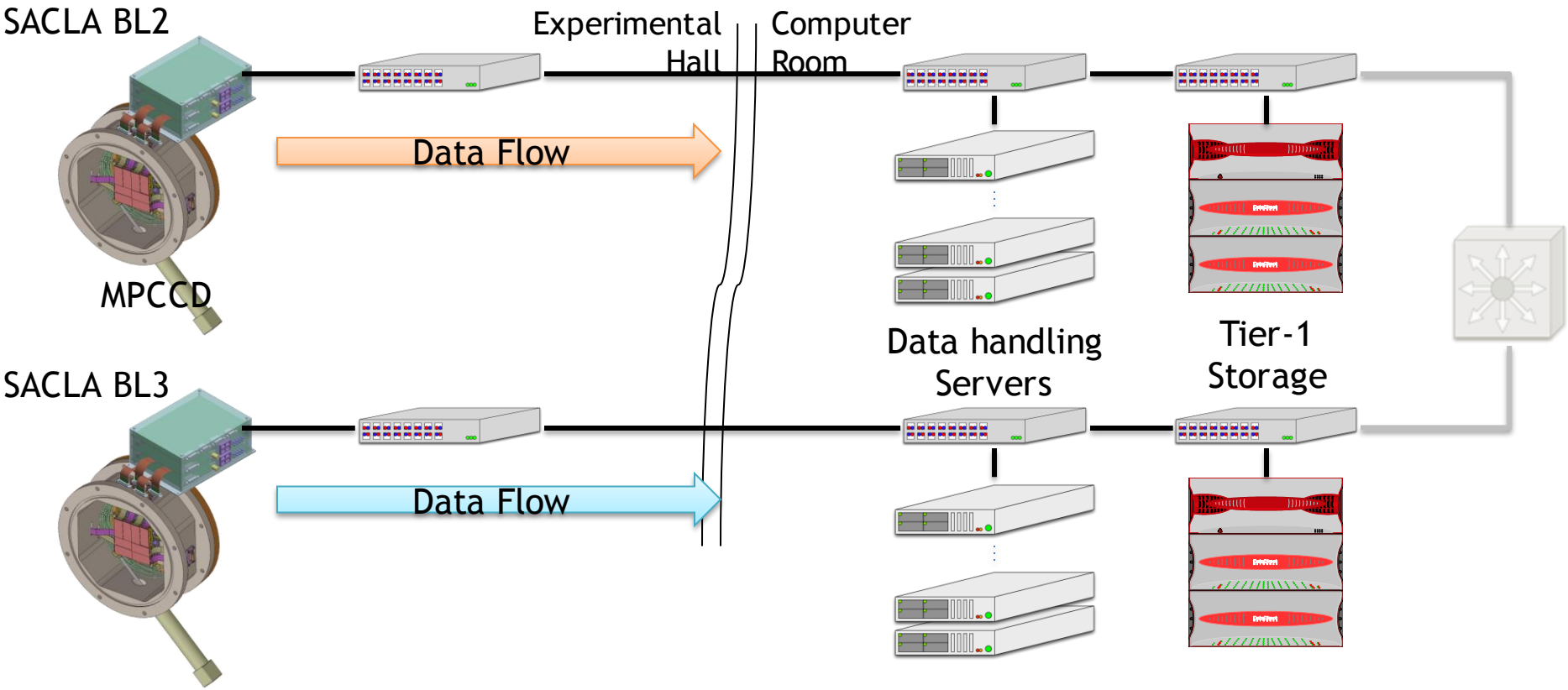


Firewall offers more essential filters.

“Drop packets from BL3-EH5 to BL2-Master”

4. Physically segmented by beamlines

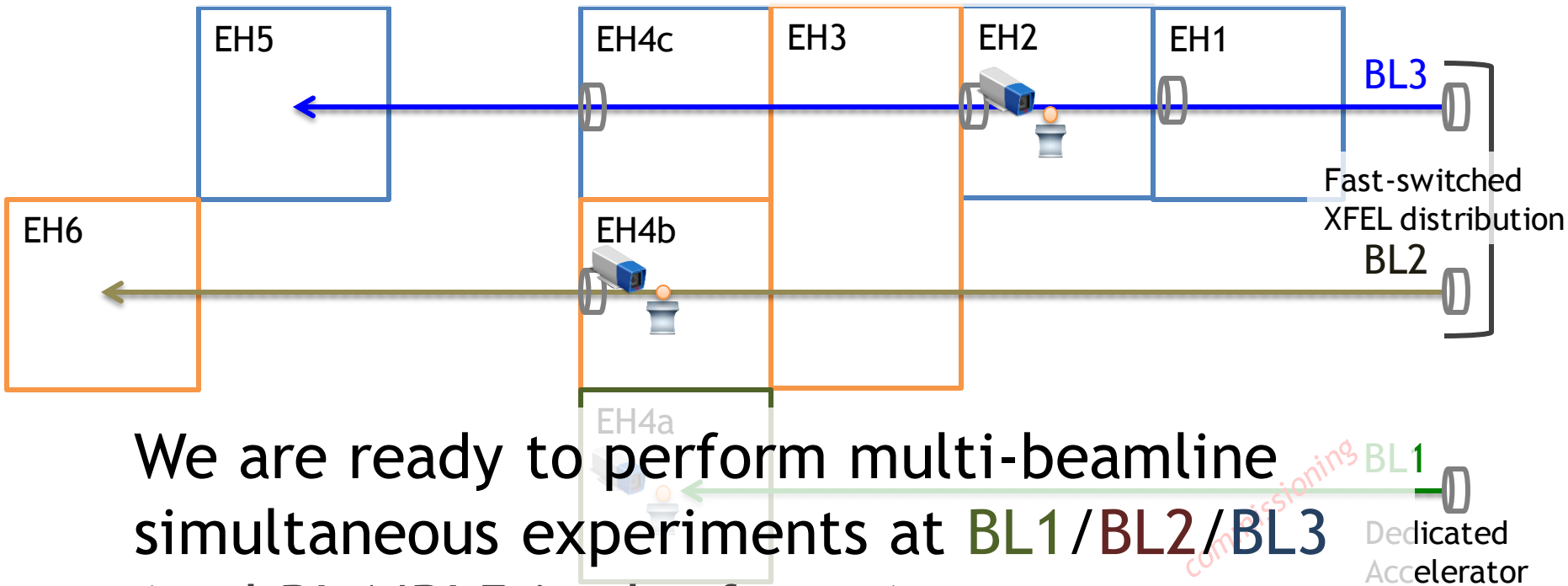
Each beamline occupies dedicate physical network from detector frontend to Tier-1 storage.
The data-handling servers are used for buffering (several seconds). In addition, on-the-fly low-level filtering are performed using the data-handling servers.



Summary

SACLA Experimental Network Policy

1. No internet connectivity
2. Segregate LANs based on purpose
3. Logically segmented by experimental area/unit, to perform multi-beamline experiments
4. Physically segmented by beamlines to guaranty DAQ performance



We are ready to perform multi-beamline simultaneous experiments at BL1/BL2/BL3 (and BL4/BL5 in the future).