International Conference on

Nuclear Decommissioning

15 – 19 May 2023, Vienna, Austria

Addressing the Past and Ensuring the Future

IAEA International Atomic Energy Agency

Challenges on Security Infrastructure for Decommissioning of Nuclear Facilities in Indonesia #50

Bambang Tri Purnomo

Nuclear Energy Regulatory Agency of Indonesia

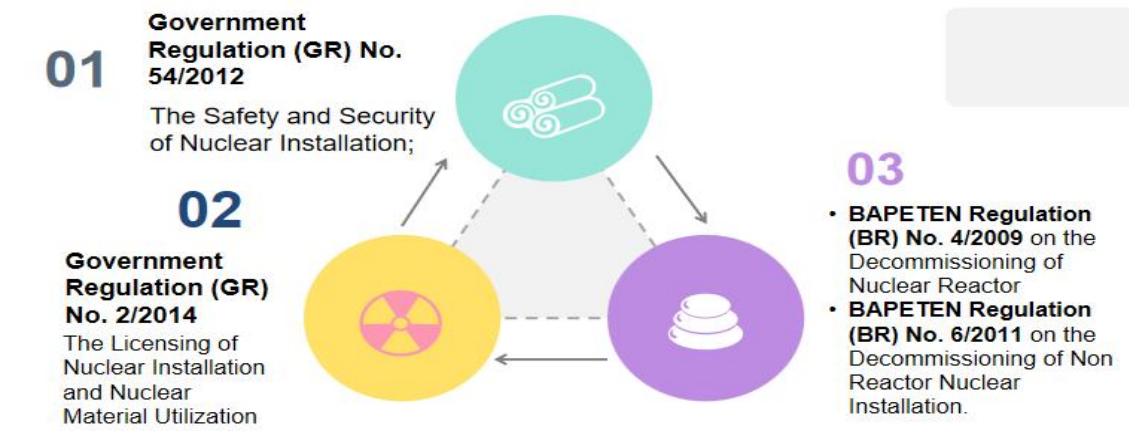
(BAPETEN)

1. Introduction

- During decommisioning process, there is probability that the threat on the theft of nuclear material and the sabotage of nuclear installation still exist.
- Therefore, a security system or physical protection system is still needed during the decommissioning stage.
- Unfortunately, the attention on how to ensure the adequacy of security infrastructure on every steps of decommissioning in Indonesia is still low.
- It is important to evaluate and improve the decommissioning security infrastructure.

3. Regulatory framework in indonesia

- The requirement related to decommissioning nuclear installation in Indonesia are mentioned in some regulations below:



- Since there is no further explanation on the security during decommissioning stage, and considering that the security aspect in decommissioning is no less important than the safety aspect, the national policy regarding security in decommissioning need to be emphasized more.

2. IAEA Guidance for the security of decommissioning

- IAEA guidance on the security of decommissioning can be found in the IAEA Nuclear Security Series (NSS) No. 35-G Security during the Lifetime of a Nuclear Facility,
- the main publication for decommissioning, General Safety Requirement (GSR) Part 6 Decommissioning of Facilities, mostly discuss about the safety requirement.

4. Comparison Between IAEA Guidelines & Indonesia Regulations On Security Of Decommissioning

IAEA Guidelines	Indonesia Regulations
NSS No. 35-G: a. Operator should revise the security plan prior to the transition to decommissioning stage, using graded approach. b. The operator should also revise the security measures for protection of the sensitive information asset, computer security, sustainability, contingency planning, emergency preparedness, incident reporting, trustworthiness, quality assurance, nuclear security culture and nuclear materials accounting and control, as applicable.	1. **GR No. 54/2012:** The licensee should ensure the physical protection of nuclear installations, special equipment, and nuclear related materials. 2. **GR No. 2/2014:** Technical requirements for obtaining Decommissioning permits includes: a. decommissioning program; b. radiation protection and safety program; c. nuclear preparedness program; and d. document management system. 3. **BR No. 4/2009 and BR No. 6/2011:** a. the decommissioning program should includes nuclear security and safeguards programs. b. the security programs for the decommissioning is an adaptation from the existing physical protection plan during operation stage.

Provisions or guidelines that need to be added to the regulations

1. Provision or guideline on the establishment of proper security plan based on every decommissioning steps using graded approach

During decommissioning process/steps, there will be some changes in the facility condition

Right now, there is no clear guideline on those regulation on how to adjust security plan during decommissioning by using graded approach

Risk can arise from the many new personnel/workers, and from the transport of nuclear material.

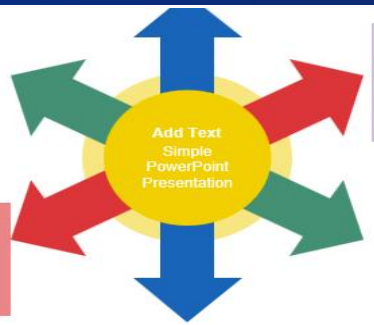
It is likely that the adjustment for decommissioning process is not just by simple adaptation, it could need recalculation on the security plan itself.

Every process or step will have different condition and risk, so it is wise to implement graded approach on the security measures, to avoid wasting resources on unnecessary security

There will also a challenge to integrate the security measures into the workflow of the decommissioning process without hindering work

2. Provision or guideline on how to prevent insider threat

Not every personnel will be involved in the decommissioning process. Some personnel could lost their job.



Meanwhile, there will be some addition of new personnel with various background come to the facility to involve in the decommissioning process

It could create lack of motivation and depression among the personnel, and could create many disgruntled employees.

These condition can increase the risk of the insider threat

The facility need to establish a program to prevent and counter it

3. Provision on the requirement on maintaining security culture

There will be increased pressure to reduce staff number, that could create uncertainty among the personnel.

There will be addition of new workers from contractor who may not understand about security culture.

There will also some changing on the structure and physical layout of the facility as it is dismantled, that may reduce the awareness of the personnel

All of those will affect the strength of security culture on the facility.

4. Provision or guideline on ensuring information security and cybersecurity

there are still a lot of important information that need to be protected during the process

The important information including schematic and diagram of the facility, specific description of the security plan and measures, nuclear material transport routes, access code, etc. So, the facility still need to establish its security.

During the decommissioning, there are also possibility that facility will still use computer based system in many aspect, including safety and security.

To protect those computer based system, facility will need to establish cybersecurity/computer security.

5. Provision on the requirement of financial guarantee of security infrastructures on long decommissioning.

Conclusion

a. Indonesia already has adequate regulations regarding decommissioning, but most of them only focus on the safety aspect.

b. Provisions related to security on decommissioning need to be revised in Indonesian regulations.

c. Several provisions that need to be added on Indonesian regulations on security of decommissioning including establishment of proper security plan using graded approach, prevention against insider threat, information security and cybersecurity, maintaining security culture, and financial guarantee of security infrastructures.